

# SOPHOS

## SafeGuard® Enterprise 5.50

### User help

Document date: August 2010



# Content

1	SafeGuard Enterprise on endpoint computers .....	2
2	Power-on Authentication .....	3
3	Power-on Authentication under Windows Vista.....	22
4	Logging on to Windows Vista.....	33
5	Logging on with the Lenovo Fingerprint Reader .....	35
6	Recovery options.....	44
7	Recovery via Local Self Help.....	45
8	Recovery via Challenge/Response.....	56
9	System Tray Icon and tool tips.....	66
10	SafeGuard Explorer extensions .....	68
11	Data Encryption .....	70
12	SafeGuard Data Exchange.....	76
13	SafeGuard Configuration Protection .....	92
14	SafeGuard Enterprise and BitLocker.....	93
15	SafeGuard Enterprise and Lenovo Rescue and Recovery .....	96
16	Technical support.....	103
17	Copyright .....	104

# 1 SafeGuard Enterprise on endpoint computers

SafeGuard Enterprise is a modular security suite that enforces security for PCs and mobile device on a cross-platform basis, using administrator-defined policies. SafeGuard Enterprise is easy to use. System administration is performed centrally via the SafeGuard Management Center.

The central protection functions of SafeGuard Enterprise on a endpoint computer are data encryption and protection against unauthorized access to a computer via external media.

## 1.1 SafeGuard Enterprise modules

### ■ SafeGuard Enterprise Device Encryption

- Power-on Authentication
- Logon is performed immediately after you switch on the computer. After successful Power-on Authentication (POA), you are automatically logged on to the operating system. You can also deactivate POA. In this case, authentication is performed via the operating system.
- Volume-based encryption
- BitLocker support

### ■ SafeGuard Data Exchange

- Easy data exchange with removable media on all platforms without re-encryption.
- File-based encryption
- All mobile writable media, including external hard disks and USB sticks, are encrypted transparently.

### ■ SafeGuard Configuration Protection

Using SafeGuard Configuration Protection you can allow only certain interfaces or peripheral devices on selected computers. This prevents malware from being introduced, as well as data exports via unwanted channels such as WLAN. This module can also detect and block harmful hardware such as key loggers.

**Note:** Please note that the features available on your computer depend on the settings defined in the SafeGuard Management Center. The security officer specifies these settings centrally in the SafeGuard Management Center via policies, and distributes them to the endpoint computers. Therefore, some features described in this manual may not be available on your computer.

## 2 Power-on Authentication

With Power-on Authentication (POA) users are required to authenticate during the pre-boot phase; that is, before the computer's operating system is started. Only when the user has been properly authenticated in the POA, the actual operating system (Windows) is started and the user logged on automatically to Windows. The procedure is the same when the computer is switched back on from hibernation (Suspend to Disk).



### 2.1 POA look and feel

The look and feel of the POA can be customized according to your company's requirements. Your SafeGuard Enterprise security officer performs the relevant adjustments via the policy settings in the SafeGuard Management Center.

The following adjustments are possible:

- **Logon image**

The default logon image that is displayed in the POA is a SafeGuard design. This screen is customizable via policy, enabling you to show a graphic, such as your company logo.

- **Dialog text**

All text in the POA is displayed in the default language that is set in the Windows Regional and Language Options on the endpoint computer when installing SafeGuard Enterprise.

You can set the default language via **Start > Settings > Control Panel > Regional and Language Options > Advanced**. If this default setting is, for example, "German", all dialog text in the POA will be displayed in German.

## 2.2 First logon after SafeGuard Enterprise installation

If SafeGuard Enterprise has been installed with Power-on Authentication (POA), the boot procedure is different during the first system start after the installation of SafeGuard Enterprise on a computer. A number of new start messages (for example, the autologon screen) are displayed because SafeGuard Enterprise has been incorporated in the boot procedure. Afterwards, the Windows operating system starts.

SafeGuard Enterprise uses certificate-based credentials to log on. Users need keys and certificates to successfully log on at the POA. However, user-specific keys and certificates are only created after a successful Windows logon. Only users who have successfully logged on to Windows on a system that has been able to communicate with the SGN server can also be authenticated in the POA.

When logging on for the first time after installation, you first have to successfully log on to Windows as usual. Afterwards you will be registered as a SafeGuard Enterprise user. This registration process is required to make sure that your credentials are recognized in the POA the next time the system is started.

**Note:** After successful registration and receipt of all required data, a tool tip confirming this is shown on your computer.

When you restart the computer, the POA is activated. From now on, you enter your Windows credentials at the POA. You are then logged on to Windows automatically without any further password entry (if automatic logon to Windows is activated).

You can log on at the Power-on Authentication via:

- user name and password
- token/smartcard and PIN

See the readme for the most up-to-date supported devices.

**Note:** The settings for the endpoint computers on which SafeGuard Enterprise is installed are defined by the security officer in the SafeGuard Management Center, and distributed to the users via policy files.

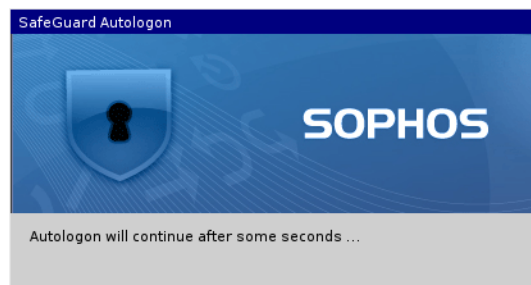
### 2.2.1 First logon procedure

The procedure for the first logon will only correspond to the one described here if POA has been installed and activated for your computer.

Depending on your system configuration, you may be prompted to press **Ctrl+Alt+Del**. The logon procedure will then continue.

### 2.2.2 SafeGuard Autologon

The computer starts and the SafeGuard Enterprise Autologon is displayed.



#### What happens?

1. An autouser is logged on.
2. The computer is automatically registered on the SafeGuard Enterprise Server, provided that a connection to the SafeGuard Enterprise Server exists.
3. The machine key is sent to the SafeGuard Enterprise Server and stored in the SafeGuard Enterprise database.
4. Machine policies are sent to the computer.

### 2.2.3 Windows logon

The Windows logon dialog is displayed.

Enter your Windows user credentials as usual.

**Note:** If you are using a **smartcard** or a **token**, enter the PIN.

### What happens?

1. A user ID and a hash of the user's credentials are sent to the server.
2. User policies, certificates, and keys are created and sent to the endpoint computer.

The user data will only be available at the Power-on Authentication after all user data noted above has been successfully synchronized between the SafeGuard Enterprise Server and the endpoint computer.

**Note:** After successful registration and receipt of all required data, a tool tip confirming this process is shown on your computer.

This means that, the next time the system is started, you only have to enter your Windows credentials (user name and password) at the Power-on Authentication, and you will be logged on automatically.

Restarting the system is necessary to activate Power-on Authentication to its full extent. After the restart, Power-on Authentication protects your computer against unauthorized access.

## 2.2.4 Power-on Authentication logon after restart

After restarting the computer the Power-on Authentication logon dialog is displayed.



Enter your user name and password.

### What happens?

1. Your credentials are evaluated. Certificates and keys are made available, and you are automatically logged on to Windows.

Logon pass-through to Windows may be deactivated by a policy setting. In this case, the Windows logon dialog is displayed, and you have to enter your credentials.

## 2.3 Logging on at the Power-on Authentication

After successful activation of the Power-on Authentication, you log on by entering your Windows user credentials in the logon dialog of the Power-on Authentication. You will be logged on to Windows automatically.

**Note:** You can deactivate the automatic logon to Windows by pressing the **Options >>** button in the logon dialog and deactivating **Pass through Logon to Windows**.

**Note:** Deactivating the automatic logon is, for example, necessary to enable other users to use Power-on Authentication on the relevant computer (see [Importing further users](#), page 8).

### 2.3.1 Logon delay on failed logon attempt

If logon at the Power-on Authentication fails, for example, due to an incorrect password, an error message is displayed, and a delay is imposed for the next logon attempt. The delay period is increased with each failed logon attempt. Failed attempts are logged.

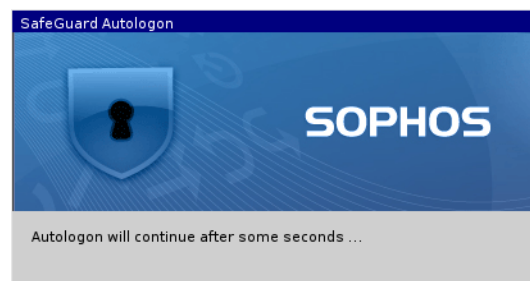
### 2.3.2 Machine lock

Depending on the policy settings, your computer may be locked after a set number of failed logon attempts. To unlock your computer, initiate a Challenge/Response procedure, see [Recovery via Challenge/Response](#), page 56.

### 2.3.3 POA user logon example

1. User 1 (Alice) switches on the XP client.

The POA Autologon dialog is displayed.



2. The Windows logon dialog is then displayed. Alice logs on to Windows.

Alice is now the so-called "owner". There is one owner per PC. By default, the first user to log on is the owner.

3. If the user's policies, certificate, and key are all on the client, an entry for Alice is created in the SafeGuard Enterprise system core.
4. Once the computer has restarted, Alice can log on at the POA.



**Note:** If the default setting applies, the first user to log on to Windows is automatically registered as the "owner" of this computer. Depending on the policy, only the owner of a computer can enable other users to log on at the Power-on Authentication. In our example, only Alice can log on at the Power-on Authentication!

**Note:** If other users intend to log on at the POA, the computer's owner has to enable it (see [Importing further users](#), page 8).

**Note:** The security officer defines in the relevant policies whether logon pass-through to Windows is activated or deactivated, and whether you are allowed to change this setting in the logon dialog.

## 2.4 Importing further users

Another Windows user (Bob) wants to log on to the computer, in addition to Alice.

1. Bob switches on the computer, and the POA is displayed.

Bob cannot log on at the POA because he does not have the necessary keys and certificates.

2. For Bob to log on at the POA, the computer's owner (Alice) must allow it.

The default setting specifies that the first user to log on after installation is registered as the owner of the computer.

**Note:** The security officer can also define the owner of a computer via a policy setting.

3. Before Alice logs on at the POA, she deactivates **Pass through logon to Windows**.



The Windows logon dialog is displayed, prompting Bob to log on.

4. Bob enters his Windows credentials.

5. If Bob's user policies, certificate, and key are all available on the computer (evident from the relevant balloon tool tip), an entry for Bob is created in the SafeGuard Enterprise system core.

The next time the computer is started, Bob can log on at the Power-on Authentication.

**Note:** If users have already logged on via POA on another machine in the environment, a security officer can use the Management Center to assign users to the POA on a new machine. Users assigned in this way can then also log on at the Power-on Authentication on these computers.

## 2.5 Temporary password in POA

SafeGuard Enterprise allows you to change the password temporarily in the POA. Changing the password in the POA temporarily is recommended if you suspect that somebody has watched you entering your password.

**Example:** You boot your notebook in a public place, e.g. at the airport. You think that somebody watched you entering your password at the POA. Since you are not connected to Active Directory (AD), you cannot change your Windows password.

**Solution:** You temporarily change your POA password, thereby ensuring that no unauthorized person knows your password. As soon as you are connected to AD again, you will be automatically prompted to change the temporary password.

To change your password in the POA temporarily:

1. In the POA logon dialog, enter the existing password.
2. Press **F8**.

If you do not enter the existing password prior to pressing **F8**, the system interprets this as a failed logon, and an error message is displayed.

3. In the dialog, enter the new password and confirm it.

The system reminds you that the password change is only temporary.

4. Click **OK**.

If you cancel this dialog, you will be logged on with your old password.

The Windows logon dialog is displayed.

**Note:** Logon will not be passed through to Windows, even if your system is configured that way. Enter the “old password“ here. The temporary password is only valid for logging on at the POA.

5. Click **OK**.

You are logged on to Windows.

For logging on at the POA, you can now only use the temporarily defined password. The temporary password is valid until the password is changed at the Windows logon. Only after doing that, logon can be passed through from POA to Windows again.

### **Changing the temporary password**

The password changed temporarily in the POA has to be changed later to make passwords synchronous again.

When logging on to Windows, SafeGuard Enterprise prompts you automatically to change your password as soon as you are connected to Active Directory again.

The dialog prompting you to change the password can be cancelled without actually changing the password. In this case, the dialog is shown each time you log on until you change the password.

**Note:** The POA password can also be changed temporarily while you are connected to Active Directory. In this case, the dialog for changing the password is shown immediately after changing the password temporarily in the POA. However, it can be cancelled and the "old password" can be used for logging on. You can change the password later.

## 2.6 Logging on at the Power-on Authentication using smartcards or tokens

There are two possible types of logon using smartcards or tokens:

- Logging on is *only allowed using smartcards or tokens*.
- Logging on is allowed *either via user name and password or via smartcard or token*.

The security officer defines the allowed logon type centrally via a policy.

Your security officer will issue your smartcard/token and provide it to you, or you deposit your Windows user credentials on your smartcard/token yourself.

**Note:** From SafeGuard Enterprise's perspective, smartcards and tokens are treated in the same way. So the terms "token" and "smartcard" can be understood as the same thing in the product and in the manual.

**Note:** The following sections use the term "token."

### 2.6.1 First token logon after installation

The first logon using a token is identical to the procedure described for logging on without a token.

If an issued token is available, you can use it to log on to Windows by entering the token PIN.

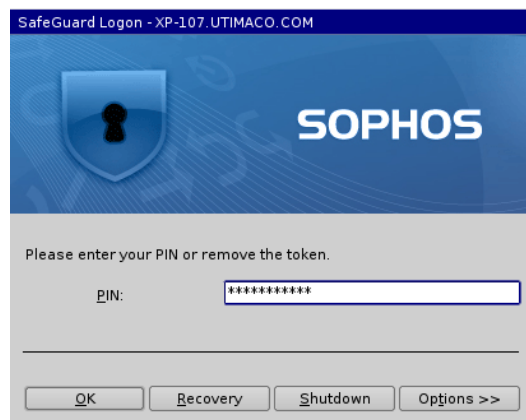
**Note:** It is recommended that you configure your token with Windows credentials (see [Storing Windows user information on your token](#), page 13) before the computer is restarted. The security policies that apply to you may require using a token at POA. If your token does not contain any user information, you will be unable to log on at the Power-on Authentication.

## 2.6.2 POA logon with token

Ensure that USB support is activated in the BIOS. Token support has to be initialized, and the token has to be issued for you.

How to log on at the Power-on Authentication using a token:

1. Plug in the token.
2. Switch on the computer and wait until the dialog for token logon is displayed.



**Note:** If your policy allows you to log on with your user credentials and you disconnect the token, you will be prompted to enter your user credentials for logging on. If the dialog for logging on with a user ID and password does not appear, you can only log on using a token at the Power-on Authentication.

3. Enter your token PIN.

You are logged on at the Power-on Authentication and to Windows (if option **Pass through logon to Windows** is activated in the logon dialog).

## 2.6.3 Changing the PIN

You can change the PIN of your token when the Windows logon dialog is displayed.

If **Pass through Logon to Windows** is activated at the Power-on Authentication (POA), the Windows logon dialog is usually not displayed. To display the Windows logon dialog, you have to deactivate this option during POA logon.

**Note:** You are automatically prompted to change the PIN if the security officer has defined rules requiring a change of PIN (for example, in specific time intervals).

How to change the token PIN:

1. In the PIN dialog used for logging on to Windows, activate **Change PIN**.



2. Enter your token PIN and click **OK**.

The PIN Change dialog is displayed.



3. Enter the new PIN and confirm it.
4. Click **OK**.

The token PIN is changed and Windows logon continues.

## 2.6.4 Storing Windows user information on your token

If no Windows user information has been stored on your token, you can deposit it on the token yourself.

**Note:** It is recommended that you configure your token during the first logon.

**Note:** The security policies that apply to you may require using a token at POA. If your token does not contain any user information, you will not be able to log on at the Power-on Authentication.

1. During the first logon after installation, connect your token with the system when the Windows logon dialog is displayed.
2. If the system detects an empty token, it automatically displays the dialog for issuing tokens.



3. Enter your Windows user name and password.
4. Confirm your password.
5. Select or enter the domain, and click **OK**.

The system tries to log you on to Windows using the data entered. If logon is successful, the data is written to the token.

You are logged on to Windows.

If token logon is defined as optional for your user (you have already logged on once at the POA with your user name and password), you can also issue the token later.

To do so, deactivate **Pass through Logon to Windows (Options >> > Pass through Logon to Windows)** in the POA logon dialog. The Windows logon dialog is displayed, and you can store the data on the token as described above.

## 2.6.5 Unlocking smartcards or tokens

If you have entered your PIN incorrectly several times, your token will be locked. The security officer can configure SafeGuard Enterprise to display the dialog for unlocking a token:



To unlock the token, the security officer has to provide you with the administrator PIN defined for your token.

Do as follows:

1. Enter the administrator PIN.

2. Enter a new PIN and confirm it.

The PIN you enter is subject to the rules defined for PINs (for example, specific character combinations may be required, PINs already used may be banned from being used again, etc.).

3. Click **OK**.

The token is unlocked and logon continues.

**Note:** If this function is not available on your computer, you can regain access to your computer via Challenge/Response.

**Note:** Via Challenge/Response you can regain access to your computer. However, you cannot change the PIN or your user credentials via Challenge/Response.

## 2.6.6 Remote Desktop Connection

Under Windows XP it is not possible to establish a Remote Desktop Connection to a computer if the user has logged on locally using a token.

Remote capture is not possible in this case.

## 2.6.7 Cryptographic tokens - Kerberos

When using cryptographic tokens, authentication at the POA is done via the certificate stored on the token.

For this type of logon, you need a fully issued token for authentication. The security officer or any other authorized person has to provide this token. To log on to the system, you only have to enter the token PIN. If this type of logon is the only type valid for your computer, you cannot log on without the token.

**Note:** When using tokens of this type, the Challenge/Response procedure will not be available in case of logon problems. If logon problems occur, contact your security officer.

## 2.7 POA autologon with a smartcard or token

Ensure that USB support is activated in the BIOS. Token support has to be initialized, and the token has to be issued for you. The respective policy has been assigned to your computer.

If a respective policy with a defined default PIN has been assigned to your computer, this may enable you to automatically log on at the Power-on Authentication using a token. You do not have to enter any credentials or PIN at logon, but are passed through at the POA. A pass-through to Windows depends on your policy settings.

How to automatically log on at the Power-on Authentication using a token:

1. Plug in the token.
2. Switch on the computer.

You are automatically logged on at the Power-on Authentication. A pass-through to Windows depends on your policy settings.

- If the autologon has been successful, Windows is started.
- If the autologon has failed, you are prompted to enter your token PIN. You are then logged on at the Power-on Authentication.

## 2.8 Virtual keyboard

At the POA, you can show/hide a virtual keyboard on the screen, and click the on-screen keys to enter credentials, etc.

**Prerequisite:** The responsible security officer has activated the display of the virtual keyboard in the policy of the type **Specific Machine Settings**.

To show the virtual keyboard in the POA, click **Options >>** in the POA logon dialog, and select the **Virtual Keyboard** check box.



The virtual keyboard supports different layouts, and it is possible to change the layout using the same options for changing the POA keyboard layout (see [Changing the keyboard layout](#), page 18).

## 2.9 Keyboard layout

Almost every country has its own keyboard layout; that is, the keys are assigned differently. The keyboard layout in the POA is significant when entering user names, passwords, and response codes.

As the default, SafeGuard Enterprise adopts the keyboard layout in the POA which is set in Windows' Regional and Language Options for the Windows default user at the time SafeGuard Enterprise is installed. If "German" is the keyboard layout set under Windows, the German keyboard layout will be used in the POA.

The language of the keyboard layout being used is displayed in the POA, for example "EN" for English. Apart from the default keyboard layout, the US keyboard layout (English) can also be used.

### 2.9.1 Changing the keyboard layout

The Power-on Authentication keyboard layout (including the virtual keyboard layout) can be changed.

To change the language of your keyboard layout:

1. Select **Start > Control Panel > Regional and Language Options > Advanced**.
2. On the **Regional Options** tab, select the required language.
3. On the **Advanced** tab, under **Default user account settings**, activate **Apply all settings to the current user account and to the default user profile**.
4. Click **OK**.

The POA recognizes the keyboard layout used for the last successful logon and automatically enables it for the next logon. This requires two reboots of the endpoint computer. If the previous keyboard layout is deactivated via **Regional and Language Options**, it is still maintained unless you select a different one.

**Note:** Additionally, it is required to change the language of the keyboard layout for non-Unicode programs.

If the language you want is not available on your system, Windows may prompt you to install it. After you have done so, you need to reboot your computer twice so that, first, the new keyboard layout can be read in by the POA and, secondly, the POA can set the new layout.

You can change the required keyboard layout for the POA using the mouse or keyboard (**Alt+Shift**).

You can see which languages are installed and available on your system via **Start > Run > regedit:**  
HKEY\_USERS\.\DEFAULT\Keyboard Layout\Preload.

## 2.10 Supported hotkeys/function keys in the Power-on Authentication

Certain hardware functionality and settings can lead to problems when booting endpoint computers causing the system to hang. The Power-on Authentication supports a number of hotkeys for modifying these hardware settings and deactivating functionality. Furthermore, a grey list listing a number of hardware settings and functionalities that are known to cause these problems is integrated in the .msi file installed on the computer.

We recommend you install an updated version of the POA configuration file prior to any significant deployment of SafeGuard Enterprise. The file is updated on a monthly basis and made available to download from here: <ftp://POACFG:POACFG@ftp.ou.utimaco.de>

You can customize this file to reflect the hardware of a particular environment.

**Note:** When defining a customized file, only this will be used instead of the one integrated in the .msi file. Only when no POA configuration file is defined or found, the default file will be applied.

To install the POA configuration file, enter the following command:

```
MSIEXEC /i <Client MSI package> POACFG=<path of the POA configuration file>
```

For further information see the knowledgebase: <http://www.sophos.com/support/knowledgebase/article/65700.html>.

Furthermore, the Power-on Authentication supports a number of function keys.

### 2.10.1 Hotkeys

**Shift-F3** = USB Legacy Support (on/off)

**Shift-F4** = VESA graphic mode (off/on)

**Shift-F5** = USB 1.x and 2.0 support (off/on)

**Shift-F6** = ATA Controller (off/on)

**Shift-F7** = USB 2.0 support only (off/on) USB 1.x support remains as set by **Shift-F5**.

**Shift-F9** = ACPI/APIC (off/on)

**Hotkeys dependency matrix**

Shift-F3	Shift-F5	Shift-F7	Legacy	USB 1.x	USB 2.0	Comment
off	off	off	on	on	on	3.
on	off	off	off	on	on	Default
off	on	off	on	off	off	1., 2.
on	on	off	on	off	off	1., 2.
off	off	on	on	on	off	3.
on	off	on	off	on	off	
off	on	on	on	off	off	
on	on	on	on	off	off	2.

1. **Shift-F5** disables both USB 1.x and USB2.0.

**Note:** Pressing **Shift-F5** during boot time will considerably reduce the time it takes to launch the POA. However, if your computer uses a USB keyboard or USB mouse, they might be disabled when pressing **Shift-F5**.

**Note:** The POA may use the USB keyboard via BIOS SMM. No USB token support.

2. If no USB support is active, the POA tries to use BIOS SMM instead of backing up and restoring the USB controller. The Legacy mode may work in this scenario.
3. Legacy support is active, USB is active. The POA tries to back up and restore the USB controller. The system might hang depending on the BIOS version used.

**Note:** The changes that can be carried out using the hotkeys may already have been specified during SafeGuard Enterprise Client installation using an `.mst` file.

After changing hardware settings using the hotkeys in the POA, a dialog is displayed prompting you to save the changed settings. This dialog shows an overview of the configuration that will be saved. To save your changes, click **Yes**. After restarting your computer, the new settings become active. If you click **No**, your changes will not be saved, and the old configuration remains active after you restart your computer.

By pressing **F5** in any POA dialog, you can open a dialog showing the hotkeys configuration used to boot the POA. If hotkeys were changed during the boot process, the relevant key states will be shown in blue. Blue means that the key was used in this state to boot the POA, however, it has not been saved yet. Unchanged values will be shown in black. To close the dialog, press **F5** again or press **Return**.

## 2.10.2 Function keys in the logon dialog

**Note:** The function keys are not hotkeys.

**F2** = abort Autologon

**F5** = displays a dialog showing the hotkey configuration used to boot the POA.

**F8** = change password in POA. Use instead of the **Enter** key to trigger a password change in the POA after logging on.

**Alt+Shift** (left-hand **Alt** and left-hand **Shift** keys) = change keyboard from German to English (or the reverse)

### **Cancel and prepare POA for shutdown**

**Ctrl+Alt+Del** = if authentication has failed but you need to shut down the PC safely. This key combination has the same function as the **Shutdown** button.

**Note:** If fingerprint logon is activated, you can use **Ctrl+Alt+Del** in the POA dialog for logging on with a fingerprint to change to the POA dialog to support logon with a user name and password. For further information on fingerprint logon, see [Logging on with the Lenovo Fingerprint Reader](#), page 35.

## 2.11 Password synchronization

SafeGuard Enterprise automatically detects when the Windows password has been changed and no longer corresponds to the one stored in the SafeGuard Enterprise database. This may arise if the Windows password has been changed via a VPN, on another computer, or in Active Directory.

If SafeGuard Enterprise detects this situation, you are prompted to enter the old password. Afterwards, the password stored by SafeGuard Enterprise is updated with the new Windows password.

Password synchronization will take place in two situations:

- During logon
- During a Windows lock/unlock procedure.

## 3 Power-on Authentication under Windows Vista

The Power-on Authentication for Windows Vista has the same look and feel and behavior as that of Windows XP. (see [Power-on Authentication](#), page 3). Differences only occur when logging on to the operating system itself. Windows Vista has several authentication methods for user logon in parallel.

**Note:** This section only describes the differences regarding Windows Vista. If differences are not explicitly stated, the procedures/processes described in the earlier Power-on Authentication section also apply to Vista.

### 3.1 First logon after SafeGuard Enterprise installation under Windows Vista

If SafeGuard Enterprise has been installed with Power-on Authentication, the boot procedure is different on the first system start after the installation of SafeGuard Enterprise on your computer. A number of new start messages (for example, the autologon screen) are displayed because SafeGuard Enterprise has been incorporated into the boot procedure. Afterwards, the Windows operating system will start.

**Note:** Under Windows Vista, you first have to press **Ctrl+Alt+Del** to start autologon and logon. The administrator can deactivate this setting in the MMC console in the group policy object editor under **Windows Settings > Security Settings > Local Policies > Deactivate Security Options** (Interactive logon: **Ctrl+Alt+Del** not required).

**Note:** SafeGuard Enterprise uses certificate-based logon. So you need keys and certificates to successfully log on at the POA. However, user-specific keys and certificates are only created after a successful Windows logon; that is, only if you have successfully logged on to Windows can you also be authenticated at the POA.

When logging on for the first time after installation, you therefore have to log on successfully at Windows as usual using your credentials. Afterwards, you are registered as a SafeGuard Enterprise user. This registration process is required to make sure that your credentials are recognized in the POA the next time the system is started.

After successful registration and receipt of all required data, a tool tip informing you of this is shown on your computer.

When you restart the computer, the POA is activated. From now on, you enter your Windows credentials at the POA. You are then logged on to Windows automatically without any further password entry (if automatic logon to Windows is activated).

You can log on at the POA via user name and password.

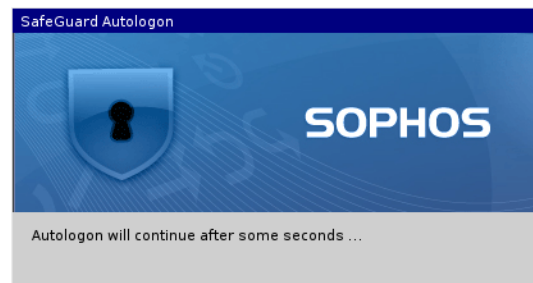
**Note:** The settings for the user PCs on which SafeGuard Enterprise is installed are defined centrally by the security officer in the SafeGuard Management Center and distributed to the endpoint computers via policy files.

### 3.1.1 First logon procedure

This section describes the procedure of the first logon to your computer after SafeGuard Enterprise has been installed. The procedure of the first logon will only correspond to the one described here if POA has been installed and activated for your computer.

### 3.1.2 SafeGuard Autologon

1. The client starts, and the SafeGuard Enterprise Autologon dialog is displayed.



- An autouser is logged on.
- The computer is automatically registered on the SafeGuard Enterprise server, provided that a connection to the SafeGuard Enterprise Server exists.
- The machine key is sent to the SafeGuard Enterprise Server and stored in the SafeGuard Enterprise database.
- Machine policies are sent to the computer.

### 3.1.3 Windows Vista logon

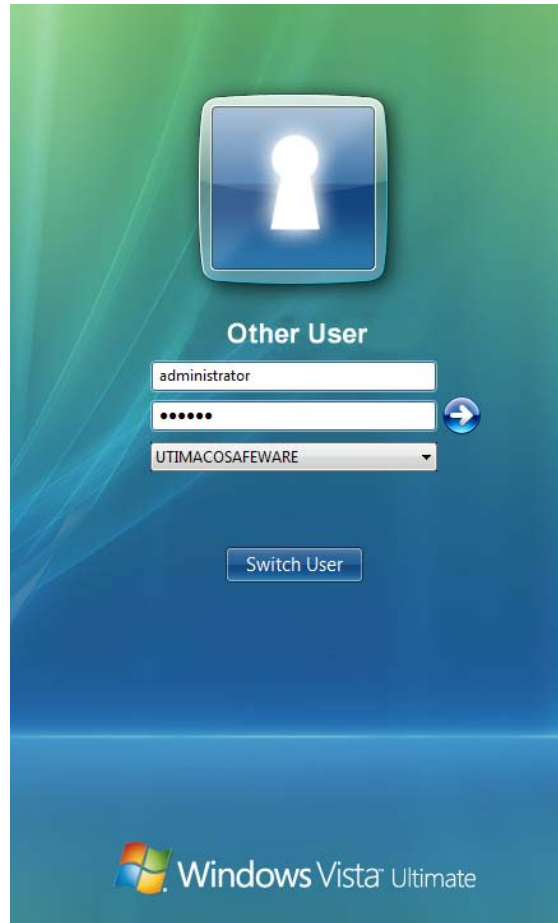
1. The Windows Vista logon dialog is displayed.



Under Windows Vista, SafeGuard Enterprise offers an additional authentication method. The example shows the SafeGuard Enterprise authentication method, and the icons for the Vista authentication method.

2. Windows Vista provides two icons for each authentication method:
  - By clicking **Other User**, you open a dialog for entering credentials.
  - By clicking on the second icon (a user name is already displayed below the icon), you open a dialog that contains the user information of the last user who has logged on to the system. You only have to enter the password.

If your user name is displayed below a SafeGuard Enterprise icon, select the relevant icon. If this is not the case, select the SafeGuard Enterprise icon **Other User**.



3. Enter your Windows user credentials as usual.
  - User ID and a hash of the user's credentials are sent to the server.
  - User policies, certificates, and keys are created and sent to the client.

The user data is only available in the Power-on Authentication after all data has been successfully synchronized between the Server and your computer.

This means that **the next time the system is started** you only have to enter your Windows user credentials (user name and password) in the POA and you are logged on automatically.

Restarting the system is necessary to activate Power-on Authentication to its full extent. After the restart, POA protects your computer against unauthorized access.

### 3.1.4 Power-on Authentication logon after restart

1. After restarting the computer, the Power-on Authentication logon dialog is displayed.



Certificates and keys are available, and you can log on at the POA using your Windows credentials.

2. Enter your user name and password, and click **OK**.

Your credentials are evaluated. After the system has verified your credentials, you are automatically logged on to Windows.

**Note:** Logon pass-through to Windows may be deactivated by a policy setting. In this case, the Windows logon dialog is displayed, and you have to enter your credentials.

## 3.2 Logging on at the Power-on Authentication under Windows Vista

After successful activation of the Power-on Authentication (initial synchronization and restart), you log on by entering your Windows user credentials in the logon dialog of the Power-on Authentication. You will be logged on to Windows automatically.

**Note:** You can deactivate automatic logon to Windows by pressing the **Options >>** button in the logon dialog and deactivating **Pass through Logon to Windows**. Deactivating the automatic logon is, for example, necessary to enable other users to use Power-on Authentication on the relevant computer. The security officer defines, in the relevant policies, whether logon pass-through to Windows is activated or deactivated and whether you are allowed to change this setting in the logon dialog.

### 3.2.1 Logon delay on failed logon attempt

If logon at the Power-on Authentication fails, for example, due to an incorrect password, an error message is displayed, and a delay is imposed for the next logon attempt. The delay period is increased with each failed logon attempt. Failed attempts are logged.

### 3.2.2 Machine lock

Depending on the policy settings, your computer may be locked after a set number of failed logon attempts. For unlocking your computer, initiate a Challenge/Response procedure, see [Recovery via Challenge/Response](#), page 56.

## 3.3 Logging on at the Power-on Authentication using smartcards or tokens under Windows Vista

There are two different possible types of logon using smartcards or tokens:

- Logging on is *only allowed using smartcards or tokens*.
- Logging on is allowed *either via user name and password or via smartcard or token*.

The security officer defines the allowed logon type centrally via a policy.

Your security officer will issue your smartcard/token and provide it to you, or you deposit your Windows user credentials on your smartcard/token yourself.

**Note:** From SafeGuard Enterprise's perspective, smartcards and tokens are treated in the same way. So the terms "token" and "smartcard" can be understood as the same thing in the product and in the manual.

**Note:** In the following sections we use the term token.

### 3.3.1 First token logon after installation

The first logon using a token is identical to the procedure described for logging on without a token.

If an issued token is available at this point, you can use it to log on to Windows by entering the token PIN.

**Note:** It is recommended that you configure your token with Windows credentials (see [Storing Windows user information on your token](#), page 30) before the computer is restarted.

**Note:** The security policies that apply to you may require using a token at POA. If your token does not contain any user information, you will be unable to log on at the Power-on Authentication.

### 3.3.2 Power-on Authentication logon with token

**Prerequisite:** Ensure that USB support is activated in the BIOS. Token support has to be initialized, and the token has to be issued for you.

How to log on at the Power-on Authentication (POA) using a token:

1. Plug in the token.
2. Switch on the computer, and wait until the dialog for token logon is displayed.



**Note:** If your policy allows you to log on with your user credentials and you disconnect the token, you are prompted to enter your user credentials for logging on. If the dialog for logging on using user ID and password is not displayed, you can only log on using a token at the POA.

3. Enter your token PIN.

You are logged on at the POA and to Windows (if the "Pass through Logon to Windows" option is activated in the logon dialog).

### 3.3.3 Changing the PIN

You can change the PIN of your token when the Windows logon dialog is displayed.

If **Pass through Logon to Windows** is activated at the Power-on Authentication (POA), the Windows logon dialog is usually not displayed. To open the Windows logon dialog, for example, to change the PIN, you have to deactivate this option during POA logon.

You are automatically prompted to change the PIN if the security officer has defined rules requiring a change of PIN (for example in specific time intervals).

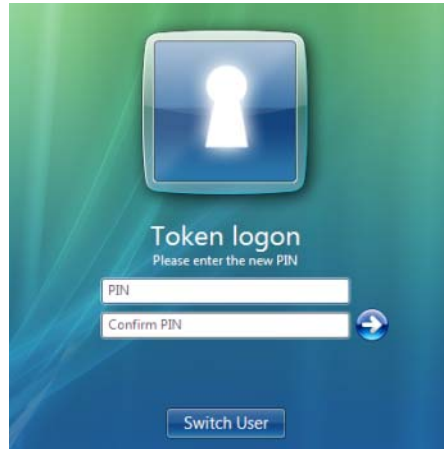
How to change the token PIN:

1. In the PIN dialog displayed for logging on to Windows, select **Change PIN**.



2. Enter your token PIN and click **OK**.

The PIN Change dialog is displayed.



3. Enter the new PIN and confirm it.
4. Click **OK**.

The token PIN is changed and Windows logon continues.

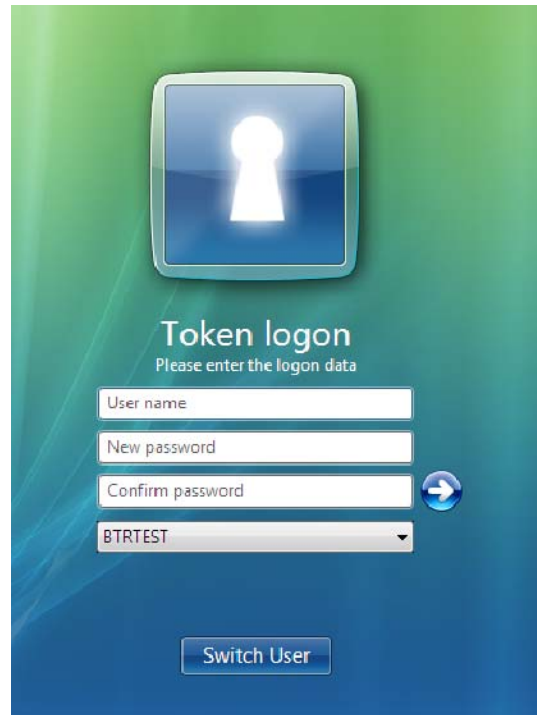
### 3.3.4 Storing Windows user information on your token

If no Windows user information has been stored on your token, you can deposit it on the token yourself.

**Note:** It is recommended that you configure your token at first logon. The security policies that apply to you may require using a token at POA. If your token does not contain any user information, you are not able to log on at the Power-on Authentication.

1. During the first logon after installation, connect your token with the system when the Windows logon dialog box is displayed.

If the system detects an empty token, it automatically displays the dialog for issuing tokens.



2. Enter your Windows user name and password.
3. Confirm your password.
4. Select or enter the domain, and click **OK**.

The system tries to log you on to Windows using the data entered. If logon is successful, the data is written to the token.

You are logged on to Windows.

If token logon is defined as optional for your user (you have already logged on once at the POA with your user name and password), you can also issue the token later.

To do so, deactivate (**Options > Pass through Logon to Windows**) in the Power-on Authentication logon dialog box. The Windows logon dialog is displayed, and you can store the data on the token as described above.

### 3.3.5 Unlocking smartcards or tokens under Windows Vista

Your token will be locked if you have entered your PIN incorrectly several times. The security officer can configure SafeGuard Enterprise to display the dialog box for unlocking a token:



To unlock the token, the security officer has to provide you with the administrator PIN defined for your token.

To unlock a token:

1. Enter the administrator PIN.
2. Enter a new PIN and confirm it.

The PIN you enter is subject to the rules defined for PINs (for example, specific character combinations may be required, PINs already used may be banned from being used again, etc.).

3. Click **OK**.

The token is unlocked and logon continues.

If this function is not available on your computer, you can regain access to your computer via Challenge/Response.

**Note:** Although you can regain access to your computer via Challenge/Response, it does not permit you to change the PIN or your user credentials.

## 4 Logging on to Windows Vista

Under Windows Vista, SafeGuard Enterprise offers an additional authentication method.

If you deactivate **Pass through Logon to Windows** in the logon dialog of the Power-on Authentication, the Windows Vista logon dialog is displayed. In this dialog, you can also select a different authentication method.

**Note:** Using a different authentication method does not mean that SafeGuard Enterprise is inactive on your computer. In this case, the logon at SafeGuard Enterprise is not done during the Windows logon but after the Windows Vista logon.

### 4.1 Logging on via SafeGuard Enterprise

Usually, you are automatically logged on to Windows after entering your password at the Power-on Authentication (POA). If you deactivate **Pass through Logon to Windows** in the POA logon dialog, and use the SafeGuard Enterprise method for logging on to Windows, SafeGuard Enterprise is available with its complete scope of functionality after logging on to Windows Vista.

The required keys are available, and all data is encrypted and decrypted according to the policies defined.

### 4.2 Logging on via an alternative authentication method

In the Windows logon dialog, you can also select an alternative authentication method for logging on to Windows instead of the SafeGuard Enterprise authentication method.

If you use an alternative method for logging on to the operating system, the logon to SafeGuard Enterprise is performed after the logon to the operating system.

After logging on to Windows Vista, the SafeGuard Enterprise authentication application is started automatically.

Depending on the logon settings in central administration, either a dialog for entering user credentials or a PIN entry dialog is displayed.

1. Enter your credentials or the PIN, and click **OK**.

Now the SafeGuard Enterprise functionality is available and you can, for example, access encrypted data, if you have the necessary key.

## 4.3 Password synchronization under Windows Vista

SafeGuard Enterprise automatically detects when the Windows password has been changed and no longer corresponds to the stored one. This may arise if the Windows password has been changed via a VPN, on another computer, or in Active Directory.

If SafeGuard Enterprise detects this situation, you are informed and prompted to enter the old password. Afterwards, the password stored by SafeGuard Enterprise is updated with the new Windows password.

Password synchronization takes place in two situations:

- During logon
- During a Windows lock/unlock procedure.

## 5 Logging on with the Lenovo Fingerprint Reader

Users must remember many different passwords and PINs in order to access their computers, applications, and networks. With a fingerprint reader, all you need to do is swipe your finger over the reader to log on instead of using a password or token.

Furthermore, you cannot lose or forget your credentials, nor can any unauthorized individuals guess this information. Using fingerprint readers thus simplifies the logon process and increases security.

SafeGuard Enterprise supports fingerprint logon for Power-on Authentication as well as the Windows logon phase. For example, you can log on to a Lenovo notebook simply by swiping your finger over the fingerprint reader integrated into the notebook. The rest of the logon procedure then runs automatically. You can also lock and unlock your desktop in Windows by swiping your finger over the fingerprint reader.

Fingerprint readers are integrated directly into certain Lenovo notebooks. However, you can also use an external USB keyboard for a fingerprint logon.

- Only one fingerprint reader may be connected to a computer at any given time.
- Token and fingerprint logon procedures cannot be combined on the same computer.
- Remote fingerprint logon is not supported.

## 5.1 Requirements

The following requirements must be satisfied in order to use a fingerprint logon:

### 5.1.1 General requirements

- Lenovo hardware
- Lenovo Fingerprint Reader in the notebook or a USB keyboard with a fingerprint reader
- The latest BIOS is recommended
- SafeGuard Enterprise, Version 5.35 or later
- The recommended vendor-specific software version must be installed before SafeGuard Enterprise:
  - ThinkVantage Fingerprint for AuthenTecor
  - ThinkVantage Fingerprint for UPEK
- The security officer must have set up the fingerprint option in the relevant **Authentication** policy.

### 5.1.2 System requirements

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

### 5.1.3 Supported hardware

- AuthenTec AES2810
- UPEK TCS3C/TCD42A

### 5.1.4 Supported software

- Lenovo Fingerprint for AuthenTec Version 3.2.0.166
- ThinkVantage Fingerprint for UPEK Version 5.8.5.6014

## 5.2 Enrolling fingerprints

In order to log on to your notebook/PC with a fingerprint, you must first enroll one or more fingerprints using the recommended vendor-specific software. The enrollment process links your enrolled finger with your credentials (user name and password).

**Prerequisites:** The following procedure assumes that both the recommended vendor-specific software and SafeGuard Enterprise are installed.

To enroll your fingerprints:

1. Log on at the Power-on Authentication (POA) by entering your user name and password.
2. Register one or more of your fingerprints by using the installed vendor-specific software. This registration links your fingerprint with your Windows credentials.
  - a) Refer to the documentation for the ThinkVantage Fingerprint software for instructions on how to enroll a fingerprint.
  - b) Enable the option **POA password in BIOS** (UPEK only. For AuthenTec this step is not necessary).
  - c) To use fingerprint logon in the POA, you first have to log on to Windows once with your fingerprint to transfer your credentials to the fingerprint reader. For UPEK you only have to swipe an enrolled fingerprint over the fingerprint reader. For AuthenTec you also have to enter your Windows password at first logon.
3. Reboot your PC/notebook.
4. To test your enrolled fingerprint, swipe your finger over the fingerprint reader after rebooting the computer.

If your fingerprint matches the enrolled one, you are automatically logged on to Windows.

## 5.3 Logging on to Power-on Authentication with a fingerprint

**Prerequisites:**

- The security officer must have set up the fingerprint option in the relevant **Authentication** policy.
- You must have enrolled one or more fingerprints.

1. Reboot your PC/notebook.

The POA dialog for logging on with a fingerprint is displayed.



2. Swipe one of your enrolled fingers over the reader.

If the software successfully recognizes your fingerprint, Power-on Authentication reads your credentials and sends them to Windows.

**Note:** The logon procedure uses icons with short text messages as prompts, notifications, and warnings (see [Icons used in the logon process](#), page 39).

You are automatically logged on to Windows without any further requests for your data.

- If the enrollment process in Windows was not completed successfully (for example, after enrolling fingerprints, you have not logged off from and logged on again to Windows) a match with the fingerprints enrolled will be found in the POA.

However, there will not be any credentials. In this case, an error message is displayed, prompting you to log on with your user name and password, however, without pass-through to Windows. Your credentials are transferred to the fingerprint reader.

- In the policies that apply to you, the security officer specifies whether pass-through to Windows has been enabled or disabled and whether you can change these settings in the POA dialog for logging on with a user name and password (see [Logging on with a user name and password](#), page 41).

### 5.3.1 Icons used in the logon process

When you log on at the Power-on Authentication with a fingerprint, the system uses icons as prompts, notifications, and warnings. These icons are displayed during the logon process, along with a short text message.



Prompts you to swipe your finger over the fingerprint reader.



Indicates that fingerprint logon is not currently enabled. This can occur, for example, if the fingerprint logon module has not yet been initialized.



Indicates that the fingerprint reader is working and is busy.



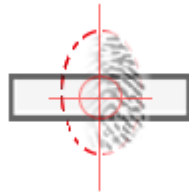
Indicates that the fingerprint was read successfully and a match was found.



Indicates that the fingerprint was read successfully, however, no match was found.



Indicates that the fingerprint could not be read. Swipe your finger across the fingerprint reader again.



Indicates that you have placed your finger too far to the left (or too far to the right). Move your finger to the center of the fingerprint reader.



Indicates that your finger swipe was too skewed. Swipe your finger across the fingerprint reader again.



Indicates that you moved your finger too fast. Swipe your finger across the fingerprint reader again.



Indicates that your finger swipe was too short. Swipe your finger across the fingerprint reader again.

### 5.3.2 Failed logon attempts

If the system is unable to read your fingerprint after five attempts, it considers this to be a failed logon attempt and logs it as an event. In this case, a logon delay goes into effect.

If the system was able to read your fingerprint without errors, but did not find a match with the registered fingerprint after five attempts, it also considers this to be a failed logon attempt and logs it as an event. In this case, a logon delay also goes into effect.

The logon delay period increases with every failed logon attempt.

### 5.3.3 Logging on with a user name and password

Even if fingerprint logon is enabled, you can still continue to log on at the Power-on Authentication with your user name and password, for example, if you cannot log on with a fingerprint because your fingerprint reader is defective.

To authenticate yourself by entering your user logon data:

1. Press the **Esc** key or **Ctrl+Alt+Del** in the POA dialog for logging on with a fingerprint.

The POA dialog for logging on with a user name and password is displayed.



**Note:** If you press **Ctrl+Alt+Del** in the POA dialog for logging on with a user name and password, the computer is shut down. In this dialog, **Ctrl+Alt+Del** corresponds to the **Shutdown** button.

The POA dialog for logging on with a user name and password also appears automatically if a fingerprint reader is unavailable or if the system does not find any user data on the fingerprint reader.

**Note:** Logging on with a user name and password is also enabled automatically if the local cache is corrupt. If this happens, your computer will be locked, and you must log on using a Challenge/Response procedure (see [Initiating a Challenge/Response procedure when logging on via fingerprint](#), page 43).

2. Optionally, press **Esc** again to return to the POA dialog for logging on with a fingerprint.

If you pressed Esc to switch to the POA dialog for logging on with a user name and password, you can still log on by swiping your finger over the fingerprint reader without having to first return to the POA dialog for logging on with a fingerprint.

## 5.4 Changing your password

1. If a fingerprint logon is enabled in Power-on Authentication, you can change your password in Windows via **Ctrl+Alt+Del**.

When you change your password, the system prompts you to swipe your finger over the fingerprint reader in order to transfer your new password to the fingerprint reader.

**Note:** Whenever you change your password, the change applies to all your enrolled fingerprints.

### 5.4.1 Synchronizing your password

If your Windows password no longer matches the password stored on the fingerprint reader, e.g., in cases where you changed your password, but the new password was not transferred to the fingerprint reader, you can synchronize your password by following the steps below:

1. Reboot your computer.
2. Press the **Esc** key or **Ctrl+Alt+Del** in the POA dialog for logging on with a fingerprint in order to switch to the POA dialog for logging on with a user name and password.
3. Click **Options**, and disable **Pass-through to Windows**.  
In the policies that apply to you, the security officer specifies whether pass-through to Windows has been enabled or disabled and whether you can change these settings in the POA dialog for logging on with a user name and password.
4. Log on with your password.
5. The Windows logon dialog is displayed. Swipe one of your enrolled fingers over the fingerprint reader.
6. The system recognizes the fingerprint, but Windows will nonetheless reject the password linked to the fingerprint. This is not viewed as a failed logon attempt, however, so no logon delay goes into effect.
7. Instead, a message indicating that the password was changed is displayed, and the system prompts you to enter your current Windows password. Enter the correct Windows password.  
If you enter an incorrect Windows password here, a failed logon attempt is logged, and a logon delay goes into effect. If you close the input prompt without entering a password, a failed logon attempt is likewise logged, and a logon delay goes into effect.

A successful transfer of the password completes the password synchronization process, and you can then use the password for your logon.

## 5.5 Initiating a Challenge/Response procedure when logging on via fingerprint

For logon recovery, you can carry out a Challenge/Response procedure. This may be necessary, for example, if the fingerprint logon does not work, and you forgot the password required to log on. The SafeGuard Enterprise Challenge/Response procedure provides a highly secure and efficient method for exchanging information confidentially.

To initiate a Challenge/Response procedure with the fingerprint logon enabled:

1. Press the **Esc** key in the dialog for logging on with a fingerprint.

The dialog for logging on with a user name and password is displayed.

2. Click **Recovery** to start the Challenge/Response procedure.

Due to a Challenge/Response procedure, you may be offered to change your password when booting your computer, for example, to enable recovery in case of a forgotten password. In this case, the system will also offer to update your fingerprint credentials.

For a detailed description of the Challenge/Response procedure, see [Recovery via Challenge/Response](#), page 56.

## 6 Recovery options

For recovery (for example, if you have forgotten your password), SafeGuard Enterprise offers different options that are tailored to different recovery scenarios:

### ■ Logon recovery via Local Self Help

If you have forgotten your password, Local Self Help enables you to log on to your computer without the assistance of a helpdesk. Even in situations where neither telephone nor network connections are available (for example aboard an aircraft), you can regain access to your computer. To log on, you simply answer a number of predefined questions in the Power-on Authentication.

For detailed information, see [Recovery via Local Self Help](#), page 45.

### ■ Recovery via Challenge/Response

The Challenge/Response mechanism is a secure and efficient recovery system that helps you if you cannot log on to your computer or access encrypted data. During the Challenge/Response procedure, you provide a challenge code generated on your computer to the help desk officer who in turn generates a response code that authorizes you to perform a specific action on the computer.

For detailed information, see [Recovery via Challenge/Response](#), page 56.

Both recovery options are enabled for use on your computer by the security officer via policies.

## 7 Recovery via Local Self Help

If you have forgotten your password and you cannot contact the help desk for assistance, SafeGuard Enterprise offers Local Self Help.

Using Local Self Help, you can regain access to your laptop in situations where neither telephone nor network connections are available, and you therefore cannot use a Challenge/Response procedure (for example, aboard an aircraft). You can log on to your computer by answering a specified number of predefined questions in the Power-on Authentication.

The responsible security officer can define the questions to be answered and distribute them to the endpoint computers. You can also define your own questions, if the relevant policy entitles you to do so. For providing the initial answers and editing the questions, SafeGuard Enterprise offers the Local Self Help Wizard. You can open the Local Self Help Wizard by clicking the SafeGuard Enterprise System Tray icon on the Windows taskbar.

### 7.1 Prerequisites

To use Local Self Help for logon recovery, the following prerequisites must be met:

- The security officer has enabled Local Self Help in the applying and effective policy of the type **General Settings** and has defined the settings for this function (e.g., the right to define your own questions).
- You have activated Local Self Help on your computer (see [Activating Local Self Help](#), page 45).

### 7.2 Activating Local Self Help

After the policy entitling you to use Local Self Help has become effective, you have to activate the function by answering the predefined questions received or by defining and answering your own questions.

Local Self Help only becomes active on your computer after you have answered and saved at least ten questions.

Depending on the policy settings, these are the following possible scenarios:

- **You have received predefined questions, and you are not entitled to define your own questions.**

Answer and save at least ten of the predefined questions received.

- **You have received predefined questions, and you are entitled to define your own questions.**

Answer and save at least ten questions (predefined questions, your own defined questions, or a combination of both).

- **You have not received predefined questions, and you are entitled to define your own questions.**

Define, answer, and save at least ten questions.

**Note:** To log on at the Power-on Authentication via Local Self Help, you have to answer five questions randomly selected from the ten questions answered.

**Prerequisite:** After receiving the policy, the tool tip indicates that there are unanswered Local Self Help questions. Restart your computer to add the **Local Self Help** command to the context menu of the System Tray icon on the Windows taskbar.

To activate Local Self Help:

1. Right-click the SafeGuard Enterprise System Tray icon on the Windows taskbar.
2. Select **Local Self Help**.

The Local Self Help Wizard Welcome dialog is displayed.

For security reasons, you are prompted to enter your password.

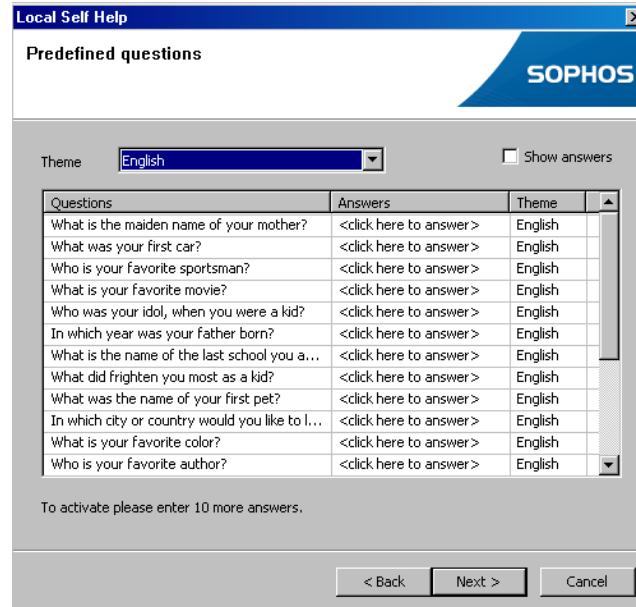
3. Enter your password, and click **Next**.

The Status Overview dialog is displayed.

This dialog offers a short instruction on how to activate Local Self Help. Furthermore, it displays status information (for example, the number of answered user-defined questions, the number of answered predefined questions, etc).

4. Click **Next**.

If you have received predefined questions with the effective policy, the Predefined questions dialog is displayed



- If you have received several different question themes, you can choose from the question themes displayed in the drop-down list of the **Theme** field.
- To display all themes in a continuous list, select the **All Themes** option (default) from the drop-down list.
- To answer the questions, click on the relevant question, and enter your answer in the **Answers** column.
- After you enter the answer, the text entered is hidden. To view the text, select **Show answers**.

**Note:** When answering the questions during a recovery process in the Power-on Authentication, you will have to enter the answers exactly as you entered them in the Local Self Help Wizard. For example, answers are case-sensitive in Local Self Help.

**Note:** When entering answers in Japanese, you have to use Romaji (Roman) characters. Otherwise the answers will not match when you answer the questions in the POA.

5. After you have finished answering the predefined questions, click **Next**.

6. If you are entitled to define your own questions, the User defined questions and answers dialog is displayed.

Questions	Answers
New question - 2	<click here to answer >
What is your favorite candy?	*****

- a) To add a new question, click **New Question**.

A new line is added to the list of questions.

- b) Enter your question in the **Questions** column and the answer in the **Answers** column.

After you enter the answer, the entered text is hidden.

- c) To display the text, select **Show answers**.

**Note:** When answering the questions during a recovery process in the Power-on Authentication, you will have to enter the answers exactly as you entered them in the Local Self Help Wizard. For example, answers are case-sensitive in Local Self Help.

**Note:** When entering answers in Japanese, you have to use Romaji (Roman) characters. Otherwise the answers will not match when you answer the questions in the POA.

7. After you have finished defining and answering your own questions, click **Next**.

The last dialog of the Local Self Help Wizard shows the new status information after you answer the questions. A message indicates whether the prerequisites for activating Local Self Help have been met.

8. Click **Finish**.

The questions and answers are saved. A message is displayed indicating that Local Self Help was activated successfully.

9. Click **OK**.

Local Self Help is active on your computer. You can use Local Self Help for logon recovery in the Power-on Authentication.

**Note:** If Local Self Help is active on your computer and you have reset your password via a Challenge/Response procedure, the answers stored for Local Self Help are no longer valid. Local Self Help is no longer active on your computer. To activate Local Self Help again, answer the questions again.

## 7.3 Editing questions

After activating Local Self Help on your computer, you can edit the questions at any time:

- For predefined questions, you can change the answers that were provided when answering the questions initially. However, predefined questions cannot be deleted.
- For user-defined questions, you can change the answers that were provided when answering the questions initially, add new questions, or delete questions.

To edit questions in the Local Self Help Wizard:

1. Right-click the SafeGuard Enterprise System Tray icon on the Windows taskbar.
2. Select **Local Self Help**.

The Local Self Help Wizard Welcome dialog is displayed.

For security reasons, you are prompted to enter your password.

3. Enter your password, and click **Next**.

The Status Overview dialog is displayed.

This dialog offers a short instruction on how to activate Local Self Help. Furthermore, it displays status information (for example, the number of answered user-defined questions, the number of answered predefined questions, etc).

4. Click **Next**.

- a) If you have received and answered predefined questions, the predefined questions dialog is displayed, containing the answered questions.
- b) If you have received several different question themes, you can choose between the question themes to be displayed in the drop-down list of the **Theme** field.
- c) To display all themes in a continuous list, select the **All Themes** (default) option in the drop-down list.

By default the answers entered are not shown as text.

- d) To show the text entered, activate the **Show answers** check box.
- e) To change the answers, click the relevant questions and enter your new answer in the **Answers** column.

5. After completing your changes, click **Next**.

If you are entitled to define your own questions, the User defined questions and answers dialog is displayed. By default the answers entered are not shown as text.

6. To show the text entered, click the **Show answers** check box.

- a) To change existing answers, click the relevant question, and enter your new answer in the **Answers** column.
- b) To add a new question, click **New Question**.

A new line is added to the list of questions. Enter your question in the **Questions** column, and the answer in the **Answers** column.

- c) To delete questions, click the relevant question, and click **Delete Question**.

A message is displayed, prompting you to confirm that you want to delete the question. Click **Yes**.

7. After completing your changes, click **Next**.

The last dialog of the Local Self Help Wizard shows the new status information after you edit the questions. A message indicates whether the prerequisites required for Local Self Help to remain active have been met.

8. Click **Finish**.

The questions and answers are saved. A message is displayed indicating that the editing procedure was successful, and Local Self Help remains active.

9. Click **OK**.

The modifications take effect.

Next time you launch Local Self Help in the Power-on Authentication, the modified/new questions are selected randomly and displayed. The modified/new answers apply.

**Note:** If the number of answered questions falls below the minimum number required due to the changes made, a warning message is displayed in the last dialog of the Local Self Help Wizard, indicating that Local Self Help will be deactivated after you close the wizard.

**Note:** If you do not want to deactivate Local Self Help, you can return to **User defined questions** and **Predefined questions** by clicking the **Back** button. You can then add or answer new questions. If you click **Finish** and the number of answered questions has fallen below the minimum number required, another warning message is displayed, indicating that Local Self Help is no longer active on your computer. However, in this case, you can reactivate Local Self Help (see [Activating Local Self Help](#), page 45).

## 7.4 Changes of conditions or parameters for Local Self Help during editing processes

During the process of defining or editing questions in the Local Self Help Wizard, Local Self Help parameters and other conditions that are crucial for the usage of Local Self Help may change.

For example:

- A new user password or certificate may be set.
- A new policy with new Local Self Help settings and/or a new set of Local Self Help questions may be transferred to your computer via the regular update mechanism.

If such changes occur during the editing process, the set of questions and answers you have defined may no longer be valid and there may not be enough questions for Local Self Help to become or stay active on your computer.

Therefore, each time you finish defining or editing questions in the Local Self Help Wizard, the wizard checks whether any of the following conditions apply and initiates the relevant action:

Condition	LSH Wizard action	Result
Local Self Help has been disabled globally by a new policy.	The Local Self Help Wizard shows a message stating that Local Self Help has been disabled globally and closes.	Local Self Help can no longer be used.
Local Self Help parameters have been changed (e.g., minimum length of answers, right to define your own questions) by a new policy. However, Local Self Help has not been disabled. The questions and answers you have defined are still valid and sufficient for Local Self Help to be active on your computer.	The Local Self Help Wizard shows a message stating that the Local Self Help parameters have changed, saves your changes and closes.	Local Self Help is active on your computer and can be used for logon recovery. However, the ratio of available questions and valid answers may have changed. To regain the initial ratio, you may need to add or delete questions and/or answers.
<ul style="list-style-type: none"> <li>■ The user password has been changed</li> <li><b>and/or</b></li> <li>■ Local Self Help parameters have been changed (e.g., minimum length of answers, right to define your own questions has been revoked etc.) by new policy. Local Self Help has not been disabled.</li> </ul> <p>However, the questions and answers you have defined are no longer valid and there are not enough questions for Local Self Help to be active on your computer.</p>	The Local Self Help Wizard shows a message stating that the user password or Local Self Help parameters have changed. Local Self Help will not be active on your computer. You are advised to rerun the wizard. The wizard closes.	To activate Local Self Help, rerun the Local Self Help Wizard and define questions and answers again. Afterwards, you can use Local Self Help for logon recovery.
The user certificate has changed.	The Local Self Help Wizard shows a message stating the user certificate has changed. Local Self Help will not be active on your computer. You are advised to rerun the wizard. The wizard closes.	To activate Local Self Help, rerun the Local Self Help Wizard and define questions and answers again. Afterwards, you can use Local Self Help for logon recovery.

## 7.5 Logging on at the POA via Local Self Help

To log on at the Power-on Authentication via Local Self Help, you have to answer five questions randomly selected from the ten defined questions correctly.

How to log on to your computer via Local Self Help in the Power-on Authentication:

1. Enter your user name in the POA logon dialog.

The **Recovery** button becomes active.

2. Click **Recovery**.

- If only Local Self Help is activated for logon recovery, Local Self Help is started.
- If Local Self Help and Challenge/Response are available for logon recovery, a dialog with both recovery methods for selection is displayed. Click **Local Self Help**.

The Local Self Help Welcome dialog is displayed.

This dialog provides a short description of the next steps.

3. Click **Next** to start answering the questions.

The first question is displayed in the Local Self Help - Question 1 of 5 dialog.

4. Enter your answer.

By default, the text entered is not displayed in the input field for security reasons. To display the answer, clear the **Hide answer** check box.



The screenshot shows a dialog box titled "Local Self Help - Frage 1 von 5". The background is blue with a shield icon containing a keyhole and the "SOPHOS" logo. The text inside the dialog reads: "Geben Sie die Antwort in das unten angezeigte Eingabefeld ein:". Below this is a question: "In welche Schule sind Sie zuletzt gegangen?". There is a text input field containing "\*\*\*\*\*". Below the input field is a checkbox labeled "Antwort verbergen" which is checked. At the bottom, there are three buttons: "Zurück", "Weiter", and "Abbrechen".

5. After answering the question, click **Next**.

You can only click **Next** and continue with the next question after you have entered an answer.

6. Continue to answer the remaining four questions. After answering the last one, click **OK**.

In the following dialog, you can display your current password.

7. To display the password, press **Enter** or the **Spacebar** or click the blue box.

Do NOT click **OK**. After clicking **OK** the boot process will continue WITHOUT showing the password.



The password will be shown for a maximum of five seconds. Afterwards, the boot process continues automatically.

**Note:** Ensure by all means that no unauthorized person can view the contents of your screen, be it by chance or on purpose. You can immediately hide your password by pressing the Spacebar, Enter, or by clicking the blue display box.

8. You can read the password and use it for logging on at the Power-on Authentication and to Windows again.

9. After reading the password, click **OK**. Otherwise, the boot process will continue automatically, five seconds after showing the password.

You are now logged on to the Power-on Authentication and to Windows.

## 7.6 Failed logon attempts

If you enter a wrong answer for one or several questions, the logon fails. In this case, a message indicating the failed logon is displayed. For security reasons, Local Self Help does not indicate which of the answers were wrong.

A failed Local Self Help recovery procedure is considered a failed logon attempt and logged as an event. In this case, a logon delay goes into effect. The logon delay period increases with every failed logon attempt.

If you restart your computer after a failed logon attempt, and select logon recovery via Local Self Help again, five questions are randomly selected again.

## 7.7 Reactivating questions and answers after password changes on several machines

If you use different computers with Local Self Help activated, and you change your Windows password on one machine, the Local Self Help questions and answers are no longer active on the second (or any further) machine after the password change has become effective. However, the questions and answers are still available in the Local Self Help Wizard. To use the same set of questions on the second computer again, confirm it via the Local Self Help Wizard.

Do the following:

1. After changing your password on one machine, log on to the second machine.

A tool tip indicates that there are unanswered Local Self Help questions.

2. Right-click the SafeGuard Enterprise System Tray icon on the Windows taskbar and select **Local Self Help**.

The Local Self Help Wizard Welcome dialog is displayed.

3. Enter your password, and click **Next**.
4. Confirm all following Local Self Help Wizard dialog pages with **Next** and click **Finish** on the last one.

The questions and answers stored previously on the computer are active again and are used when logging on to the POA via Local Self Help.

## 8 Recovery via Challenge/Response

For recovery, SafeGuard Enterprise offers a **Challenge/Response procedure** for exchanging information confidentially. The Challenge/Response procedure is very secure and efficient.

If you use SafeGuard Enterprise and you have, for example, forgotten your password, you can regain access to your computer very quickly through a central help desk.

**Note:** We recommend to primarily use Local Self Help to recover a forgotten password. With recovery via Local Self Help you can have the current password displayed in a confidential way in the Power-on Authentication and may continue using this password. This will avoid that the password has to be reset at all and will also avoid help desk assistance.

During the Challenge/Response procedure, you generate a challenge code (an ASCII character string), and provide this code to a help desk staff member. Based on the challenge code provided, the help desk officer then generates a response code that authorizes you to perform a specific action on your computer.

### 8.1 Typical scenarios for which you can require help desk assistance

- You have forgotten your password.
- You have entered your password incorrectly too often at POA level, and the computer has been locked.
- You have forgotten or lost your token/smartcard.
- The Power-on Authentication's local cache is partly damaged.
- A different user has to boot the SafeGuard Enterprise protected computer.
- A user has to boot the SafeGuard Enterprise protected computer from external media.

### 8.2 Procedures for which a response can be requested and the relevant scenarios

- **Booting the SafeGuard Enterprise Client without user logon:** Booting the computer without user logon helps if you have entered your password incorrectly (for example due to typing errors, activated CAPS LOCK key, etc), but you know the correct password. The Challenge/Response procedure will log you on to your computer without resetting the password.

If you have entered the password incorrectly too often, the help desk will automatically generate a response code for booting the client without user logon (the scenario is included in the challenge). Afterwards, you can log on with your user name and password again.

- **Booting the SafeGuard Enterprise Client with user logon:** If you have forgotten your password, request a challenge without trying to enter your password first. The help desk can then generate a response for logon with and without a user name. When logging on with your user name, ask your help desk to have your old password displayed during the Challenge/Response procedure. This will avoid having to reset the password. Otherwise, when logging on with your user name, you have to reset your password for the Windows logon during the Challenge/Response procedure.

**Note:** For users working offline, that is, not connected to the domain controller, some special issues need to be considered (see [Challenge/Response for offline users](#), page 61).

- **Restoring the SafeGuard Enterprise policy cache:**

This procedure is necessary, if the SafeGuard policy cache is damaged. The local cache stores all keys, policies, user certificates and audit files. By default, logon recovery is deactivated when the local cache is corrupted, i.e. it will be restored automatically from its backup. In this case, no Challenge/Response procedure is required for repairing the local cache. However, logon recovery can be activated by policy, if the local cache is to be repaired explicitly via a Challenge/Response procedure. In this case, you are prompted automatically to initiate a Challenge/Response procedure, if the local cache is corrupted.

- **Booting from external media or floppy disk:** The Challenge/Response procedure can also be used to allow a computer to be booted from external media. To do so, select **Continue Booting from: Floppy Disk/External Medium** in the POA logon dialog, and initiate the Challenge/Response procedure. The help desk can now generate a response for the following actions:
  - Booting the SGN Client with user logon
  - Booting the SGN Client without user logon
  - Allowing the procedure of booting from external media

## 8.3 The Challenge/Response procedure

1. Power-on Authentication (POA) starts.

Upon generating the challenge, a time period of 30 minutes is available for correctly entering the response generated by the help desk in a Challenge/Response procedure. After 30 minutes, the response code will no longer be valid and can no longer be used.

2. Request a challenge:

Open the Challenge dialog in the Power-on Authentication. A challenge code in the form of an ASCII character string is generated and displayed.

3. Contact the help desk.

Communicate your user data (user ID, computer ID, etc) as shown in the Challenge dialog, along with the challenge code.

4. The help desk generates a response code via the SafeGuard Management Center.

5. The help desk provides the response via phone or SMS.

6. Enter the response code at the Power-on Authentication.

You can now perform the authorized action. For example, resetting the password.

You can resume working.

## 8.4 Requesting a challenge

1. In the Power-on Authentication (POA) logon dialog, click **Recovery**.

The **Recovery** button is only activated when you enter a user name or at least one character in the PIN dialog.

**Note:** If you have entered your password/PIN incorrectly too often or if the policy cache is damaged, SafeGuard Enterprise informs you automatically, and offers to solve the problem via Challenge/Response.

Your user data and a randomly generated challenge code are displayed. For better readability, the challenge code is divided into five-character blocks.

Challenge/Response - Step 2 of 3

**SOPHOS**

If you have forgotten your password, you can call your Helpdesk to receive a password for singular use.

User domain: MY\_COMPANY  
 User name: administrator  
 Computer domain: MY\_COMPANY.EDU  
 Computer name: WIN-8E06AE481BF

Challenge: IBG7Z C14D9 GK9BJ L7GLT TDF38 Y1SML  
 This challenge will expire in: 14:43 minutes

Back Next Cancel Spelling Aid

2. Call the SafeGuard Enterprise help desk, and provide your user data as well as the challenge code to the help desk officer.

To facilitate the process of stating the challenge code, you can display a spelling aid by clicking **Spelling Aid**.

The help desk officer will be able to identify the scenario for which you need the response code from the challenge code.

3. Click **Next**.

## 8.5 Entering the response

1. Enter the response code received from the help desk officer in the Response dialog, and confirm it by clicking **OK**.

If you enter the response code incorrectly, the character block containing the error will be marked in red.

2. You are logged on at the Power-on Authentication.

If necessary, SafeGuard Enterprise will prompt you to change your Windows user credentials.

## 8.6 Best practice

### 8.6.1 You have entered the password incorrectly too often

1. You have entered your password incorrectly in the Power-on Authentication too often (typing errors, activated **Caps Lock** key etc), however, you know the correct password. You are connected to the domain.
2. Your PC is locked, and you are prompted to initiate a Challenge/Response procedure to unlock your computer.
3. Your help desk officer generates a response for booting without user logon.
4. Booting without user logon means that you do not have to change your password prior to logging on to Windows. The Windows logon dialog box is displayed. You can enter your Windows password in this dialog box, and you are logged on to the system.
5. The counter of the maximum number of password entry attempts allowed is reset.

You can also request a response with user logon. In this case you are prompted to change your Windows credentials prior to logging on to Windows.

## 8.6.2 You have forgotten your password

We recommend to primarily use the following methods to recover a forgotten password to avoid that the password has to be centrally reset:

- Use Local Self Help. With recovery via Local Self Help you can have the current password displayed and may continue using this password without having to reset it and without any help desk assistance. For further information, see <Nicht definierter Querverweis>.
- When using Challenge/Response: Ask your help desk to generate a response with user logon and to have your old password displayed during the Challenge/Response procedure. This will avoid having to reset it. You may continue working with the old password and change it locally afterwards, if desired.

If the above methods are not applied, proceed as follows:

1. If you have forgotten your password, you will receive a response for booting your computer by means of a user logon. In this case, you have to change your password when logging on to Windows (provided that the domain is accessible).
2. After changing the password, use the new password for logging on at the Power-on Authentication.

## 8.6.3 You have forgotten or lost your token

In this case, the Challenge/Response procedure with user logon has to be performed.

1. You are prompted to change your password during the Challenge/Response procedure.  
The dialog box for changing the password is only displayed if a connection to the domain controller is established.
2. If logon using a token and PIN is mandatory, you can decide whether you want to change the password or skip the password change by clicking **Cancel**.

- **You have forgotten your token**

Skipping the password change by clicking **Cancel** in the dialog only makes sense if you have forgotten your token but will have it for future logons. Upon clicking **Cancel**, you are logged on to the system and you can resume using your computer.

Without a token, you can only log on via Challenge/Response in the Power-on Authentication. Once you have your token again, you can use it to log on at the POA.

- **You have lost your token**

If you have lost your token, enter a new password in the dialog box for changing your password. You will be logged on to Windows with this password. If the policies on your computer allow it (token logon at the POA is not mandatory), you can also log on at the Power-on Authentication using this password.

Unauthorized use of the token by anyone finding it can be ruled out. Unauthorized users cannot use the token for logging on - even if they know the PIN - as your password has been changed.

#### **8.6.4 You have forgotten your PIN**

1. If you have forgotten the PIN of your token, request a response and enter a new password. You are logged on to Windows with this password, and you can also use it to log on at the Power-on Authentication, provided that you are authorized for logging on using a password.
2. A security officer has to assign a new PIN to the token, and store your new logon data on it. You can then use it for logging on.

#### **8.6.5 You cannot access your computer anymore**

If you cannot access your computer anymore, the Power-on Authentication might be corrupted. Even in this critical situation SafeGuard Enterprise offers a Challenge/Response procedure with help desk assistance enabling you to regain access to your encrypted drives. Challenge/Response in this case is carried out via a WinPE environment. When encountering such critical situation, we recommend that you contact your SafeGuard Enterprise help desk. The help desk officer will provide you with the necessary files and guide you through the necessary steps to regain access to your computer.

### **8.7 Challenge/Response for offline users**

Some special issues apply when using the Challenge/Response procedure for offline users. For offline users (that is, users who are not connected to the domain controller), an automatic password change cannot be initiated during the Challenge/Response procedure.

### 8.7.1 Challenge/Response for offline users with logon mode user name/password

**Example:**

You are working offline (you are not connected to the domain controller), and you have forgotten your password. Using the Challenge/Response procedure, you can quickly and easily regain access to your computer.

SafeGuard Enterprise can also log you on to Windows automatically during the Challenge/Response procedure. However, as you would not know the password after this procedure, you would have to repeat it each time you boot your computer. Furthermore, you would not be able to unlock your computer in case it was locked (for example, a lock on the screen saver activation). In this case, you would have to reboot your computer risking the loss of data (and initiate a Challenge/Response procedure again).

**Note:** For this reason, SafeGuard Enterprise offers the possibility to show the password during a Challenge/Response procedure. As an offline user you should have your password displayed during a Challenge/Response procedure. Tell the help desk officer that you would like to have your password displayed. The help desk officer has to activate password display explicitly prior to generating your response code.

Proceed as follows:

1. Initiate the Challenge/Response procedure by clicking **Recovery** in the POA logon dialog.
2. Call your help desk, and communicate your challenge.
3. Tell the help desk officer that you would like to boot your computer with a user logon and that your password is to be displayed.
4. Click **Next** in the Challenge/Response dialog, and enter the response.
5. Click **OK**.

6. You are asked whether your old password is to be displayed on screen.



7. Answer **Yes**, and click **OK**.
8. The next dialog informs you that your password will be displayed when you press **Enter** or the **Spacebar** on your keyboard, or when you click in the text.

Do **not** click **OK**. If you click **OK**, the boot process will continue **WITHOUT** showing the password.

The password will be shown for 5 seconds. The boot process will then continue automatically.

9. Press **Enter** or the **Spacebar** on your keyboard, or click in the text.

The password is displayed.

**Note:** Take every precaution to ensure that no unauthorized person can view the contents of your screen - be it by chance or on purpose. You can immediately hide your password by pressing the **Spacebar**, **Enter**, or by a mouse click. The password will only be shown for 5 seconds at the maximum.



10. You can read the password, and use it for logging on at the Power-on Authentication and to Windows.

You can resume working with your computer.

### 8.7.2 Challenge/Response for offline users with logon mode "Only Token"

In this case, if you have forgotten your PIN or forgotten/lost your token, the procedure to be used depends on whether you know your Windows credentials.

- You know your Windows credentials

- a) If you know your Windows credentials, initiate the Challenge/Response procedure as described. You are automatically logged on to Windows, and you can use your computer.

Logon mode "Only Token" is reset for the duration of the work session following the Challenge/Response procedure. Consequently, logging on to Windows using your user name and password will also be possible.

In case your computer should be locked, you can therefore unlock it by entering your Windows password. Logging on at the Power-on Authentication, however, is only possible via Challenge/Response.

- You do not know your Windows credentials
  - a) If you do not know your Windows credentials and you have forgotten your PIN, you can also start a Challenge/Response procedure during which your password will be displayed.
  - b) Tell your help desk officer that your password should be displayed.  
As logon mode "Only Token" will be deactivated you can also unlock your computer should it be locked using this password.  
Logging on at the Power-on Authentication, however, is only possible via Challenge/Response.

## 9 System Tray Icon and tool tips

You can easily access all of the important SafeGuard Enterprise Client functions on your computer. The SafeGuard Enterprise System Tray Icon is placed on the Windows taskbar to allow access to these functions.

**Note:** The System Tray Icon's behavior on your computer is defined by the security officer. The security officer specifies in a policy whether the icon is displayed on your computer. It can also be set to "silent". In this case, balloon tool tips are not displayed on your computer.

Via the System Tray Icon you can view information or perform specific actions. By clicking the icon with your right mouse button, you can show a menu providing the following entries:

- **Display:**
  - **Key ring:** Shows all keys available for you.
  - **Certificate:** Shows information concerning your certificate.
- **Create new key:** Opens a dialog box for creating a new key that is used for data exchange via removable media (see SafeGuard Data Exchange).
- **Local Self Help**

If Local Self Help is activated for your computer via the relevant policy, the Local Self Help command is shown on the context menu of the System Tray icon. Using this command, you can launch the Local Self Help Wizard. Local Self Help is a logon recovery method that does not require any help desk assistance. For further information on Local Self Help, see [Recovery via Local Self Help](#), page 45

- **Change Media Passphrase:** Opens a dialog box for creating a new key that is used for data exchange via removable media (see [SafeGuard Data Exchange](#), page 76).
- **Synchronize:** Starts data synchronization with the SafeGuard Enterprise Server. Tool tips show the data synchronization's progress and result.

**Note:** You can also start synchronization by double-clicking the System Tray Icon.

- **Status:** Provides a dialog box offering information on the current status of the SafeGuard Enterprise protected computer:

Field	Information
Last policy receipt	Shows the date and time of when the computer last received a new policy.
Last key receipt	Shows the date and time of when the computer last received a new key.

Field	Information
<b>Last certificate receipt</b>	Shows the date and time of when the computer last received a new certificate
<b>Last contact to server</b>	Shows the date and time of the last server contact.
<b>SGN user state</b>	<p>Shows the status of the user who is logged on to the computer (Windows logon):</p> <ul style="list-style-type: none"> <li>■ <b>Pending</b> The replication of the user in the POA is pending, i.e. the initial user synchronization has not yet been completed. This information is especially important after your first logon to SafeGuard Enterprise as you can only log on at the Power-on Authentication after initial user synchronization has been completed.</li> <li>■ <b>SGN user</b> The user has been assigned to the SafeGuard Enterprise installation as a SafeGuard Enterprise user.</li> <li>■ <b>SGN guest</b> The user logged on to Windows is a SafeGuard Enterprise guest user. The user is allowed to log on to Windows without being assigned to this SafeGuard Enterprise protected computer as a SafeGuard Enterprise user.</li> <li>■ <b>SGN guest (service account)</b> The user logged on to Windows is a SafeGuard Enterprise guest user who has logged on using a service account for administrative tasks.</li> <li>■ <b>Unknown</b> Indicates that the user status could not be determined.</li> </ul>
<b>Policy Cache State</b> <b>Data packets prepared for transmission</b>	Indicates whether there are any packages to be sent to the SafeGuard Enterprise Server.
<b>Local Self Help (LSH) State</b> <b>Enabled</b> <b>Active</b>	Indicates whether Local Self Help has been enabled via policy and whether it has been activated by the user on the computer. For further information on Local Self Help, see <a href="#">Recovery via Local Self Help</a> , page 45

- **Help:** Opens the SafeGuard Enterprise Online Help.
- **About SafeGuard Enterprise:** Shows information about your SafeGuard Enterprise Version.

## 10 SafeGuard Explorer extensions

You can access encryption-related functions via corresponding entries in Windows Explorer context menus.

### 10.1 Explorer extensions for file-based encryption

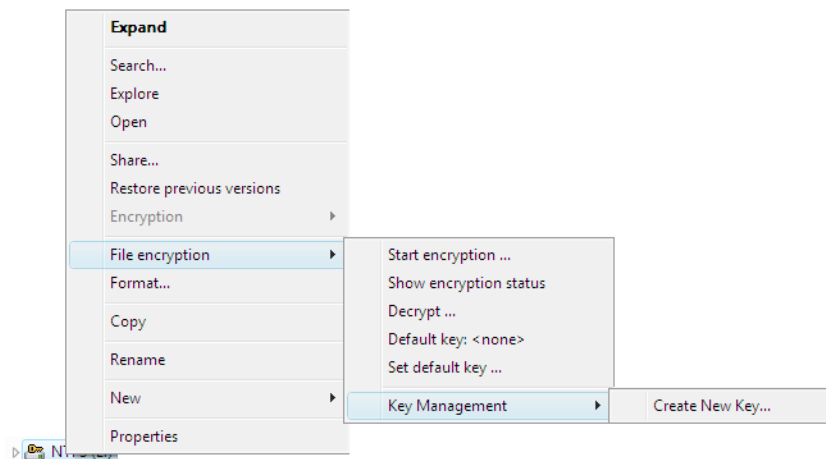
You can access the functions for file-based encryption via the corresponding entries in Windows Explorer context menus. The functions are available in the context menus of

- volumes
- removable media
- directories
- files

The entry **File encryption** is added to the context menu. You can access the individual functions via this menu.

If no file-based encryption policy applies to the volume selected, you can only determine the encryption state and display the dialog for generating new keys via the context menu.

If a file-based encryption policy applies to the selected volume, removable media, directory, or file, the following entries are added to the context menu:



**Note:** The functions displayed depend on the settings defined in the policies. Furthermore, they depend on whether the relevant function is available for the volume selected. The function scope varies depending on whether file-based or volume-based encryption was used for the relevant volume.

The following functions are available:

- **Start encryption:** If you select this option in a volume's context menu, all files can be encrypted or newly encrypted.
- **Show encryption status:** Indicates whether a volume, removable media, or a file has been encrypted, which key has been used, whether the key is included in your key ring, and whether you have access to this file.
- **Decrypt:** Decrypts the selected volume or file.
- **Default key:** Shows the key currently used for new files added to the volume (by saving, copying or moving). You can define the standard key for each individual volume or removable media separately.
- **Set default key:** Opens a dialog for selecting a different default key.
- **Key Management: Create New Key:** Opens a dialog for creating user-defined local keys.

## 10.2 Explorer extensions for volume-based encryption

The entry **Encryption** is added to the Windows Explorer context menu.

If the volume is encrypted, a key symbol is displayed next to the menu entry. If a green key symbol is shown, you have the required keys and you can access the volume.

**Note: File encryption > Show encryption status** shows the encryption status of the files on the volume from a file based encryption point of view. Files on an encrypted volume can also be encrypted in a file based manner. If this is the case, a dialog will be displayed accordingly.

### 10.2.1 Add/Remove Keys

You can add/remove keys to/from the encrypted volume if the settings specified in the applicable policies allow it. By doing so, you enable all owners of the relevant key to access the encrypted data on this volume.

You can assign keys to the volume via the volume's **Properties** dialog. This dialog includes tab Encryption (right-click on **Volume > Properties > Encryption**).

Select a key from the lower list, and click **Add Key**. The file is moved upwards from the key selection list. It is included in the list of keys that can be used to access the encrypted volume.

Using **Remove Keys**, you can remove the key from the list of keys used for accessing the media.

## 11 Data Encryption

SafeGuard Enterprise encrypts data on a computer either in a volume based or a file based manner. In the security policies, your security officer defines the volumes (drives) that are to be encrypted.

### 11.1 Initial encryption for file based encryption

If a policy stipulating the encryption of files applies to a location on your computer, a yellow key symbol is displayed next to the relevant files in Windows Explorer.

The yellow key symbol alone does not necessarily indicate that all files on the drive have already been encrypted. First, an initial encryption has to be performed.

If encryption is stipulated for files, initial encryption will either start automatically, or you will have to start it manually.

### 11.2 Transparent encryption

The files on an encrypted drive are encrypted transparently. You will not see any prompts for encryption or decryption when opening, editing, and saving files. When you open the files, they will be decrypted and you can edit them. On closing or saving the files, they will be encrypted again.

If you copy or move files (also via Save as) from an encrypted drive to an unencrypted file location on your computer, they will be decrypted. The files will be stored in the new file location in plain text.

## 11.3 Restrictions for initial encryption of SafeGuard Enterprise protected computers

Initial configuration of SafeGuard Enterprise protected computers may involve creating encryption policies that may be distributed inside a configuration package to computers.

However, when the SafeGuard Enterprise Client is not connected to a SafeGuard Enterprise Server immediately after the configuration package is installed, but is temporarily offline, only encryption policies with the following specific settings will become immediately active on the SafeGuard Enterprise protected computer:

- Device protection of type volume-based using the Defined Machine Key as encryption key

For all other policies involving encryption with user-defined keys to become active on the SafeGuard Enterprise protected computer, the respective configuration package has to be reassigned to the computer as well. The user-defined keys will then only be created after the SafeGuard Enterprise Client is connected to SafeGuard Enterprise Server again.

This is because the Defined Machine Key is created on the SafeGuard Enterprise protected computer at the first restart after installation, whereas the user-defined keys can only be created on the computer after it has been registered at the SafeGuard Enterprise Server.

## 11.4 Volume-based encryption

Volume-based encryption for a disk on the SafeGuard Enterprise protected computer starts automatically if the security officer has defined the policy accordingly.

1. A dialog is displayed, and you are prompted to select a key enabling you to access the volume.



**Note:** Every user whose key ring includes this key can access this volume. The security officer defines the scope of keys offered. If the security officer has defined a specific key, you will not be able to select a key.

2. Click **OK** to start encryption.

During the encryption process, an Encryption Viewer shows the encryption progress. It will be shown in minimized view on the Windows taskbar. You can open the Encryption Viewer simply by clicking on the icon. If you want the Encryption Viewer minimized, you can request a notification that encryption has been completed by activating **Show notify before close**. The viewer automatically closes when the encryption is complete. You can use the encrypted volume like any unencrypted volume on your computer.

**Note:** For Windows 7 Professional, Enterprise and Ultimate, a system partition is created on endpoint computers without a drive letter assigned. This system partition cannot be encrypted by SafeGuard Enterprise.

## 11.5 File-based encryption

The encryption of a volume either starts automatically or you have to initiate the process.

1. If encryption is not started automatically, select **File Encryption > Start Encryption**.
2. If the security officer has not defined a specific key, a dialog is displayed in both cases, prompting you to select a key that allows you to access this volume.



**Note:** Every user whose key ring includes this key can access this volume. The security officer defines the scope of keys offered. If the security officer has defined a specific key, you will not be able to select a key.

**Note:** For exchanging data with users who have SafeGuard Enterprise installed on their computers, but do not use the same key as you, **local, user-generated keys** are usually required. These keys are also required for secure data exchange with users who do not use SafeGuard Enterprise. You can identify local keys by their prefix (Local\_).

**Note:** If **Re-encrypt files if already encrypted with a different key** is activated, encrypted files, for which a key exists, are decrypted and encrypted again using the new key.

3. Select a key, and click **OK**.

All data on the relevant volume is encrypted.

### 11.5.1 Defining a default key

By defining a default key, you specify the key to be used for encryption during operation.

1. You can define the default key via the context menu of a file on a volume, or via the context menu of the removable medium itself.
2. Select **File encryption > Set Default key** to display a dialog for key selection.

The key you select is used for all subsequent encryption processes on the volume.

3. If you want to use a different key, define a new default key.

### 11.5.2 Encryption state

On volumes encrypted in a file-based manner, the individual files are marked by key symbols in different colors. The key colors indicate the encryption status.

- **Green key:** The file is encrypted, and you can access it.
- **Grey key:** An encryption policy applies to the file. However, it is not yet encrypted.
- **Red key:** The file is encrypted with a key that is not included in your key ring. You cannot access it.

You can also view the encryption state of a file via its context menu. By selecting **File encryption > Show encryption status** you can open a window showing the encryption state.

If you select **File encryption > Encryption status** from the context menu of the volume itself, a dialog is displayed showing all files and their encryption states.

## 11.6 Volume access restrictions

SafeGuard Enterprise denies access to volumes in the following cases:

### 11.6.1 Volumes with failed encryption

If a policy exists that defines that a volume or a volume type is to be encrypted, and specific steps in the encryption process fail, access to the volume is denied.

When you try to access the volume, a relevant message is displayed.

## **11.6.2 Unidentified File System Objects**

Unidentified File System Objects are volumes that cannot be clearly identified as plain or encrypted by SafeGuard Enterprise.

If a policy exists that defines that a volume of this type is to be encrypted, access to this volume is denied. When you try to access the volume, a relevant message is displayed.

If there is no encryption policy for an Unidentified File System Object, you can access the volume.

## 12 SafeGuard Data Exchange

SafeGuard Data Exchange allows you to encrypt data stored on removable media that is connected to your computer, and exchange it with other users. All encryption and decryption processes are run transparently and involve minimum user interaction.

Only users who have the appropriate keys available can read the contents of the encrypted data. All subsequent encryption processes are run transparently. Transparent encryption means data that has been encrypted and saved is automatically decrypted by an application when the data is accessed again.

When you save the relevant file, it is automatically encrypted again. During daily work you will not notice that the data is encrypted. However, when you disconnect the removable media, the data remains encrypted and is protected against unauthorized access. Unauthorized users can access the files physically, but they cannot read them without SafeGuard Data Exchange and the relevant key.

**Note:** The behavior of SafeGuard Data Exchange on your computer is centrally defined by the security officer.

In central administration, the security officer defines how data on removable media is handled. The security officer can, for example, define encryption as mandatory for files stored on any removable media. In this case, all unencrypted files existing on the device are initially encrypted. In addition, all new files saved to removable media are encrypted. If existing files are not to be encrypted, the security officer can choose to allow access to existing unencrypted files. In this case, SafeGuard Data Exchange does not encrypt the existing unencrypted files. However, new files are encrypted. So you can read and edit the existing unencrypted files, but as soon as you rename them, they are encrypted. Alternatively, you will not be allowed to access unencrypted files, and they will remain unencrypted.

There are two possible methods for exchanging encrypted files stored on removable media:

- **SafeGuard Enterprise** is installed on the recipient's computer: You can use keys available to both of you, or you can create a new key. If you generate a new key, you have to provide the data recipient with the passphrase for the key.
- **SafeGuard Enterprise is not** installed on the recipient's computer: SafeGuard Enterprise offers SafeGuard Portable. This utility can be automatically copied to the removable media in addition to the encrypted files. Using SafeGuard Portable and the relevant passphrase, the recipient can decrypt the encrypted files and encrypt them again without SafeGuard Data Exchange being installed on their computer.

## 12.1 Single media passphrase for every removable device connected to the computer

SafeGuard Data Exchange supports the definition of a single media passphrase that will give you access to all removable devices connected to your computer. This is independent of the key that is used for encrypting the individual files.

If specified, access to encrypted files can be granted by presenting only one media passphrase. The media passphrase is bound to computers for which you have logon permission. This means that you use the same media passphrase on each computer.

The media passphrase can be changed and will be synchronized automatically on each computer you are working on, as soon as you connect removable media to this computer.

A media passphrase makes sense in the following scenarios:

- You want to use encrypted data on removable media also on computers where SafeGuard Enterprise is not installed (SafeGuard Data Exchange in combination with SafeGuard Portable)
- You want to exchange data with external users: by providing them with the media passphrase, you can give them access to all files on the removable media with one single passphrase, regardless of which key was used for encrypting the individual files.

You can also restrict access to all files by only providing the external user with the passphrase of a specific key (a "local key," which can be created by a SafeGuard Data Exchange user). In this case the external user will only have access to files that are encrypted using this key. All other files will not be readable.

**Note:** A media passphrase is not necessary if you use SafeGuard Enterprise group keys to exchange data on removable media within a workgroup where the members share such a key.

**Note:** In this case - if specified by your security officer - access to encrypted files on removable media is fully transparent. It is not necessary to present any passphrase or password.

**Note:** This is because group keys and media passphrases for removable media can be used simultaneously. Since the system automatically detects an available group key, access for users sharing this key is fully transparent. If no group key is detected, SafeGuard Data Exchange will display a dialog, and prompt the user to enter a media passphrase or the passphrase for a local key.

If SafeGuard Data Exchange is installed on your computer, removable media will be handled as predefined by your security officer. A security officer can define the following behavior settings for SafeGuard Data Exchange (a combination of several settings is also possible):

- **Initial encryption of all files:** In this case encryption of all data contained on removable media will start as soon as the device is connected to your computer. This setting ensures that the removable media contain only encrypted data. When encryption starts, you will either be asked to select a key, or a predefined key will be used.
- **You are allowed to cancel initial encryption:** When initial encryption starts, a dialog is displayed that allows you to cancel initial encryption.
- **You are not allowed to access unencrypted data:** In this case SafeGuard Data Exchange will only accept encrypted data on removable media. If unencrypted data exists on removable media, the system will not allow you to access it. Only after encrypting the files will you be able to access the data.
- **You are allowed to decrypt files:** In this case you can explicitly decrypt files on removable media. A file that has been explicitly decrypted remains as plain text on the removable medium, if it is, for example, transferred to a third party.
- **You are allowed to define a media passphrase for removable media:** You are prompted to enter a media passphrase the first time you connect removable media.
- **Plain text folder on removable media:** The security officer may define a plain text folder that will be created on all of your removable media. Files in this folder will not be encrypted by SafeGuard Data Exchange

### 12.1.1 Supported media

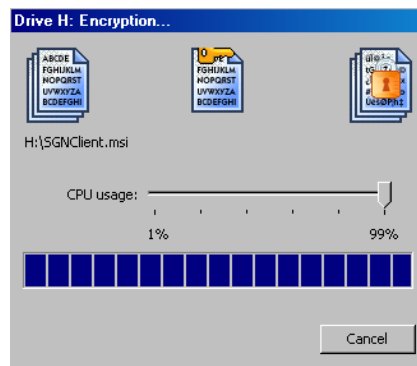
SafeGuard Data Exchange supports the following removable media:

- USB sticks
- External hard disks connected via USB or FireWire
- CD RW drives (UDF)
- DVD RW drives (UDF)
- FireWire
- Memory cards in USB card readers (incl. ZIP, JAZ)

## 12.2 Encrypting removable media

### 12.2.1 Initial encryption

Encryption of unencrypted data contained on removable media either starts automatically as soon as you connect the media to the system, or you have to start the process manually.



1. To start the encryption process, select **File encryption** > **Start encryption** via the context menu in Windows Explorer. If no specific key has been defined, a dialog is displayed for key selection.



2. Select a key, and click **OK**. All data contained on the removable media is encrypted.
3. The default key is used as long as no other key is set as the default. If you change the default key, the new one is used for initial encryption of removable devices that are connected to the computer afterwards.

**Note:** For exchanging data with users who have **SafeGuard Enterprise** installed on their computers but do not use the same key as you do, local user-generated keys or a media passphrase is required. These keys are also required for secure data exchange with users who do not use **SafeGuard Enterprise**. You can identify local keys by their prefix (Local\_).

If **Re-encrypt files if already encrypted with a different key** is activated, encrypted files with an existing key will be decrypted and encrypted again using the new key.

#### **Initial encryption time out**

If initial encryption is configured to start automatically, you may have the right to cancel initial encryption. In this case, the **Cancel** button is activated, a **Start** button is displayed, and the start of the encryption process is delayed for 30 seconds. If you do not click the **Cancel** button during this time period, initial encryption starts automatically after 30 seconds. If you click **Start**, initial encryption is started immediately.

### **12.2.1.1 Initial encryption in case of using the media passphrase**

If the usage of a media passphrase has been defined via policy, you are prompted to enter the media passphrase prior to initial encryption. The media passphrase is valid for all of your removable media and is bound to your computer or to all computers for which you have logon permission.

Initial encryption will not start before you have entered the media passphrase. After you have done so, initial encryption will start automatically.

After entering the media passphrase once, initial encryption will start automatically when you connect a different device to your computer.

**Note:** On computers where your media passphrase is not set, initial encryption will not start.

### **12.2.2 Transparent encryption**

If the settings defined for your computer stipulate that files have to be encrypted on removable media, all encryption and decryption processes run transparently.

The files are encrypted when they are written to removable media and decrypted when they are copied or moved from removable media to another file location.

**Note:** The data is only decrypted if it is copied or moved to a location for which no other encryption policy applies. The data is then available at this location in plain text. If a different encryption policy applies to the new file location, the data is encrypted accordingly.

### 12.2.2.1 Media passphrase

If specified by policy, you are prompted to enter the media passphrase, when you connect a removable device for the first time after the installation of SafeGuard Data Exchange.

If the dialog is displayed, read the information carefully, and specify a media passphrase. You can use this single media passphrase to access all encrypted files on your removable media, regardless of the key that was used to encrypt them.

The media passphrase is valid for all devices you connect to the computer. The media passphrase can also be used with SafeGuard Portable and allows you to access all files, regardless of the key that was used to encrypt them.

### 12.2.2.2 Change/reset media passphrase

You can change your media passphrase at any time using **Change Media Passphrase** from the System Tray icon menu. A dialog is displayed in which you enter the old and new media passphrase and confirm the new one.

If you have forgotten your media passphrase, this dialog also provides an option to reset it. If you activate the **Reset Media Passphrase** option and click **OK**, you are informed that your media passphrase will be reset at the next logon.

Log off immediately and log on again. Then select **Change Media Passphrase** from the Tray icon's menu. You are informed that there is no media passphrase on your computer and prompted to enter a new one.

### 12.2.2.3 Media passphrase synchronization

The media passphrase on your devices and on your computer will be synchronized automatically. If you change the media passphrase on your computer and connect a device that still uses an old version of the media passphrase, you will be informed that the media passphrases have been synchronized. This is true for all computers for which you have logon permission.

**Note:** After you have changed your media passphrase, you should connect all of your removable media with your computer. This ensures that the new media passphrase is used on all your devices immediately (synchronization).

#### 12.2.2.4 Defining a default key

By defining a default key you specify the key to be used for encryption during normal operation.

You can define the default key via the context menu of a file on removable media, or via the context menu of the removable media. Additionally, you can set a key as default immediately when you create a new local key in the "Create key" dialog.

Select **File encryption > Set default key** to open a dialog or key selection.

The key you select in this dialog is used for all subsequent encryption processes on the removable medium. If you want to use a different one, you can define a new default key at any time.

By policy, a default key to be used for encryption can be specified. If it is not defined by policy, you are prompted to specify an initial default key.

### 12.3 Exchanging data using SafeGuard Data Exchange

Following are typical examples for secure data exchange via SafeGuard Data Exchange:

- Exchanging data with SafeGuard Enterprise users who have at least one key that is also included in your key ring.

In this case, encrypt the data on the removable media using a key that is also included in the recipient's key ring (e.g., on his/her notebook). The recipient can use the key to access the encrypted data transparently.

- Exchanging data with SafeGuard Enterprise users who do not have the same keys as you do.

In this case, create a local key and encrypt the data using this key. Keys created locally are secured by a passphrase and can be imported by SafeGuard Enterprise. You provide the data's recipient with the passphrase. Using the passphrase, the recipient can import the key and access the data.

- Exchanging data with users without SafeGuard Enterprise

For users who do not have SafeGuard Enterprise installed on their machines, SafeGuard Portable is available. To exchange data using SafeGuard Portable, local keys must also be used in combination with a passphrase.

In addition, SafeGuard Portable has to be copied to the removable medium. You also have to provide the recipient of encrypted data with the relevant passphrase. Using the passphrase and SafeGuard Portable, the user can decrypt the encrypted files, edit them for example, and save them encrypted again on the removable medium. As SafeGuard Portable is a self-sufficient application, no additional software needs to be installed on the host system in order to access encrypted data.

**Note:** The security officer determines whether SafeGuard Portable is copied to removable media via the security policy that applies to you.

### 12.3.1 Importing keys from a file

If you have received removable media containing encrypted data which has been encrypted using user-defined local keys, you can import the key required for decryption to your private key ring.

To import the key, you need the relevant passphrase. The person who encrypted the data has to provide you with the passphrase.

Select the relevant file on the removable device and click **File encryption > Key Management > Import Key**.

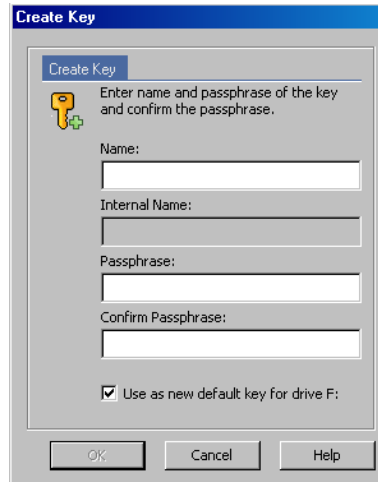


Enter the passphrase in the dialog that is displayed. The key is imported, and you can access the file.

### 12.3.2 Creating local keys for SafeGuard data exchange

To create a user-defined local key, proceed as follows:

1. Right-click the SafeGuard Enterprise System Tray icon on the Windows taskbar.
2. Click **Create new Key**.



3. In the Create Key dialog, enter a **Name** and a **Passphrase** for the key.

The internal name of the key is displayed in the field below.

4. Confirm the passphrase.

If you enter an insecure passphrase, a warning message is displayed. To increase the level of security, we recommend you use complex passphrases. You can also decide to use the passphrase despite the warning message. The passphrase also has to correspond with the company policies that are defined. If it does not, a warning message is displayed.

5. With the **Use as new default key for drive** option, you can set the new key immediately as the default key for the displayed drive.

The default key you specify here is used for encryption during normal operation. It will be used until a different one is set.

6. Click **OK**.

The key is created and becomes available as soon as the data has been successfully synchronized with the SafeGuard Enterprise Server.

If you define this key as the default key, all data copied to the removable medium from now on is encrypted using this key.

For the recipient to be able to decrypt all data contained on the removable medium, you may have to re-encrypt the data on the removable medium using the key created locally. To do so, select **File encryption > Start encryption** from the device's context menu in Windows Explorer. Select the required local key and encrypt the data. This is not necessary if you use a media passphrase.

## 12.4 Writing files to CD/DVDs using the Windows CD Writing Wizard

**Note:** With Windows XP, you can only write files to CDs with the Windows CD Writing Wizard. Windows XP does not support writing files to DVD with the CD Writing Wizard.

SafeGuard Data Exchange 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 Data Exchange adds a dialog to the CD Writing Wizard. There you can specify how the files are written to CD (encrypted or plain).

**Note:** If there is no encryption rule for the CD recording drive, files are always written to the CD in plaintext. The SafeGuard Data Exchange dialog, where the encryption state of files to be written to the CD can be specified, is not 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 plain files

Under **Status**, the keys used for encrypting already encrypted files are displayed.

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

Files to be written to CD may be encrypted with different keys if the encryption rule for the CD recording drive has been changed. If the encryption rule was deactivated when files were added, the relevant plain files can be found in the folder for files to be copied to CD.

### 12.4.1 Encrypting files on CD

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

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

### 12.4.2 Writing files to CD in plain

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

### 12.4.3 Copy SafeGuard Portable to optical media

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

### 12.4.4 Writing CDs/DVDs with Windows Vista

Windows Vista also provides a CD Writing Wizard for CDs/DVDs.

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

For the Live File System, no Recording Wizard is required. 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 are encrypted automatically when they are copied to CD/DVD.

## 12.5 SafeGuard Portable

Using SafeGuard Portable, you can exchange encrypted data via removable media with recipients who do not have SafeGuard Data Exchange installed on their machines. Data encrypted via SafeGuard Data Exchange can be encrypted and decrypted using SafeGuard Portable. This is achieved by automatically copying a program (SGPortable.exe) to the removable media.

**Note:** SafeGuard Portable only encrypts or decrypts files encrypted with AES 256.

Using SafeGuard Portable in combination with the relevant media passphrase gives you access to all encrypted files, regardless of which key was used for encrypting them. Or, the passphrase of a local key only gives you access to files that have been encrypted using this specific key. The recipient can decrypt encrypted data and encrypt it again.

**Note:** The media passphrase or the passphrase of a local key has to be communicated to the recipient beforehand.

The recipient can use existing keys created via SafeGuard Data Exchange for encryption, or create a new key via SafeGuard Portable (for example for new files).

SafeGuard Portable does not have to be installed on or copied to the machine of your communication partner. It remains on the removable media.

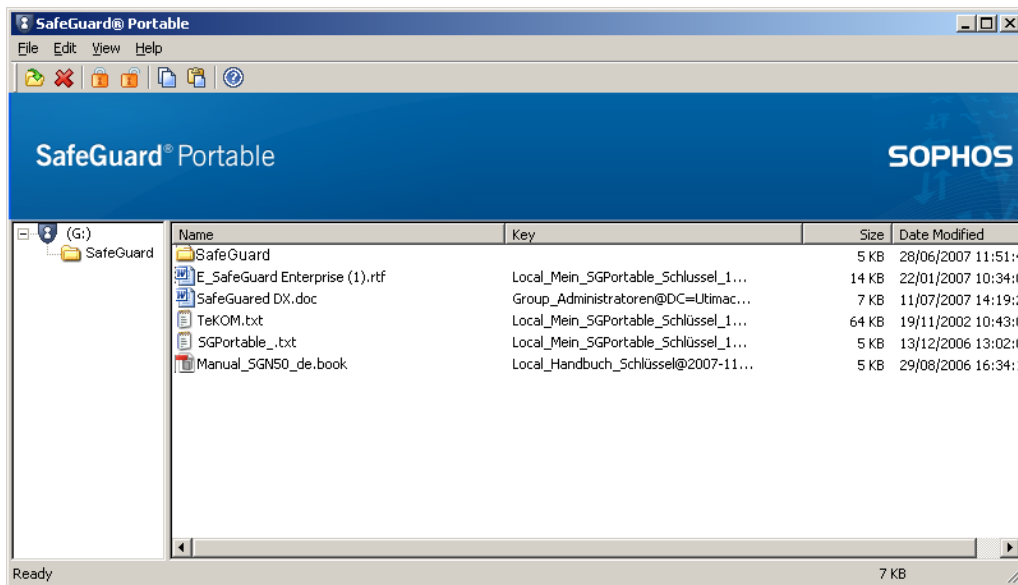
**Note:** As a SafeGuard Enterprise user, you usually do not need SafeGuard Portable. The following description assumes that users do not have SafeGuard Enterprise installed on their computer and therefore have to use SafeGuard Portable to edit encrypted data.

## 12.5.1 Editing files using SafeGuard Portable

You have received removable media containing files encrypted with SafeGuard Data Exchange, along with a folder named `SGPortable`. This folder contains the file `SGPortable.exe`.

1. Start SafeGuard Portable by double-clicking on `SGPortable.exe`.

Using SafeGuard Portable, you can decrypt the encrypted data contained on the removable media and then re-encrypt it. SafeGuard Portable offers functionality that is similar to Windows Explorer



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

**Note:** You can only decrypt files if you know the relevant passphrase for the key used.

2. To edit files on the removable media, 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 from the context menu:

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

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

### 12.5.1.1 Setting encryption keys

To encrypt a file on a removable media, and create an encryption key:

1. From the context menu or from the **File** menu, select **Set Encryption Key**.  
The Enter Key dialog is displayed.
2. Enter a **Name** and a **Passphrase** for the key. **Confirm** the passphrase, and click **OK**.  
The passphrase has to correspond to the company policies that are defined. If it does not, a warning message is displayed.

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

### 12.5.1.2 Encrypting

To encrypt a file on removable media:

1. In SafeGuard Portable Explorer, select the file and, using the context menu, select **Encrypt**.  
The file is encrypted with the key last used by SafeGuard Portable.  
When saving new files on removable media using a drag-and-drop procedure in the SafeGuard Portable Explorer, you are asked if 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 (and confirm the passphrase) in this dialog. Click **OK**.

2. Select the file to be encrypted with the key you have just set, and select **Encrypt** from the context menu or from the **File** menu.

The file is encrypted, and a message is displayed upon completion.

**Note:** The key last used and set by SafeGuard Portable is used for all subsequent encryption processes you perform with SafeGuard Portable, unless you set a new key.

### 12.5.1.3 Decrypting

To decrypt a file on removable media:

1. Select the file in SafeGuard Portable Explorer, and select **Decrypt** from the context menu.

The dialog for entering the media passphrase or the passphrase of a local key is displayed.

2. Enter the relevant passphrase (the sender has to provide you with this passphrase), and click **OK**.

The file is decrypted.

The media passphrase gives you access to all encrypted files on the removable media, regardless of which key was used to encrypt them. If you only have the passphrase of a local key, you will only have access to files which are encrypted using this key.

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

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 that have been encrypted with the same key.

SafeGuard Portable stores the passphrase for as long as the application is running. The last key used by SafeGuard Portable is used for encryption.

After you decrypt the files, they are available in plaintext on the removable media. Files that have been decrypted are encrypted automatically when you close SafeGuard Portable.

#### 12.5.1.4 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:

1. Simply move the required files into the SafeGuard Portable Explorer using drag & drop.  
The system asks you whether you want to encrypt the relevant file.
2. Confirm to have the file encrypted with the key last used and copied to the removable media.

#### 12.5.1.5 Encryption state

To determine a file's encryption state:

1. Select the file, and select the **Encryption State** from the context menu or from the **File** menu.  
The encryption state is also indicated in the **Key** column next to the file name in SafeGuard Portable Explorer.

### 12.5.2 Other operations using SafeGuard Portable

The following operations are also available:

- **Open:** This menu command is only available via the SafeGuard Portable File menu.  
Upon opening an encrypted file with this menu command, you are prompted to enter your passphrase. Enter your passphrase, and click **OK**. The file is decrypted and opened.
- **Delete:** Deletes the selected file.
- **Copy to:** This menu command is only available in the context menu that you can open 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.
- **Exit:** This menu command is only available from the SafeGuard Portable File menu.  
**Exit** closes SafeGuard Portable.

## 13 SafeGuard Configuration Protection

Using SafeGuard Configuration Protection, you can define the interfaces and peripheral devices allowed on endpoint computers. This prevents malware from being introduced as well as data exports via unwanted channels such as WLAN. This module can also detect and block harmful hardware such as key loggers.

In general, ports or devices can be allowed or blocked on your computer using policies. Furthermore, usage can be restricted to certain devices.

Restrictions to certain devices are possible for the following types of ports:

- USB
- PCMCIA
- Firewire

For these ports, the devices allowed and disallowed can be exactly defined.

The security officer centrally defines which ports and devices may be used.

If a specific port is not allowed in general, a notification message is displayed once upon receipt of the policy containing this information. The port cannot be used.

The notification message is displayed as a tool tip of the separate configuration protection icon on the Windows taskbar.

If port or storage media usage restrictions were defined for your computer, the tool tip alerts you as soon as you try to use ports or storage media that are not allowed.

## 14 SafeGuard Enterprise and BitLocker

BitLocker Drive Encryption is a full disk encryption feature with pre-boot authentication that is included with Microsoft's Windows Vista and Windows 7 operating systems. It is designed to protect data by providing encryption for the boot volume.

### 14.1 Encryption policies for BitLocker

The security officer can create a policy for (initial) encryption in the SafeGuard Management Center, and distribute it to the BitLocker endpoint computers where it is executed.

Since the BitLocker clients are managed transparently in the Management Center, the security officer does not have to make any special BitLocker settings for encryption. SafeGuard Enterprise knows of the status of the clients and selects the BitLocker encryption accordingly. When a BitLocker client is installed with SafeGuard Enterprise and volume encryption is activated, the volumes are encrypted by BitLocker.

### 14.2 Initial encryption on the BitLocker protected computer

When the encryption policy is sent to the BitLocker protected computer and before the computer starts the initial encryption, the encryption keys are generated by BitLocker. You are asked where to store the BitLocker encryption key. A backup of this key is additionally stored in the SafeGuard Enterprise database for recovery.

When SafeGuard Enterprise is installed on your computer, the SafeGuard Enterprise product icon is displayed in the system tray of the PC's taskbar. You can centrally access all important functions provided by SafeGuard Enterprise on your computer. Please note that the features available depend on the settings defined in the SafeGuard Management Center. The security officer specifies these settings centrally in the SafeGuard Management Center, and distributes them to the endpoint computers.



**Note:** If a BitLocker-encrypted hard disk in a computer is replaced with a new BitLocker-encrypted hard disk, and the new hard disk is assigned the same drive letter as the previous hard disk, SafeGuard Enterprise only saves the recovery key of the new hard disk.

**Note:** In case a volume is already encrypted with BitLocker, before installing the BitLocker support of SafeGuard Enterprise, you need to back up the keys of the formerly encrypted volume by using the backup mechanisms offered by Microsoft.

## 14.3 Decryption with BitLocker

Computers encrypted with BitLocker cannot be decrypted automatically. Decryption must be carried out using the Microsoft "Manage-bde" tool.

## 14.4 Authentication with BitLocker

BitLocker offers a range of authentication options. BitLocker users can either authenticate via a Trusted Platform Module (TPM) or USB stick or a combination of both.

The security officer can set the various logon modes in a policy in the SafeGuard Management Center and distribute it to the BitLocker endpoint computers.

The following logon modes exist for SafeGuard Enterprise BitLocker users:

- TPM only
- TPM + PIN
- TPM + USB Stick
- USB Stick only (TPM-less)

### 14.4.1 Trusted Platform module (TPM)

TPM is a smartcard-like module on the motherboard performing cryptographic functions and digital signature operations. It can create, store and manage user keys. It is protected against attacks.

### **14.4.2 USB stick**

The external keys can be stored on an unprotected USB stick.

### **14.4.3 Authentication at the BitLocker computer**

During preboot of your BitLocker computer you are asked to insert the TPM PIN or USB stick for authentication.

## 15 SafeGuard Enterprise and Lenovo Rescue and Recovery

For information on the Lenovo Rescue and Recovery (RnR) versions supported by SafeGuard Enterprise, see the following knowledge base article: <http://www.sophos.com/support/knowledgebase/article/108383.html>

It is possible to restore complete operating system backups on an encrypted partition without the need to decrypt the hard disk first. This saves a lot of time when performing disaster recovery. SafeGuard Enterprise has been officially certified by Lenovo for this functionality.

The main function of Lenovo Rescue and Recovery is to restore data at the press of a key. Even if the primary operating system is damaged and no longer boots, Rescue and Recovery saves data via an emergency environment (WinPE). You can access the rescue tools from the Microsoft Windows Desktop or by pressing the blue "ThinkVantage" key integrated in Lenovo systems.

Lenovo Rescue and Recovery is most useful for mobile users who do not have administrative support. For example, on a business trip, they can use it to restore their computers.

### 15.1 Overview

SafeGuard Enterprise is integrated with Rescue and Recovery functionality and supports Lenovo features such as the "ThinkVantage" blue button on the keyboard of Lenovo notebooks, or the blue "Enter" button on Lenovo PC keyboards.

This integrated functionality lets you pair this efficient backup and recovery method with SafeGuard Enterprise encrypted operating system partitions. Backups from encrypted SafeGuard Enterprise systems can be stored on any disk drive used by RnR. Therefore, in an emergency, a system can be restored by loading the backup from a virtual or service partition or from a removable device such as a CD/DVD or a USB hard disk.

SafeGuard Enterprise is unaffected by a system restore and all the encryption settings are still in place, so there is no need to reinstall any software. You do not have to restart encryption.

In a SafeGuard Enterprise environment Rescue and Recovery is based on WinPE recovery. WinPE can be started from different environments:

- from a virtual or service partition
- from a removable device such as a CD/DVD or a USB hard disk.

## 15.2 Requirements

- Latest BIOS for the PC/notebook.
- For information on compatibility of Rescue and Recovery versions with SafeGuard Enterprise versions, see the knowledgebase: <http://www.sophos.com/support/knowledgebase/article/108383.html>
- Lenovo Rescue and Recovery can be used to recover SafeGuard Enterprise encrypted volumes. The `SGNClient.msi` installation package must be installed.
- For Rescue and Recovery, volumes must be encrypted with the defined machine key. For volumes encrypted with any other keys, Rescue and Recovery is not supported.

## 15.3 Installation

When Rescue and Recovery software is installed on a hard disk without a service partition, the following applies:

The Rescue and Recovery environment is installed on a virtual partition on the computer's hard disk "C:" partition (primary partition of the master hard disk)

In the sections that follow, note the sequence in which Rescue and Recovery and SafeGuard Enterprise are installed. It is recommended that you install Lenovo Rescue and Recovery first, and SafeGuard Enterprise afterwards.

### 15.3.1 Installing both Rescue and Recovery and SafeGuard Enterprise

The following installation sequence is recommended:

1. Install the latest version of Rescue and Recovery.
2. Install the latest version of the SafeGuard Enterprise Device Encryption module (`SGNClient.msi`).

SafeGuard Enterprise checks if Rescue and Recovery is installed, and adds its own files and configurations to the Lenovo recovery environment.

3. Check that the Power-on Authentication is activated, so no unauthorized backups can be restored.

You activate the Power-on Authentication when installing SafeGuard Enterprise.

### 15.3.2 SafeGuard Enterprise Device Encryption is already installed

The necessary installation steps for Rescue and Recovery depend on where RnR WinPE will be located.

- RnR WinPE is located on the first hard disk on a service or virtual partition

In this case no automatic SafeGuard Enterprise settings are carried out for the RnR WinPE environment. You must start a SafeGuard Enterprise tool named `SetupWinPE.exe` to setup RnR WinPE for use with SafeGuard Enterprise. This tool will perform all necessary modifications for the WinPE environment.

**Note:** `SetupWinPE.exe` can also be used if the current installed RnR is upgraded with a new version. In case of an RnR upgrade we recommend to start `SetupWinPE.exe` again to make sure all necessary WinPE modifications are carried out.

**Note:** Note, that this tool can only be used for an RnR WinPE located on a local hard disk.

- a) Install Rescue and Recovery on the local hard disk.
- b) Start the following tool:  
`SetupWinPE.exe -r`
- c) Restart the Windows operating system.

- RnR WinPE is located on a CD-ROM or external hard disk

When WinPE is created by the RnR function Create Rescue and Recovery Media all necessary modifications are already performed for the RnR WinPE environment.

- a) Install Rescue and Recovery.
- b) Restart the Windows operating system.

### 15.3.3 Rescue and Recovery is already installed

RnR WinPE is located on the first hard disk on a service or virtual partition.

In this case all necessary drivers and files are copied to the corresponding locations of RnR WinPE, and the necessary registry entries are added to the registry files of WinPE.

Install the latest version of the SafeGuard Enterprise Device Encryption module (`SGNClient.msi`).

SafeGuard Enterprise checks if Rescue and Recovery is installed and adds its own files and configurations to the Lenovo recovery environment (WinPE).

## 15.4 Upgrade

Upgrade implies that SafeGuard Enterprise and Rescue and Recovery are installed, and you want to upgrade one or both of the two to a newer version.

### 15.4.1 Upgrade SafeGuard Enterprise

If you upgrade SafeGuard Enterprise, this updates the entire system, so you will not need to set any further configurations.

### 15.4.2 Upgrade Rescue and Recovery

If you upgrade Rescue and Recovery, run SetupWinPE.exe before you reboot after the update.

## 15.5 Uninstallation

When uninstalling the software products:

- It is recommended that you uninstall SafeGuard Enterprise first, and then Rescue and Recovery. If SafeGuard Enterprise is uninstalled while Rescue and Recovery is still installed, all SafeGuard Enterprise specific modifications, such as added drives, files, and registry entries are removed from RnR WinPE.
- Do not uninstall SafeGuard Enterprise immediately after the system has been restored. After a system restore, boot the computer once and then uninstall SafeGuard Enterprise.
- If Rescue and Recovery is removed while SafeGuard Enterprise is still installed, then RnR modifications of the MBR boot sector are removed, and the original MBR boot sector is restored.

## 15.6 Boot environment and recovery options

SafeGuard Enterprise allows you to boot into the Rescue and Recovery environment after successfully having logged on at the Power-on Authentication (POA).

### From the local hard disk

- The virtual partition on the local hard disk or the local service partition.
- The volumes must have been encrypted in SafeGuard Enterprise with the defined machine key. All necessary drivers must have been added to RnR WinPE. Then the defined machine key is available in the RnR WinPE environment and the volumes can be accessed again.

**Note:** SafeGuard Enterprise does not allow you to boot into the Rescue and Recovery environment when booting directly from BIOS.

### From a bootable CD/DVD or any bootable removable media

- In this case no authentication at the POA is performed, and there are no keys available, so encrypted volumes cannot be accessed. If the Rescue and Recovery is booted directly from BIOS, the operating system will be recovered. SafeGuard Enterprise will be removed during the restore process. To secure the system again, SafeGuard Enterprise must be reinstalled.

## 15.7 Creating a backup

You create backups using Rescue and Recovery in Windows. On computers on which Rescue and Recovery is already installed, and SafeGuard Enterprise is installed later on, a message is displayed prompting the user to create a new backup of the system.

Before creating a backup of your system using Rescue and Recovery, please read the documentation provided by Lenovo.

SafeGuard Enterprise only provides support for saving the backups:

- to the local hard disk
- second hard disk
- USB hard disk
- network
- USB memory stick
- CD/DVD

By default the backups are saved in the C:\RRUbackups folder. This folder is protected by Rescue and Recovery if it is stored on a local partition on the primary hard disk drive. If so, it cannot be deleted or removed.

## 15.8 Restoring file backups

Rescue and Recovery can restore files or folders from backups in which SafeGuard Enterprise is installed. Simply start Windows, and then Rescue and Recovery, and restore the selected files. You do not have to reboot your machine after the restore is completed: you can work with your files immediately.

## 15.9 Restoring the SafeGuard Enterprise system

To restore a system backup that includes SafeGuard Enterprise, boot into the Rescue and Recovery environment. The RnR environment appears as soon as you press one of following keys during the boot process:

- "Thinkvantage" (Lenovo Notebooks)
- "Blue Enter" key (Lenovo Desktop PCs)
- **F11** with other keyboards

1. If you use a Lenovo computer:

- a) Start the Rescue and Recovery environment from a local hard disk by pressing the blue "ThinkVantage" button on the Lenovo notebook keyboard, or the blue "Enter" button on a Lenovo PC keyboard.

The Power-on Authentication is displayed.

- b) Enter the SafeGuard Enterprise credentials.

2. If you do not use a Lenovo computer:

- a) Log in at the POA with your SafeGuard Enterprise credentials.
- b) While the computer continues booting, press **F11** to start the Rescue and Recovery environment.

The user interface for Rescue and Recovery is displayed. The welcome screen is displayed.

3. Click **Next**.

4. On the left-hand side menu, select **Restore Backup**.

A dialog is displayed in which you can select the backup.

5. Select the backup and restore it.

## 15.10 Service and factory recovery partitions

Lenovo supplies new computers with special pre-installed partitions:

- **Lenovo service partition:** contains the Rescue and Recovery boot environment.
- **Factory recovery partition:** contains all information about the computer's factory settings and factory recovery functions.

These partitions are visible in Windows under separate drive letters.

**Note:** When these partitions are available on the computer, they will never be encrypted even if an encryption policy is defined to, for example, encrypt all volumes.

If there are no such partitions on the computer, but you would like to create one, do so before installing SafeGuard Enterprise. For further information, refer to the Lenovo documentation.

## 15.11 Disabled POA and Lenovo Rescue and Recovery

If the Power-on Authentication is disabled on your computer, the Rescue and Recovery authentication should be enabled for protection against access to encrypted files from the Rescue and Recovery environment.

For details on activating the Rescue and Recovery authentication, refer to the Lenovo Rescue and Recovery documentation.

## 16 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](mailto:support@sophos.com), including your Sophos software version number(s), operating system(s) and patch level(s), and the text of any error messages

## **17 Copyright**

Copyright © 1996 - 2010 Sophos Group and Utimaco Safeware AG. All rights reserved.

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.

Sophos is a registered trademark of Sophos Plc and the Sophos Group. SafeGuard is a registered trademark of Utimaco Safeware AG - a member of the Sophos Group. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

All SafeGuard products are copyright of Utimaco Safeware AG - a member of the Sophos Group, or, as applicable, its licensors. All other Sophos products are copyright of Sophos plc., or, as applicable, its licensors.

You will find copyright information on third party suppliers in the file entitled Disclaimer and Copyright for 3rd Party Software.rtf in your product directory.