

Professional IT-Security for your Corporation

Utimaco Safeware

www.utimaco.com

SafeGuard[®] RemovableMedia

Version 2.00

**Windows XP
Windows Vista**

utimaco[®]
s a f e w a r e

CONTENT

CHAPTER 1	What is SafeGuard RemovableMedia?	1
	1.1 Supported media	2
CHAPTER 2	Installation	3
	2.1 Interactive installation	3
	2.2 Installation without user interaction	4
	2.2.1 Installation program components	5
	2.2.2 Key distribution via Setup (console).....	5
CHAPTER 3	Quick Start: You want to	6
	3.1 Secure data on your removable media	6
	3.2 Exchange data securely using removable media	8
	3.3 Enforce the exclusive use of encrypted data on removable media	10
CHAPTER 4	Detailed description	12
	4.1 The control dialog	13
	4.1.1 Configuring SafeGuard RemovableMedia	14
	4.2 List of removable devices	14
	4.3 Encrypt new and modified files	15
	4.4 Keys.....	15
	4.5 Manage/Manage Keys	16
	4.5.1 Creating keys	17
	4.5.2 Importing key from file	18
	4.5.3 Setting a key to passive	19
	4.5.4 Backup	19
	4.5.5 Restore.....	20
	4.6 Selecting keys	21
	4.7 Encrypt existing files	22
	4.8 Allow access to plain files.....	22

CONTENT

	4.9 Use these settings for all new drives except CD/DVD	22
	4.10 Private store 'My Safe'	23
	4.10.1 Activating private store 'My Safe'	23
	4.10.2 Unlocking and locking private store 'My Safe'	24
	4.11 Tray icon	24
	4.12 SafeGuard RemovableMedia and DVD/CD-RW drives	25
	4.12.1 Writing encrypted files to CD using the Windows CD Writing Wizard	25
	4.12.2 Windows Vista	26
	4.13 Explorer extensions	27
CHAPTER 5	SafeGuard Portable	28
	5.1 Editing files using SafeGuard Portable	29
	5.1.1 Setting encryption keys	30
	5.1.2 Encrypting	30
	5.1.3 Decrypting	31
	5.1.4 Encrypting new files using SafeGuard Portable	31
	5.1.5 Encryption state	31
	5.1.6 Open	32
	5.1.7 Delete	32
	5.1.8 Copy to	32
	5.1.9 Exit	32
CHAPTER 6	Administration	33
	6.1 Settings	33
	6.1.1 Key handling	34
	6.1.2 Local file encryption	34
	6.1.3 Floppy drive	34
	6.1.4 Event log	35
	6.1.5 Drive policy (under Drive policy node)	35
	6.1.6 Force control dialog	36

CONTENT

6.1.7 Allow default settings	36
6.1.8 Plain directory	36
6.1.9 File types to be encrypted.....	37
6.1.10 Copy SafeGuard Portable	37
6.1.11 Enforce policy selection.....	37
6.1.12 Control dialog (under Control node).....	37
6.1.13 Overlay Icon	38
6.1.14 Explorer extensions.....	38
6.1.15 Tray Icon	38
6.2 SafeGuard RemovableMedia management API	39
6.3 SafeGuard RemovableMedia console application	39

1 What is SafeGuard RemovableMedia?

SafeGuard RemovableMedia is a software package with which you can encrypt data on any removable media that are connected to your computer. To do this, it uses file based encryption technology which implements the state-of-the-art AES 256 algorithm. It runs exclusively on your computer. You do not need to install any additional software on the removable medium! All encryption/decryption tasks run transparently on your computer with minimal user interaction.

As soon as you connect a removable medium to your computer, it is identified by SafeGuard RemovableMedia and a dialog appears in which you can decide how to handle the data on it. If you decide to allow only encrypted access to the removable medium, SafeGuard RemovableMedia will prompt you to create a key. This key is then used to encrypt the data on the medium. Only the person who owns this key can read the content of the encrypted files on the removable medium. All subsequent encryption tasks run transparently. For the user, transparent encryption means that all data stored in an encrypted format is automatically decrypted when it is opened by an application. When the file is saved, it is automatically encrypted again. During your everyday tasks, you will be unaware that you are working with encrypted data. However, if you disconnect the removable medium, the files on it remain encrypted and are therefore protected against unauthorized access. Unauthorized users may be able to access these encrypted files physically. But unless they have SafeGuard RemovableMedia and the corresponding key they will not be able to read them.

When you install SafeGuard RemovableMedia on your computer, the default setting is to prohibit access to any removable media until you tell SafeGuard RemovableMedia how to handle the files on the removable medium. You do this in the dialog which appears when you connect a removable medium to your computer. You can configure SafeGuard RemovableMedia to only allow encrypted files on removable media. In this case, all files already stored on the particular medium will be encrypted and all files which are saved to the medium after this will be stored there in encrypted format. If you decide not to encrypt all existing files, you can allow access to unencrypted files which are already stored on the medium. In this case SafeGuard RemovableMedia will not encrypt the unencrypted files it finds when you connect removable media to the system, but it will encrypt all new files you store on this media. As a result, you can read plaintext files that are present on the removable media, but they are encrypted as soon as you save them there.

You can also use SafeGuard RemovableMedia to exchange encrypted files that are already present on the removable medium. There are two ways you can do this:

1. The recipient of these files must have SafeGuard RemovableMedia installed on their computer and have already received the key from you.
2. Along with the encrypted data, the recipient also receives a SGPortable.exe file which is located on the removable medium. The recipient can then use SafeGuard Portable and the corresponding key to decrypt and then re-encrypt the encrypted files without having to install SafeGuard RemovableMedia on their machine.

SafeGuard RemovableMedia offers companies a means of enforcing specific company policies concerning the use of removable media. For example, it can be configured in such a way as to make it mandatory to store data on removable media in encrypted form only and therefore ensure that no plaintext data leaves the company. You can even predefine which keys are to be used. Company policies are enforced by using an administrative template, which is used to grant or deny certain rights to users.

SafeGuard RemovableMedia supports the use of what is known as a "key ring". A user can own several keys which they then use to encrypt or decrypt data. The files on removable media can be encrypted with different keys.

Although SafeGuard RemovableMedia is a simple and easy-to-use tool it is nevertheless extremely powerful and can be used in many ways.

1.1 Supported media

SafeGuard RemovableMedia supports the following removable media:

- USB sticks
- USB hard disks
- CD-RW drives (UDF)
- DVD-RW drives (UDF)
- FireWire
- Diskettes
- Storage cards in USB card readers.

2 Installation

HINT:

You can only install SafeGuard RemovableMedia if you have Windows Administrator privileges.

2.1 Interactive installation

1. To start the **interactive installation program** double-click **sgrm.msi**. An Installation Wizard guides you through the uncomplicated installation process for SafeGuard RemovableMedia.
2. The *License contract* dialog then appears. If you accept the terms of this license, select the "I accept the license contract" checkbox and click *Next*. If you do not accept the license terms, the installation procedure is cancelled.
3. The *Infofile* dialog appears. SafeGuard RemovableMedia is continually undergoing further development. For this reason, your version may include new features that are not described in this manual. This *Infofile* contains the latest information that you should read very carefully before you continue with the installation.
4. The *target folder* window opens. This shows you the target folder in which the installation will be performed. You can also change this target folder in the dialog you see next by clicking *Select functions*. Click *Next*.
5. This opens the *Select function* dialog. Here you can select the *Target folder* in which you want to install SafeGuard RemovableMedia. If you want to perform the installation in a different folder, click *Browse...* and select the one you want. If you have already installed another of Utimaco's SafeGuard products, you cannot select a different target folder.
Click the *Disk Cost* button to display all available disk drives on your computer. Here you can see how much memory is required to install SafeGuard RemovableMedia, and whether your drives have enough memory for this.
In the selection menu on the left, you can select the SafeGuard RemovableMedia components you want to install.
 - **Client** installs the client software with SafeGuard Portable.
 - **Administration** installs the administrative documentation, the SafeGuard RemovableMedia console and the SafeGuard RemovableMedia API.
Select the components you want to install on your computer and click *Next*.

6. In the next window, click *Next* to start installation.

If the installation is successful, a dialog appears. Click **Finish** to finish the installation.

HINT:

After installation is complete, you must restart your computer. The next dialog prompts you to do this.

2.2 Installation without user interaction

To perform an installation without user interaction you must call the `msiexec` program from the console with a specific set of parameters.

```
msiexec /I <path+MSI installation package name > /qn ADDLOCAL=ALL|  
<components>
```

```
i/
```

This shows that the procedure is an installation.

```
<path>
```

Drive letter and folder of the MSI file.

```
/qn
```

Does not display a user interface during installation.

```
ADDLOCAL=
```

Lists the components that are to be installed.

```
ALL
```

Installs all components

```
<components>
```

The components that are to be installed.

This folder is used as the default folder for installation:

```
<SYSTEM>:\Programs \Utimaco
```

Example:

```
msiexec /i D:\SGRemovableMedia\Version_1.10_Beta\sgrm.msi /qn  
ADDLOCAL=ALL
```

After installation is complete, your computer reboots automatically.

2.2.1 Installation program components

- **RemovableMedia**
Installs the SafeGuard RemovableMedia user documentation.
- **Client**
Installs the Client software with SafeGuard Portable.
- **german**
Installs the German language package to allow you to switch the software's language to German. The default language is English.

2.2.2 Key distribution via Setup (console)

If you want to install an existing backup file during installation, enter this command via the console. Note where the sgrm.msi file is stored on your computer and enter the correct path.

```
msiexec /i sgrm_German.msi RMFILE="c:\install\sgrm.rmb"  
RMFILEPWD="1q2w3e4r"
```

RMFILE = path and name of the backup key file

RMFILEPWD = password for the backup key file.

You can use the installed backup key as soon as installation is complete.

3 Quick Start: You want to ...

The following sections describe three main scenarios which are covered by SafeGuard RemovableMedia. Follow the instructions below to get your system running with the basic settings.

To fine-tune your system, you will find a more detailed description of the different options of SafeGuard RemovableMedia in the chapters that follow.

3.1 Secure data on your removable media

SafeGuard RemovableMedia can be used to secure data stored on your removable media by means of encryption. It guarantees that no unauthorized person can access your data in case of theft or loss. It can be configured in such a way that all data that is already stored on the media, and all data that is written to it after SafeGuard RemovableMedia is installed, will be encrypted. Only a person who owns the key used for encryption of the files can access the data. The example below refers to this scenario. You can secure your data in just two steps: specify how SafeGuard RemovableMedia should handle data on the removable media and create/select a key. To secure the data on your removable media, follow these steps:

1. Install SafeGuard RemovableMedia on your computer.
2. Connect your removable media.
3. SafeGuard RemovableMedia displays a dialog in which you select the access mode.
4. On the left-hand side of the dialog the system displays a list of the drive letters of all removable media. [The drive letters of some removable media are only displayed when they are connected to the system \(e.g. USB sticks\). If your desired medium is not displayed, connect it to the system. A removable medium may also contain more than one drive. Each drive is displayed separately. Select the drive letter for which you want to make the settings.](#)
5. To encrypt the data on the medium, select **Encrypt new and modified files**. [When you select this option, all files that are written to the removable medium will be encrypted. Files that are already stored on the medium stay unencrypted \(plain\) but you cannot open them \(access denied\). This option does not affect files that are already stored on the removable medium!](#)
6. To create a key for the selected disk drive, click the **Manage...** button. The *Manage Keys* window appears.
7. In the *Manage Keys* window, click the **Create Key** button.

8. Then, in the *Create Key* window, enter a name and a passphrase for the key. Confirm this passphrase and click **OK**.
9. To encrypt existing files on the removable medium, select **Encrypt existing files** and **Allow access to plain files**.

This will immediately encrypt all files stored on the removable medium at this time, so that there are no more unencrypted files on it.

Ensure the **Allow access to plain files** option is also checked, because SafeGuard RemovableMedia needs to have access to the plain files on the medium, for encryption.
10. Optionally you can select the **Use this setting for all new drives except CD/DVD** option.

If you select this option, you will not have to specify the settings for each of your devices. The specified settings then apply to all removable media, that you connect to your system. They represent a kind of default policy for your system. If you make use of this option, you will not have to complete the dialog when you connect a different removable medium. The settings automatically apply to any connected medium.

SafeGuard RemovableMedia distinguishes between CD/DVD and "all other" removable media, so this setting changes to **Use this setting for all new CD/DVD drives** when you select a CD/DVD drive from the list on the left-hand side.
11. Click **OK**.
 - ▶ As a result, if you selected the **Encrypt existing files** option, all files on your removable medium are immediately encrypted (initial encryption). If you did not trigger initial encryption, only files that are saved to the medium in the future will be encrypted. All files you save to the removable medium will be encrypted. All encryption/decryption tasks run transparently in the background. You will not notice that you are working with secured data. Your removable medium is secured by SafeGuard RemovableMedia!

After you have defined how the removable medium is to be handled, SafeGuard RemovableMedia automatically copies an SGPortable.exe file onto it. SafeGuard Portable allows you to exchange data with other removable media without having to install SafeGuard RemovableMedia. For further information about this tool refer to "SafeGuard Portable" on page 28.

3.2 Exchange data securely using removable media

SafeGuard RemovableMedia can be used to exchange files on removable media in a secured way.

There are two ways of exchanging data securely with removable media.

1. The recipient of these files must have SafeGuard RemovableMedia installed on their computer and have already received the key from you.
2. Along with the encrypted data, the recipient also receives a SGPortable.exe file which is located on the removable medium. Using SafeGuard Portable and the corresponding key, the recipient of the encrypted files can decrypt them and the re-encrypt them without having to install SafeGuard RemovableMedia on their machine.

The example used here describes the method in which the recipient has already installed SafeGuard RemovableMedia on their computer. Chapter 5, SafeGuard Portable, contains all the information you need to use SafeGuard Portable.

To exchange data securely, follow these steps:

1. Install SafeGuard RemovableMedia on your computer.
2. Connect your removable medium.
3. SafeGuard RemovableMedia displays a dialog in which you select the access mode.
4. On the left-hand side of the dialog you see a list of the drive letters for all removable media. Some of these drive letters are only displayed when the removable media are actually connected to the system (e.g. USB sticks). If the drive letter for the medium you want to use is not displayed, connect it to the system. A removable medium may also contain more than one drive. Each drive is displayed separately.
Select the drive letter, for which you want to make the settings.
5. In order to encrypt the data on the media, select **Encrypt new and modified files**.
When you select this option, all files that are written to the removable media will be encrypted. Files that are already stored on the media remain in plaintext but you cannot open them (access denied). This option does not affect files that are already stored on the removable medium!
6. To create a key for the selected disk drive, click **Manage...**
This opens the *Manage Keys* window.
7. In the *Manage Keys* window, click the **Create Key** button.
8. In the *Create Key* window, enter a name and a passphrase for the key.

Before you can exchange encrypted files it is essential, that the person with whom you want to exchange these files, owns the key that was used to encrypt them. You therefore need to provide the key (key name and passphrase) to this person. To access the files, the recipient must then add this key to their key ring.

Make sure you remember the key passphrase!

9. After confirming the passphrase click **OK**.
 10. The key now appears in the key list in the control dialog.
If the list contains more than one key, select the one you want.
 11. To encrypt existing files on a removable medium, select **Encrypt existing files**.
This will immediately encrypt all files that are currently stored on the removable medium. As a result this medium will no longer contain any unencrypted files.
 12. Alternatively, you can select the **Use this setting for all new drives except CD/DVD** option.
If you do this, you will not need to specify the settings for each of your devices. The specified settings will apply to all removable media you connect to your system. If you select this option, you will not need to complete the dialog when you connect a different removable medium. The settings automatically apply to any medium you connect.
If you do not select this option, you can specify different settings.
SafeGuard RemovableMedia distinguishes between CD/DVDs and "all other" removable media. Therefore this setting changes to **Use this setting for all new CD/DVD drives** when you select a DVD/CD-ROM drive in the list on the left-hand side.
 13. Click **OK**.
 14. Provide the key (key name and passphrase) to the person with whom you want to exchange data.
They must then enter this data in the SafeGuard RemovableMedia control dialog in order to add this key to their key ring.
 15. You can now give your medium to this person.
As SafeGuard RemovableMedia has the correct key, no user interaction is necessary when the recipient connects the media to the system. All encryption and decryption tasks run transparently in the background.
This works for all persons who have SafeGuard RemovableMedia installed on their computer and who own the key you used to encrypt your data.
- ▶ As a result, both persons now own the same key and therefore are able to access the files. Every time you select another key from your key ring and use it to encrypt files, you have to provide the relevant key to the person with whom you want to exchange these files.

3.3 Enforce the exclusive use of encrypted data on removable media

Companies may want to enforce certain security policies. For example, they may decide that every file that enters or leaves the company on removable media must be encrypted. SafeGuard RemovableMedia not only allows the company to ensure that files saved to removable media are always encrypted, but it also prevents plaintext files from being brought into the company, by only accepting encrypted files from removable media. This can be enforced on client computers by using group policy settings that are defined via a SafeGuard RemovableMedia administrative template. SafeGuard RemovableMedia settings can be specified for computers or users. To ensure that only encrypted files are used on removable media, proceed as follows:

1. Install SafeGuard RemovableMedia on your client computers.
2. Add the administrative template SGuard.adm to your group policy (under User Configuration). The template is stored in `<Installation Drive>\Program Files\Utimaco\ADM`.

3. Specify the following setting in the ADM template:

Activate **Encrypt new and modified files** under

```
Computer Configuration\  
Administrative templates\  
SafeGuard  
\RemovableMedia\  
Drive Policy\  
Drive Policy
```

This triggers the encryption of all files that are written to removable media. Files that are already stored on the media remain in plaintext, but users cannot open them (access denied). As SafeGuard RemovableMedia does not permit access to plaintext files until you explicitly activate the corresponding option, you can no longer access the plaintext files on the removable media.

When SafeGuard RemovableMedia detects a removable medium it displays its control dialog. Users cannot access the medium until they create an encryption key that can be used for it.

4. You can also specify the key that is to be used to encrypt the files on the removable medium. To do so, follow these two steps: Specify an encryption key name in the adm template. Then create a key using the `sgrmcmd` command line tool (“SafeGuard RemovableMedia console application” on page 39):

To do so this, specify the following settings under:

```
Computer Configuration\  
Administrative templates\  
SafeGuard\  
SafeGuard
```

RemovableMedia\
Key Handling

Enter a name for the key to be used in field **Encryption Key Name**.

5. Using the sgrmcmd command line tool to create a key with this name.
sgrmcmd must run on the user's machine under the user's account.
This setting means that you must use the specified key. As no user interaction was explicitly allowed in the ADM template, the SafeGuard RemovableMedia control dialog does not appear.
- ▶ Once these settings are made on the client computers, users can only use encrypted files on their removable media. When they connect a medium, SafeGuard RemovableMedia instantly displays the dialog for selecting a key. Alternatively, they can use the predefined key for all encryption tasks that involve removable media.

This means the company can be sure that only encrypted files are read from and saved to the users' removable media.

Users cannot access plaintext files on their removable media.

4 Detailed description

After it has been installed, the default setting for SafeGuard RemovableMedia is to prevent any access to removable media. Access to removable media is not granted until you have specified how SafeGuard RemovableMedia is to handle removable media when they are connected to your computer. To do this, SafeGuard RemovableMedia automatically displays a dialog once it has identified that a removable medium is present.

In your company's environment, the settings made by the system administrator for SafeGuard RemovableMedia in your group policy, determine whether you can change a setting or not. These settings are made centrally by a system administrator and define how your computer reacts. As a result, this section may describe options, that are disabled on your computer. If this is the case, these options have been disabled due to your company's security policy.

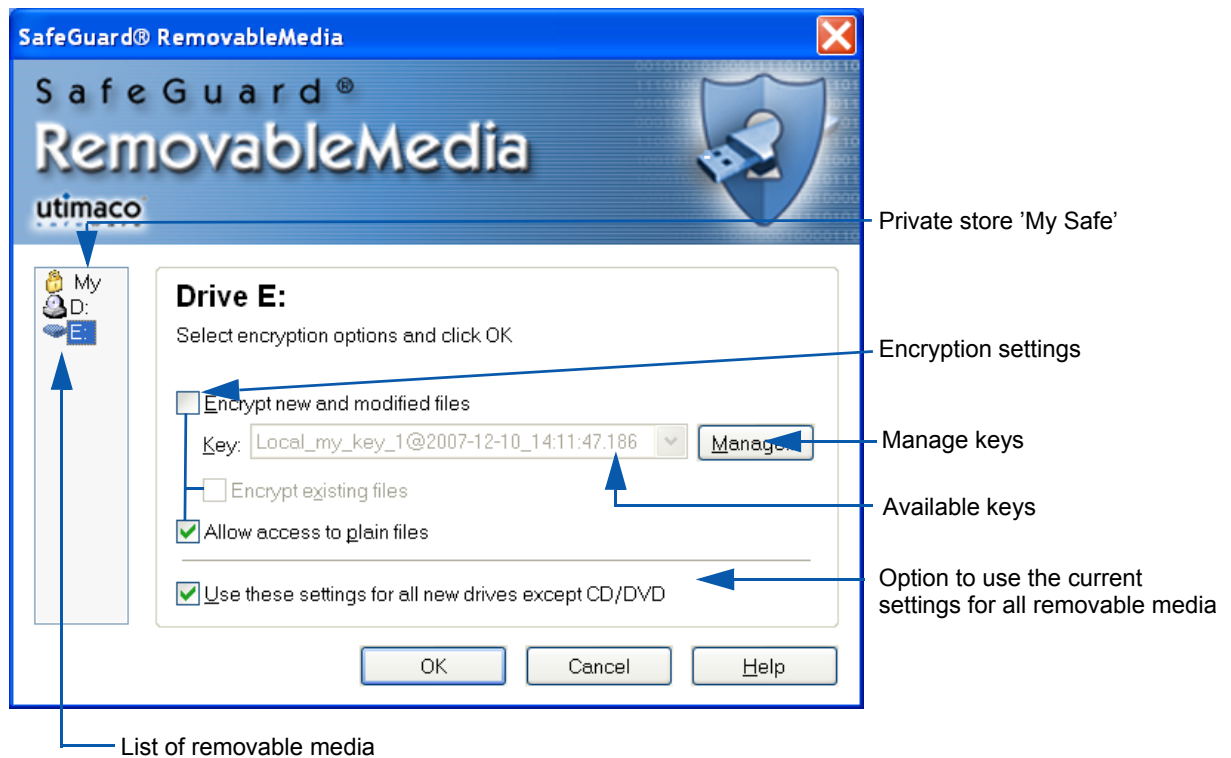
HINT:

A system administrator can even configure SafeGuard RemovableMedia in such a way that no dialog is displayed at all, and the SafeGuard RemovableMedia settings for your removable media apply automatically.

The settings you make are stored on each removable medium. If SafeGuard RemovableMedia detects a removable medium, it will handle this medium according to the settings stored on it until you change them.

4.1 The control dialog

Once it detects a removable medium, SafeGuard RemovableMedia displays its control dialog to specify how this device/drive is to be handled



HINT:

SafeGuard RemovableMedia can be configured in such a way that this dialog is not displayed and the media it detects are handled according to predefined policies. These policies can either be specified by a user (by activating **Use these settings for all new drives except CD/DVD**) or centrally, by a system administrator.

4.1.1 Configuring SafeGuard RemovableMedia

To configure SafeGuard RemovableMedia to suit your own specific requirements:

1. Select a drive.
2. Specify how encrypted files are to be handled
 - **Options:**
 - Encrypt new and modified files
 - Encrypt existing files
 - Allow access to plain files
3. Create/select an encryption key.
4. Repeat these steps for all drives displayed.

HINT:

In a company environment, the central settings made by the system administrator will define whether or not users can change any settings.

4.2 List of removable devices

The drive letters of all removable media that have been detected are displayed on the left-hand side of the control dialog. Drive letters shown in bold represent newly-detected media.

If a private store (My Safe) was activated on your computer via centrally defined settings, drive **MS** will be displayed in addition. Whether or not the private store is available, can only be defined via central settings in group policies.

You must select each drive letter to specify the settings for each removable medium. If these settings are made centrally, you can display them by clicking on the drive letter you require.

HINT:

Some removable media drive letters are only displayed when they are connected to the system (e.g. USB sticks). If you cannot see a drive letter for the medium you want to use, connect it to the system. Removable media may also contain more than one drive. Each drive is displayed separately.

4.3 Encrypt new and modified files

When you select this option, all files that are written to the removable medium will be encrypted. Files that are already stored on the medium remain in plain, but you cannot open them. Access to these files is denied.

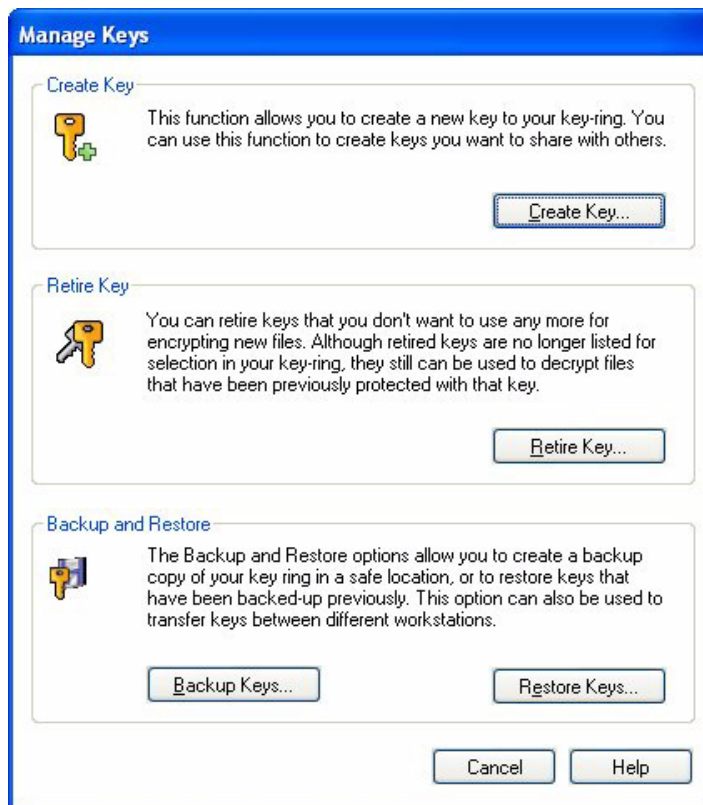
This option does not affect files that are already stored on the removable medium!

4.4 Keys

Before you can encrypt data you need an encryption key. If you select an encryption option, you must then create or select a key so that you can encrypt the data. A key consists of a **name** and a **passphrase**.

4.5 Manage/Manage Keys

When you click the *Manage* button, the *Manage Keys* window opens. In this window you can add a key, set a key to passive (after which you can only use the key to decrypt data, not to encrypt it) or back up or restore a key.



4.5.1 Creating keys

To create a key, proceed as follows:

1. In the *Manage Keys* window, click the *Create Key* button. This opens the *Create Key* window.

2. Enter a **Key Name** (key names are case sensitive!) and a **Passphrase** for the key. SafeGuard Removable Media automatically generates a unique name for the key. This name will be displayed in field *Full Name*. The key will also be displayed under this name in the list of available keys. The full name cannot be changed.
3. Confirm the passphrase. If you enter an insecure passphrase, a warning message will be displayed. To enhance the level of security, we recommend the use of complex passphrases. However, you can decide to use the insecure passphrase despite the warning message.

HINT:

To exchange encrypted data, you have to provide the passphrase of the key used for encryption to the relevant recipient. The recipient can import this key. Once you both share the same key, you can exchange encrypted data

- ▶ After clicking OK the key will be displayed in the control dialog's key list and you can select it for each

drive. You can add an unlimited number of keys. Your key ring consists of all keys you have created or imported. Now you can decrypt all data that have been encrypted using one of the keys included in your key ring.

4.5.2 Importing key from file

If you have received removable media containing encrypted data which has been encrypted using a key that is not included in your key ring, you can import the required key to your key ring. To import the key, you need the relevant passphrase. The person who has encrypted the data has to provide you with the passphrase.

Select the relevant file on the removable media and choose **SafeGuard Removable Media > Import key** from the file's context menu.



Enter the passphrase in the dialog displayed. The key will be imported and you can access the file.

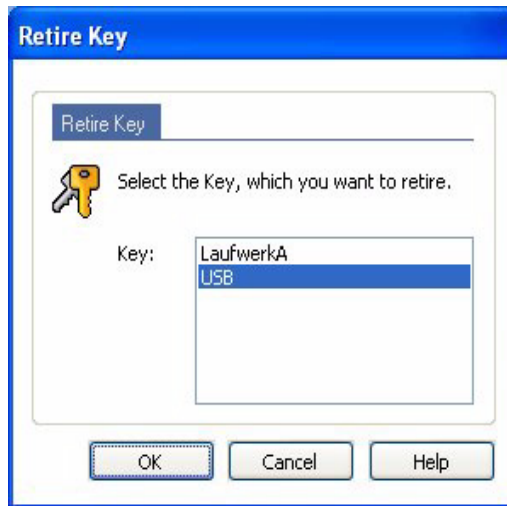
Dispose key upon logoff

If you activate this option, the key will only be added temporarily to your key ring. It will be available for the duration of the current work session. As soon as you log off from Windows or reboot the computer, the key will no longer be available. If required, it has to be imported again.

4.5.3 Setting a key to passive

If you set a key to passive it can no longer be used to encrypt data. However, if you used this key to encrypt data you can still use it to decrypt this data. This is why this key is still stored on your computer.

In the *Manage Keys* window, click the *Retire Key* button and then, in the *Retire Key* window select the key you want and click OK. This key now no longer appears in the key list in the main dialog.



This is a good function to use if, for example, a member of staff who knows the keyword leaves the company, if only one person knows the key or if, for security reasons, a new encryption key has to be generated at regular intervals.

4.5.4 Backup

You can prepare a backup of your key ring which you can upload at any time (Restore).

To do so, go to the *Manage Keys* window and click the *Backup* button. In the *Backup Keys* window, enter path and file name for the backup file. The file extension must be `.rmb`. *SafeGuard RemovableMedia* suggests file name `sgrm.rmb` by default. Enter the password (you must enter the password twice) and click OK. A `.rmb` file will be created on your computer.

HINT:

When you create a backup, the tool creates an encrypted copy of your key ring. This procedure does not involve the key in the local machine store.



For security reasons, we strongly recommend that you create a backup of your key ring at regular intervals.

4.5.5 Restore

If you have made a backup of your key ring, you can restore it at any time.

To do this, go to the *Manage Keys* window and click the *Restore* button. Then select the path, enter the password for this key and click OK.

You can also select the *Overwrite keys of the same name* option here. If you do not activate this option, any existing keys that have the same name are not overwritten.

The key is then displayed again in the control dialog where you can select it to encrypt data.



4.6 Selecting keys

Once you have created the keys, you can select them from the key list in the control dialog and use them to encrypt files on a particular removable medium.

You can also change a drive's encryption key once it has been used for encryption. For this you only need both keys. The files will then be re-encrypted with the new one. New files will be encrypted with the new key. Files that have already been encrypted will keep their original encryption key.

If you also want to use the new key for files that have already been encrypted on the medium, check the **Encrypt existing files** option after you changed the key. This will trigger a new initial encryption, where the files are decrypted and then re-encrypted with the new key.

HINT:

Be careful when you use a new key for data that has already been encrypted. If you have previously shared the key with someone to exchange encrypted data, they will not be able to access the data until you provide them with the new key.

4.7 Encrypt existing files

When you select this option, all files already present on the removable medium will be encrypted immediately when you click OK in the control dialog.

HINT:

*To encrypt existing files, select the **Allow access to plain files** option, because you need to access plain files before you can encrypt them on the medium.*

Be careful when you use this option. Removable media may contain files that you do not want to be used in your network. If you encrypt these files, they can be opened as usual when SafeGuard RemovableMedia is installed.

For example, if you want to prevent unwanted external data being brought into your company on removable media by only accepting encrypted data, this feature might not be the best method of achieving this. This is because, if unwanted data is already present on the medium when the encryption process starts, these files will also be encrypted. Once these files are encrypted, they can be opened on any computer on which SafeGuard RemovableMedia is installed and where the corresponding key is available. This option should only be used if you are sure that there is no unwanted data on the medium.

To ensure that no unwanted data, that may be present on the medium, can be accessed, you can use the *Encrypt new and modified files* option. This setting makes sure that newly saved files are encrypted, and that access to any unwanted plain files already present on the medium is denied.

4.8 Allow access to plain files

The default setting is to deny access to plaintext files. You can activate this option to have access to plaintext files on the medium. If you do not save these files, they will remain on the medium as plaintext files. If you save them to the removable medium, they will be encrypted.

4.9 Use these settings for all new drives except CD/DVD

This option allows you to specify a kind of default policy for your system. If you select this option, you will not need to specify the settings for each of your devices. The specified settings then apply to all removable media you connect to your system. If you select this option, you will not need to complete the dialog when you connect a different removable medium. The settings apply automatically to any connected medium, so that the SafeGuard RemovableMedia control dialog does not appear each time you connect removable media to your system.

You can change these default values at any time. To do this, start the SafeGuard RemovableMedia control dialog by right-clicking the tray icon in the Windows Toolbar and then clicking the SafeGuard RemovableMedia entry. You will now see the control dialog in which you can select a drive letter and specify the new settings for it.

SafeGuard RemovableMedia distinguishes between CD/DVDs and "all other" removable media. Therefore this setting changes to Use this setting for all new CD/DVD drives when you select a CD/DVD drive from the list on the left-hand side.

4.10 Private store 'My Safe'

In private store 'My Safe', files can also be stored in encrypted form on the computer's local hard disk.

HINT:

This functionality has to be explicitly activated via a group policy setting. Otherwise this function will not be available.

'My Safe' will be created as a predefined directory named `My Safe` under `My Documents` (the directory containing for example subdirectory `My Pictures` etc.). All files stored in this directory (and also all files stored in `My Safe` subdirectories) will be encrypted with a key that has to be generated once.

Whereas a user will automatically have access to all SafeGuard RemovableMedia keys once he has logged on to the system successfully, access to this private store will not be granted automatically. The user has to unlock the private store explicitly in order to access it. The store can also be locked again at any time.

4.10.1 Activating private store 'My Safe'

The prerequisite for users to be able to use the private store is that they have been allowed to do so via the group policy applying to the relevant user.

If this is the case, an icon will be displayed for private store 'My Safe' in the control dialogs's list of available media.

1. To be able to use 'My Safe', a key has to be generated once.
2. Select drive **MS** from the list of available drives in the control dialog of SafeGuard Removable Media.

3. Click **Unlock** in the *My Safe* dialog.
As no key has been defined yet the dialog for generating the key for the private store will be displayed automatically.
4. Enter a **Passphrase** and **confirm** it.
5. The key will be created and private store 'My Safe' will be unlocked.

HINT:

The generated key will only be used for the private store. It will not be available in the control dialog's key selection list and it cannot be changed.

4.10.2 Unlocking and locking private store 'My Safe'

To be able to use the private store, you always have to explicitly unlock it first.

To do so, select the **MS** icon from the list of available removable media, click **Unlock** and enter the **Passphrase**.

You can lock the store at any time in the same way using button **Lock**. If the private store is locked, the files stored in it cannot be accessed.

4.11 Tray icon

SafeGuard RemovableMedia adds an icon to the Windows Taskbar. Right-click on the icon to display a menu that lists the following entries:

- **SafeGuard RemovableMedia**
Displays the SafeGuard RemovableMedia control dialog where you specify or modify the settings for your removable medium.
If all settings are made centrally, and the user is not allowed to change the settings, this dialog can be used to display the settings for the different drives.
- **Help**
Launches the SafeGuard RemovableMedia online help.
- **About**
Displays information about your version of SafeGuard RemovableMedia.

4.12 SafeGuard RemovableMedia and DVD/CD-RW drives

SafeGuard RemovableMedia distinguishes between CD/DVDs and "all other" removable media. If you use packet writing (UDF) with your CD/CD/DVD-RW recording drive you can use CDs and DVDs in the same way as any other removable media, apart from encrypting existing files on it.

Because of this difference you cannot activate the *Encrypt existing files* option in the SafeGuard RemovableMedia main dialog for CD/DVD drives. In the adm template you also have to specify separate settings for the DVD/CD-RW drives.

If you use CD burning software and do not use packet writing (UDF), you are not able to write SafeGuard RemovableMedia encrypted files to DVD/CD-RW because they will be decrypted automatically. But you can use the Windows CD Writing Wizard for writing these encrypted files to CD (also on DVD under Windows Vista).

4.12.1 Writing encrypted files to CD using the Windows CD Writing Wizard

SafeGuard RemovableMedia allows you to write encrypted files to CDs using the Windows *CD Writing Wizard*.

To do so, an encryption rule has to be specified for the CD recording drive. SafeGuard RemovableMedia adds a dialog to the CD Writing Wizard. In this dialog you can specify how the files will be written to CD (encrypted or in plaintext).

HINT:

If there is no encryption rule for the CD recording drive, files are always written to CD in plaintext. The SafeGuard RemovableMedia dialog, where you can specify the encryption state of files to be written to the CD can be specified, will not be displayed.

After you have entered a name for the CD, the *SafeGuard Removable Disk Burning extension* is displayed.

Under *Statistic* the following information is displayed:

- how many files are selected to be written to CD
- how many of them are encrypted
- how many of them are plaintext files

Under *Status* information on the keys used for encryption are displayed.

For encrypting files which are to be written to CD always the key, which is specified in the encryption rule for the CD recording drive is used.

A situation where files to be written to CD are encrypted with different keys may arise, when the encryption rule for the CD recording drive has been changed. Plaintext files may be found in the temporary area where the files are held before they are copied to the CD, when the encryption rule was deactivated when they have been added.

Encrypting files on CD

If you want to write the files to the CD in encrypted form, click the **(Re)Encrypt all files** button.

If necessary, already encrypted files will be re-encrypted and plaintext files will be encrypted. On the CD, the files are encrypted using the key which was specified in the encryption rule for the CD recording drive.

Writing files to CD in plaintext

If you select **Write all files in plain**, the files are first decrypted and then written to the CD.

Copy SafeGuard Portable to optical media

If you select this option, SafeGuard Portable will also be copied to the CD. This allows reading and editing files encrypted with SafeGuard RemovableMedia without having SafeGuard RemovableMedia itself installed.

4.12.2 Windows Vista

Windows Vista also provides the CD Writing Wizard for DVDs.

The SafeGuard Disc Burning Extension for the CD Writing Wizard is only available for burning CDs/DVDs in **Mastered** format. The Wizard will only be displayed, if data are to be written on CDs/DVDs in **Mastered** format.

For the Live File System no Recording Wizard has to be used. In this case the recording drive is used like any other removable media. If there is an encryption rule for the recording drive, the files will be encrypted automatically when they are copied to the CD/DVD.

4.13 Explorer extensions

SafeGuard RemovableMedia adds extensions to Windows Explorer. The entry **SafeGuard RemovableMedia** is displayed in the File menu and in the context menus for drives, directories and files.

The following functions are available via entry SafeGuard RemovableMedia:

- Import keys
- Show data encryption state
- Show the control dialog of SafeGuard RemovableMedia

To import a key from an encrypted file to your key ring, select **SafeGuard RemovableMedia > Import key** from the context menu. You will need the key's passphrase for importing the key. The file's sender has to provide you with the passphrase.

To open the control dialog, select **SafeGuard RemovableMedia > SafeGuard RemovableMedia** from the context menu.

To display a dialog providing information on the file (key name, is this key included in your key ring yes/no, are you allowed to access the file yes/no), select **SafeGuard RemovableMedia > Show Encryption State** from the context menu.

The color of the key shown besides the files in Windows Explorer also indicate the encryption state:

Green Key

The file is encrypted and you can access it.

Red Key

The file is encrypted and you cannot access it.

If no key is displayed, the file is not encrypted.

5 SafeGuard Portable

SafeGuard Portable allows you to exchange encrypted data with removable media, without your communications partner first having to install SafeGuard RemovableMedia. When you use SafeGuard Removable Media to encrypt a file for the first time, it creates an SGPortable.exe file on your removable medium.

Your communications partner can then use SafeGuard Portable on the removable medium together with the appropriate passphrase to decrypt the encrypted data and then encrypt it again.

HINT:

The passphrase has to be communicated to the recipient beforehand.

In this situation your communications partner can either use the existing key generated by SafeGuard RemovableMedia for the encryption or (for example, for newly arrived data) generate a new key with SafeGuard Portable to encrypt this new data.

SafeGuard Portable does not need to be installed on or copied to your communications partner's computer. It remains on the removable media.

This makes SafeGuard the ideal tool for exchanging encrypted data with removable media without having to install additional software for this purpose.

Any data that was encrypted by a SafeGuard RemovableMedia key can be decrypted and re-encrypted again with the help of SafeGuard Portable.

HINT:

SafeGuard Portable is designed to be used on computers on which SafeGuard RemovableMedia is not installed.

The result of this is that the encryption policies defined with SafeGuard RemovableMedia cannot be evaluated if SafeGuard Portable is used.

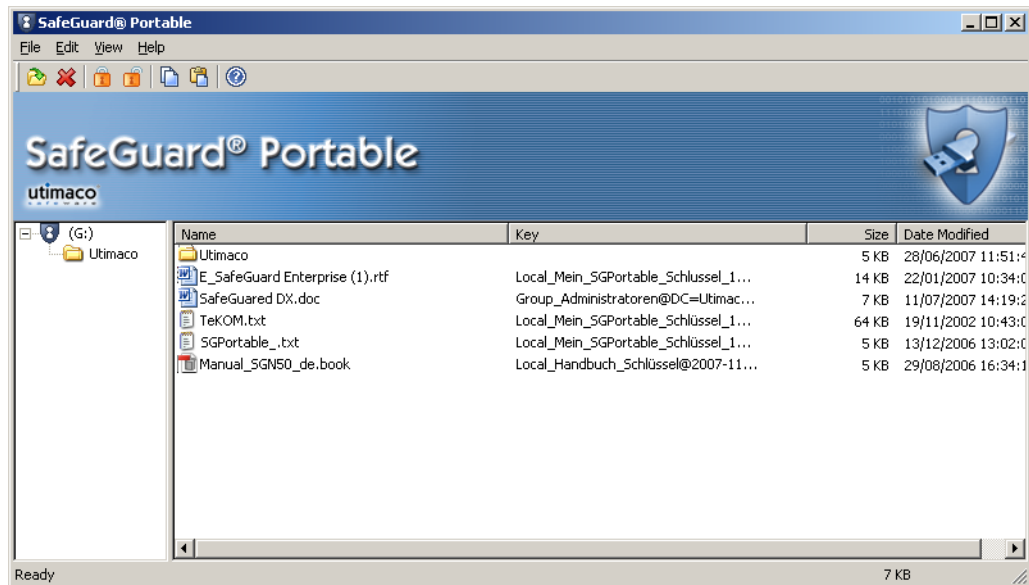
If SafeGuard RemovableMedia and SafeGuard Portable are used in parallel on the same computer, the user can use SafeGuard Portable to encrypt and decrypt SafeGuard RemovableMedia files independently of the policy settings.

If you therefore want to ensure that SafeGuard Portable users cannot use SafeGuard Portable to decrypt data that was encrypted with SafeGuard RemovableMedia, you should only use keys whose passphrase is not known by the SafeGuard Portable users.

5.1 Editing files using SafeGuard Portable

You have received a removable medium containing files encrypted with SafeGuard Removable Media as well as a folder named *SGPortable*. This folder contains the file *SGPortable.exe*.

Start SafeGuard Portable by double-clicking on *SGPortable.exe*. Using SafeGuard Portable you can decrypt the encrypted data contained on the removable medium and encrypt them again. SafeGuard Portable offers a similar functionality as Windows Explorer.



In addition to the file details known from Windows Explorer (Name, Size, ...) SafeGuard Portable shows column *Key*. This column indicates whether the relevant data are encrypted. If a file is encrypted, the name of the used key is displayed.

HINT:

You can only decrypt files, if you know the relevant passphrase for the key used.

To edit files on the removable medium (encrypt/decrypt, ...), select the file via a left click and choose the relevant command from the context menu (via a right click) or from the *File* menu.

The following menu commands are available in the context menu via your right mouse button:

Set Encryption Key	Opens the <i>Enter Key</i> dialog. In this dialog you can generate an encryption key via SafeGuard Portable.
Encrypt	Encrypts the activated file on your removable medium. The key last used is used for encryption.
Decrypt	Opens the Enter Passphrase dialog. Enter the passphrase for decrypting the selected file in this dialog.
Encryption State	Displays a dialog and shows the file's encryption state.
Copy to	Copies the file to a folder of your choice and decrypts it.
Delete	Deletes the activated file from your removable medium.

You can also select commands Open, Delete, Encrypt, Decrypt and Copy via the icons shown in the toolbar.

5.1.1 Setting encryption keys

To encrypt a file on removable media and to create a key using SafeGuard Portable for this purpose, select menu command *Set Encryption Key* from the context menu via your right mouse button or from the *File* menu. The *Enter Key* dialog is displayed.

Enter a **Name** and a **Passphrase** for the key. **Confirm** the passphrase and click **OK**.

The key is created and will be used for encryption from now on.

5.1.2 Encrypting

To encrypt a file on removable media, select the file in SafeGuard Portable Explorer and choose command *Encrypt* from the context menu using your right mouse button. The file will now be encrypted using the key last used by SafeGuard Portable.

When saving new files on removable media using a drag-and-drop operation in the Explorer, you will be asked whether you want to encrypt the files. If this is the case and there has been no encryption using SafeGuard Portable before, a dialog for setting the key opens. Enter the name of the key and the passphrase (the passphrase has to be confirmed by repetition) in this dialog and click **OK**.

Select the file to be encrypted with the key you have just set using your left mouse button and choose the *Encrypt* command from the context menu via your right mouse button or from the *File* menu. The file will now be encrypted. Upon successful completion of this process a message will be displayed.

HINT:

From now on the key last used and set by SafeGuard Portable will be used for all subsequent encryption processes you perform with SafeGuard Portable unless you set a new key.

5.1.3 Decrypting

To encrypt a file on removable media, select the file in SafeGuard Portable Explorer and choose command *Decrypt* from the context menu using your right mouse button. The dialog for entering the passphrase is displayed. Enter the relevant passphrase (the sender has to provide you with this passphrase) and click **OK**. The file will now be decrypted.

When decrypting a file which has been encrypted using a key you have generated in SafeGuard Portable, this file will be decrypted automatically.

HINT:

After decrypting files on removable media and entering the key's passphrase you do not have to enter it again the next time you encrypt or decrypt files which have been encrypted with the same key. SafeGuard Portable "remembers" the passphrase as long as the application is running. The last key used by SafeGuard Portable is used for encryption.

After decrypting the files they are available in plaintext on the removable medium. To ensure that they remain encrypted on the removable medium, the files have to be explicitly encrypted. Simply copying the relevant file to the removable medium will not suffice.

5.1.4 Encrypting new files using SafeGuard Portable

You can also copy your own files in encrypted form on removable media using SafeGuard Portable.

To do so, simply move the required files into the SafeGuard Portable Explorer using a drag-and-drop operation. The system asks you whether you want to encrypt the relevant file. If you confirm, the file will be encrypted with the key last used and copied to the removable medium.

5.1.5 Encryption state

To determine a file's encryption state, select the file using your left mouse button and choose the *Encryption State* command from the context menu via your right mouse button or from the *File* menu. The encryption state will also be indicated in column *Key* next to the file name in SafeGuard Portable Explorer.

5.1.6 Open

This menu command is only available via the SafeGuard Portable *File* menu. Upon opening an encrypted file via this menu command you will be prompted to enter your passphrase. Enter your passphrase and click **OK**. The file will be encrypted and opened.

5.1.7 Delete

Deletes the selected file.

5.1.8 Copy to

This menu command is only available in the context menu you can display using your right mouse button in SafeGuard Portable Explorer. Using this command you can copy files from removable media to another drive on your computer.

5.1.9 Exit

This menu command is only available in the SafeGuard Portable *File* menu. *Exit* closes SafeGuard Portable.

6 Administration

If you are using Active Directory Group Policies to administer your network, you can use the SafeGuard RemovableMedia administrative template to define the settings for SafeGuard RemovableMedia centrally.

All settings can be made in the user settings and/or computer settings for your Group Policy Object (GPO).

If users are not allowed to change a setting, the settings made under **User Configuration** will always overrule those made under Computer Configuration. Only if no settings have been made under User or Computer Configuration does the user's default policy - specified by activating the **Use these settings for all new drives ...** - come into effect.

To define the settings for SafeGuard RemovableMedia centrally, follow these steps:

1. Open the GPO in which you want to make your SafeGuard RemovableMedia available in the Management Console (MMC).
2. If you have not yet done so, add the "SGuard.adm" adm file (stored in `<Installation Drive>\Program Files\Utimaco\ADM`) to the "Administrative Templates" section in the GPO's "User Configuration" or "Computer Configuration". The "SafeGuard \ RemovableMedia" nodes contain settings that are transferred to the clients if the appropriate user/computer logs on to the network.

HINT:

The settings made in the administrative template are only applied when SafeGuard RemovableMedia is started. Just opening the SafeGuard RemovableMedia dialog will not suffice: to apply them, the user must log on to Windows again.

6.1 Settings

For most settings, you can specify whether or not they can be changed by the user. Example:

- Encrypt new and modified files.
- User can enable/disable encryption for new files.

If both options are activated, the user is allowed to disable the encryption of new files in the SafeGuard RemovableMedia control dialog. If you do not want to allow the user to disable encryption, deselect the second option.

If you want to allow the user to change the settings, these centrally-defined settings will only become the default values after the user logs on.

If the user changes the setting, the client remembers the user's setting, and it is not overwritten by the settings in central administration.

The same principle applies to all the other settings that a user can be allowed to change.

HINT:

The next sections do not describe whether or not a user is allowed to change a setting.

6.1.1 Key handling

Here you can specify the name of an encryption key, which users require to encrypt their data. If you do not allow users to select a key, this is the only key they can use.

HINT:

*The key whose name is specified here must be present on the user's computer, before this setting is made. If it is not, the user will not be allowed access to encrypted files.
If your company wants to enforce the use of a specific company key, it must first be distributed to the users. To do this, use the SafeGuard RemovableMedia console applications in the API.*

6.1.2 Local file encryption

This setting activates private store 'My Safe' on the user's computer. The user can only apply the local file encryption of SafeGuard RemovableMedia after option *Enable local encryption* has been activated.

The list of available removable media in the control dialog will include 'MS' (for 'My Safe'). The user can generate a key for the private store and use it on their computer.

6.1.3 Floppy drive

If option *Floppy drive will be ignored by removable media detection* is activated, files saved to floppy disks will not be encrypted. In this case, the list of available removable media will not include floppy disk drives.

6.1.4 Event log

Specifies the events to be logged by SafeGuard RemovableMedia. You can select between:

- errors and information
- no logging
- only errors (default)

SafeGuard RemovableMedia logs errors and information in the Windows event logging.

6.1.5 Drive policy (under Drive policy node)

- These settings are used to specify a default encryption policy for all removable media except DVD/CD-RW drives.

HINT:

*The settings for DVD/CD-RW drives are included under node **Drive Policy for DVD/CD-RW Drives**. Here, the same settings as for drive policies apply, except for **Encrypt existing files**. This option is not available for DVD/CD-RW drives.*

- **Encrypt new files**
When you select this option, all files that are written to the removable medium will be encrypted. Files already present on the medium remain in plaintext but the user cannot open them. Access is denied. This option does not affect files that are already stored on the removable medium!
- **Encrypt existing files (needs access to plain files)**
When you select this option all files already present on the removable medium when the policy is activated, will be encrypted immediately when the device is connected.
If selected, the *Allow access to plain files* option will also have to be activated. This is because you need to access plaintext files before you can encrypt plaintext files on the medium. Make sure that the *Allow access to plain files* option is selected! For technical reasons, consistency checks cannot be performed in the Microsoft Management Console and therefore this setting cannot be activated automatically.
Be careful when you use this option. The removable medium may contain files that you do not want to be used in your network. If you specify that these files are to be encrypted, they can be opened as usual when SafeGuard RemovableMedia is installed.
This option should only be used if you are sure that there is no unwanted data on the user's medium.
- **Allow access to plain files**
Activate this option to allow users access to plaintext files on the medium. As long as they do not save

these files, they remain as plaintext files on the medium. If they save them to the removable medium, the files will be encrypted.

- **Store user settings on the removable media and apply them**

If you select this option, the current SafeGuard RemovableMedia user settings will be written to the removable media. Upon reconnecting the relevant medium to the system these settings will be transferred and applied to the relevant drive. If the settings have been modified in the meantime, they will be overwritten by the settings transferred from the medium.

6.1.6 Force control dialog

This option defines if and when the control dialog, in which the user defines the settings for encryption (e.g. key generation etc.), will be displayed automatically.

- **Yes**

The control dialog will be displayed automatically as soon as removable media are connected to the computer.

- **Yes, if no policy is available** (default)

The dialog will only be displayed, if no policy is available and user interaction is required. This is for example the case, if the user has to generate/select a specific key for the relevant medium.

- **No**

The control dialog will never be displayed automatically. If required, the user has to display it via the taskbar icon.

6.1.7 Allow default settings

If this option is activated, the user is allowed to activate option *Use these settings for all new drives*.

This enables the user to define a specific default setting to apply to all new drives.

6.1.8 Plain directory

Via this setting you can specify a directory on the removable medium in which files will not be encrypted, even if encryption has been activated for the medium itself.

If you enter a directory name in the input field, files located in this directory on the removable medium remain unencrypted.

For example, if you enter directory name `plain` in this field, files located in `..\plain` on the removable medium remain unencrypted. All other files will be encrypted.

6.1.9 File types to be encrypted

Here you can specify the file types to be encrypted. Only files with the specified extension will be encrypted. All other files will stay plain.

It is possible to specify several file types. File types have to be separated by semicolons (example: `doc;xls;ppt`).

6.1.10 Copy SafeGuard Portable

If you activate this option, SafeGuard Portable will automatically be copied to all removable media connected to the system, if encryption has been activated for the respective media.

6.1.11 Enforce policy selection

This setting can be used to force the user to select a policy for any newly attached device. If activated, the SafeGuard RemovableMedia control dialog can only be closed after a policy for this new device has been defined.

6.1.12 Control dialog (under Control node)

If you activate this option, the control dialog will not be displayed automatically as soon as removable media are connected to the computer.

HINT:

Independent of this setting the control dialog is always displayed, if removable media with incomplete settings (e.g. missing key) are connected to the computer.

6.1.13 Overlay Icon

Using this option you can specify whether files handled by SafeGuard RemovableMedia, are marked by overlay icons (keys) or not:

- **Yes:** Overlay icons will be displayed.
- **No:** No overlay icons will be displayed.
- **Smart:** Overlay icons will only be displayed for files on removable media and in „MySafe“.

6.1.14 Explorer extensions

If you activate this option, the SafeGuard RemovableMedia Explorer extensions will not be displayed on the client computers.

6.1.15 Tray Icon

Using this option you can control the behavior of the SafeGuard RemovableMedia tray icon in the Windows Task bar:

- **Yes:** The tray icon will be displayed.
- **No:** The tray icon will not be displayed.
- **Smart:** The tray icon will only be displayed, if removable media are connected to the computer.

6.2 SafeGuard RemovableMedia management API

The SafeGuard RemovableMedia API provides a programming interface for customers who want to develop their own applications to perform specific administration tasks in SafeGuard RemovableMedia. The API has been developed in C/C++ and provides interfaces that comply with the C language standard.

The current version of the tool provides key management functions such as:

- **Backup** (back up a key ring)
- **Restore** (restore a key ring)
- **Create Key** (generate a new key for the user's key ring)
- **Retire Key** (set key to passive)
- **Remove Key** (removes a key from a user's key ring)
- **Set Attribute** (set a key attribute)
- **Is Key Available** (is the key available?)

Note that the SafeGuard RemovableMedia Console is a full, released application. It is based on the API that is supplied with this product.

You will find full details of all the encryption management functions in the next section, "SafeGuard RemovableMedia console application".

6.3 SafeGuard RemovableMedia console application

You can use the SafeGuard RemovableMedia console tool to perform administration tasks from the Windows command line in Windows. It is based on the SafeGuard RemovableMedia Management API and offers the same functionality without the necessity to develop an application with the SafeGuard RemovableMedia Management API. SafeGuard RemovableMedia can run interactively from the command line or as an automated script.

The current version of the tool offers encryption management functions such as:

- **Backup** (backup a key ring)
- **Restore** (restore a key ring)
- **Create Key** (generate a new key for the user's key ring)
- **Retire Key** (the key is set to passive)

- **Remove Key** (removes a key from a user's key ring)
- **Set Attribute** (set a key attribute)
- **Is Key Available** (check if the key is available)

If you would like to use one of the functions mentioned above via the console, open the command line window in your operating system and enter the following command:

```
sgrmcmd
```

When you enter this command, make sure you have entered the correct path. You will find *sgrmcmd.exe* in the folder in which you have installed SafeGuard RemovableMedia.

sgrmcmd.exe runs. It provides you with several encryption management functions, which are described individually in the following sections.

Backup

Stores the personal key ring in a backup file which you must specify.

Syntax:

```
sgrmcmd BACKUP key backup file identifier
```

Separate each command with a blank space.

HINT:

If you enter this command, the system displays the options for the individual commands:

```
sgrmcmd RESTORE
```

Here we have used RESTORE as an example because it is not possible to enter any options for the BACKUP command.

Restore

Restores a key from a backup file.

Syntax:

```
sgrmcmd RESTORE key backup file identifier option
```

Here you can enter:

-E	This marks the key as non-exportable. This means you cannot create a backup of this key.
-H	Marks the key as passive. Although the key can still be used for decryption, it can no longer be used to encrypt files.
-L	The key is saved in the local machine store. Every user who is logged on can use this key. This option presents a certain security risk because this key is "available" to everyone who logs on to your computer.
-O	Overwrites a key that has the same name.

Create Key

Generates a new key.

Syntax:

```
sgrmcmd CREATEKEY key name key passphrase option
```

Here you can enter:

-E	This marks the key as non-exportable. This means you cannot create a backup of this key.
-H	Marks the key as passive. Although the key can still be used for decryption, it can no longer be used to encrypt files.
-L	The key is saved in the local machine store. Every user who is logged on can use this key. This option presents a certain security risk because this key is "available" to everyone who logs on to your computer.

Retire Key

Sets a key to passive. Although the key can still be used for decryption, it can no longer be used to encrypt files.

Syntax:

```
sgrmcmd RETIREKEY key name
```

Remove Key

Deletes a key from the key ring.

Syntax:

```
sgrmcmd REMOVEKEY key name
```

Set Attribute

Sets an attribute for a key

Syntax:

```
sgrmcmd SETATTRIBUTE key name
```

Here you can enter:

-E	This marks the key as non-exportable. This means you cannot create a backup of this key.
-H	Marks the key as passive. Although the key can still be used for decryption, it can no longer be used to encrypt files.
+H	Marks a passive key as active again. This therefore means that this key can be used to encrypt and decrypt files again.

Is Key Available

Checks whether a key is present in the key ring and active.

Syntax:

```
sgrmcmd ISKEYAVAILABLE key name
```

Technical Support

Online Documentation

Our knowledge database provides answers to many typical questions about the SafeGuard product range, including its functionality, implementation, administration and troubleshooting.

Link to support area: <http://www.utimaco.com/myutimaco>

To access the public area of the knowledge database you can logon as a guest user. To access the restricted area of the knowledge database you need a valid software maintenance agreement. Our support staff continually adds to the contents of both areas, and keeps them up to date on an on-going basis.

Advanced support services and telephone support

For customers with a valid maintenance contract, qualified support staff is available to provide advice and assistance. To receive a contract offer tailored to your specific needs, please contact your Utimaco sales partner.

We hope you understand that some enquiries from customers without a maintenance agreement may require several working days to process. In urgent cases, please contact the Utimaco sales partner from whom you bought your licenses or software subscription.

Utimaco Safeware



**Utimaco Safeware AG
(Personal Device Security)**
Hohemarkstraße 22
DE-61440 Oberursel
Phone +49 (0) 61 71 88-0
Fax +49 (0) 61 71 88 -10 10
E-Mail: info.de@utimaco.de

**Utimaco Safeware AG
(Transaction Security)**
Germanusstraße 4
DE-52080 Aachen
Phone +49 (0) 2 41 16 96-1 00
Fax +49 (0) 2 41 16 96-1 09
E-Mail: info.de@utimaco.de

**Utimaco B.V.
(Benelux)**
Hoevestein 11B
NL-4903 SE Oosterhout NB
Phone (NL) +31 (0) 162 480 240
Phone (BE) +32 (0) 16 44 01 35
Fax (NL) +31 (0) 162 430 330
E-mail: sales@utimaco.nl

Utimaco Safeware (Schweiz) AG
Zürcherstraße 20
CH-8952 Schlieren
Phone +41 (44) 7 35 40 80
Fax +41 (44) 7 35 40 85
E-Mail: info.ch@utimaco.ch

Utimaco Safeware AG
Triesterstraße 10/2
AT-2351 Wiener Neudorf
Phone +43 2236 205 655
Fax +43 2236 205 655 - 50
E-Mail: channel.at@utimaco.at

Utimaco Safeware AB
Box 16, Malaxgatan 1
SE-16493 Kista
Phone +46 (8) 5 84 00-6 00
Fax +46 (8) 5 84 00-6 10
E-Mail: info.se@utimaco.com

Utimaco Safeware Oy
Airport Plaza Presto
Äyritie 12 b
FIN-01510 Vantaa
Phone +3 58 (9) 85 53-2 00
Fax +3 58 (9) 85 53-20 30
E-Mail: info.fi@utimaco.com

Utimaco Safeware France
8, place Boulnois
F-75017 Paris
Phone +33 (1) 56 21 25 25
Fax +33 (1) 42 67 30 00
E-Mail: info@utimaco.fr

Utimaco Safeware Ltd.
Ash House
Fairfield Avenue
Staines
Middlesex TW18 4AB
Phone: +44 1784 22 42 25
Fax: +44 1784 22 42 29
E-Mail: sales.uk@utimaco.co.uk

Utimaco Safeware Inc.
10 Lincoln Road
Suite 102
Foxboro, MA 02035
Phone +1 (508) 543-1008
Fax +1 (508) 543-1009
Toll Free +1 877-UTIMACO
E-Mail: sales.us@utimaco.com
www.utimaco.us

Utimaco Safeware K.K.
Nisso 16 Building, 3F
3-8-8 Shin Yokohama,
Kohoku-ku
Yokohama 222-0033
JAPAN
Phone +81 (0) 45 - 470 -1430
Fax +81 (0) 45 - 470 -1431
E-Mail: info.jp@utimaco.jp

Utimaco Safeware Asia Ltd.
Unit 602, Stanhope House
734 King's Road
Quarry Bay
Hong Kong
Phone +8 52 25 20 26 08
Fax +8 52 25 29 26 18
E-Mail: info@utimaco-asia.com