

SOPHOS

Sophos SafeGuard Disk Encryption 5.50 Sophos SafeGuard Easy 5.50 User help

Document date: August 2010



Content

1	About Sophos SafeGuard	2
2	Key backup for recovery.....	4
3	Power-on Authentication	5
4	Power-on Authentication under Windows Vista.....	16
5	Logging on to Windows Vista.....	20
6	Logging on with the Lenovo Fingerprint Reader	22
7	Recovery options	31
8	Recovery via Local Self Help.....	32
9	Recovery via Challenge/Response.....	43
10	System Tray icon and balloon tool tip	47
11	SafeGuard Explorer extensions	50
12	Data Encryption	52
13	SafeGuard Data Exchange.....	55
14	Sophos SafeGuard and Lenovo Rescue and Recovery	72
15	Technical support.....	79
16	Copyright	80

1 About Sophos SafeGuard

Sophos SafeGuard is a reliable data security solution that uses a policy-based encryption strategy to provide reliable protection for information on endpoint computers. Data encryption and protection against unauthorized access are the main security functions of Sophos SafeGuard. For end users Sophos SafeGuard is very easy and intuitive to use. The Sophos SafeGuard authentication system, Power-on Authentication (POA), provides powerful access protection and offers user-friendly support when recovering credentials.

Administration is carried out via the SafeGuard Policy Editor which is used to create and manage security policies and to provide recovery functions. A Sophos SafeGuard protected computer receives policies via a configuration package created via the SafeGuard Policy Editor. The configuration package can be distributed via company software mechanisms, or the configuration package is installed manually on the computer.

Note: Sophos SafeGuard is available with different product bundles: SGE (SafeGuard Easy) and ESDP (Endpoint Security and Data Protection). From version 5.50 SGE is the new product name for SafeGuard Enterprise Standalone. For each bundle, different modules and functions are available. The modules and functions not available for ESDP are marked by notes in this manual.

The following modules are available for Sophos SafeGuard protected computers:

■ SafeGuard Device Encryption

Power-on Authentication

User logon is performed immediately after switching on the computer. After successful Power-on Authentication the user will be automatically logged on to the operating system. You can also deactivate Power-on Authentication. In this case user authentication is performed via the operating system.

Volume based encryption

All data on volumes (incl. boot files, swapfiles, idle files/hibernation files, temporary files, directory information etc.) are encrypted transparently without the user having to change the normal operating procedure or consider security.

■ SafeGuard Data Exchange

Note: SafeGuard Data Exchange and SafeGuard Portable are not available with ESDP.

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.

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

1.1 Sophos SafeGuard features

Sophos SafeGuard offers the following features for your convenience:

■ Recovery options in the Power-on Authentication

For recovery (for example, in case you have forgotten your password), Sophos SafeGuard offers the following options:

- If you have forgotten your password, you can use **Local Self Help** to regain access to your computer without the assistance of a helpdesk. To log on to your computer, you simply have to answer a number of predefined questions in the Power-on Authentication. With Local Self Help, you can regain access to your laptop, for example, in situations where neither telephone nor network connections are available (for example aboard an aircraft). For details on Local Self Help, see [Recovery via Local Self Help](#), page 32.
- With **Challenge/Response**, Sophos SafeGuard also offers a help desk assisted recovery mechanism for typical recovery scenarios. Challenge/Response is a secure and efficient recovery system that helps you if you cannot log on to your computer or access encrypted data. For details on Challenge/Response, see [Recovery via Challenge/Response](#), page 43.

■ Sophos SafeGuard System Tray icon

You can access all important functions provided by Sophos SafeGuard via the Sophos SafeGuard System Tray icon. The System Tray Icon is placed on the Windows task bar. For details on the System Tray icon, see [System Tray icon and balloon tool tip](#), page 47.

■ Sophos SafeGuard Explorer extensions

You can access encryption-related functions via corresponding entries in Windows Explorer context menus, see [SafeGuard Explorer extensions](#), page 50.

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

2 Key backup for recovery

For logon recovery, Sophos SafeGuard offers a Challenge/Response procedure (see [Recovery via Challenge/Response](#), page 43) for exchanging information confidentially. The Challenge/Response procedure is very secure and efficient.

To enable recovery via Challenge/Response, the required data has to be available to the help desk. The data required for recovery is saved in specific key recovery files (.XML files).

During the configuration of your computer via the installation of the Sophos SafeGuard configuration package, the key recovery file is created automatically at a location specified by the security officer. If the security officer has not specified a file location, you will be prompted to save the file manually.

The security officer can specify a file location for these files when creating the configuration package. Usually the file location is a shared path. The key recovery file is created automatically at this location.

If the specified file location is not accessible when Sophos SafeGuard tries to create the file, a balloon tip pops up, a message gets written into the system event log and Sophos SafeGuard will try to save the file again later. If the security officer has not specified a file location, a dialog is displayed, prompting you to save the file manually.

If the security officer has specified a network share for the key recovery file and you are logged on to Windows with a local user account (for example, if the computer is not a domain member), you will be prompted for a network share logon. Your security officer should provide you with the required user name and password.

Note: Save the file when prompted and ensure that the help desk has access to it. The file is encrypted and can be saved to any external media to provide them to the helpdesk. You can also send the file via e-mail. If you do not save the file, you will be prompted to do so every time you restart your computer until you have saved it.

You can create a new key backup via the Sophos SafeGuard System Tray icon at any time. Creating a new key recovery file may, for example, be necessary if existing key files have been corrupted or are no longer available to the help desk.

3 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).



3.1 POA look and feel

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

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 Sophos SafeGuard.

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.

3.2 First logon after Sophos SafeGuard installation

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

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 Sophos SafeGuard 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, 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 Windows user name and password.

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

3.3 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 ().

3.3.1 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.

3.3.2 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 43.

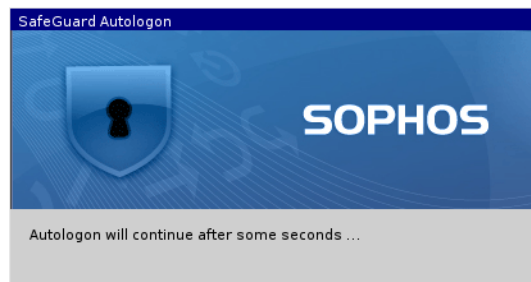
3.3.3 First POA user logon example

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.

1. User 1 (Alice) switches on the XP endpoint computer.

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 endpoint computer, an entry for Alice is created in the Sophos SafeGuard 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.

3.4 Importing further users

Another Windows user (Bob) wants to log on to the endpoint 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. An entry for Bob is created in the Sophos SafeGuard system core.

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

3.5 Temporary password in POA

Sophos SafeGuard 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, Sophos SafeGuard 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.

3.6 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 12).

3.7 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, Sophos SafeGuard adopts the keyboard layout in the POA which is set in Windows' Regional and Language Options for the Windows default user at the time Sophos SafeGuard 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.

3.7.1 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.

3.8 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 Sophos SafeGuard. 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.

3.8.1 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 Sophos SafeGuard 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**.

3.8.2 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 computer 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 22.

3.9 Password synchronization

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

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

Password synchronization will take place in two situations:

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

4 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 5). 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.

4.1 First logon after Sophos SafeGuard installation under Windows Vista

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

When logging on for the first time after installation, you have to log on successfully at Windows as usual using your credentials. Afterwards, you are registered as a Sophos SafeGuard 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, 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).

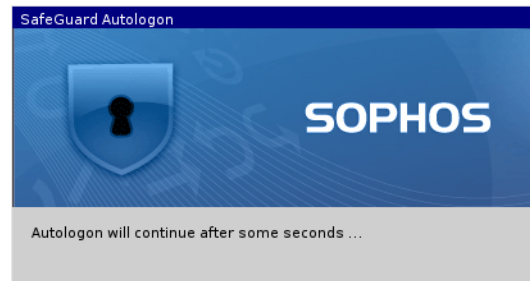
You can log on at the POA via user name and password.

Note: The settings for the endpoint computers on which Sophos SafeGuard is installed are defined by the security officer in the SafeGuard Policy Editor and distributed to the endpoint computers via policy files.

4.1.1 First logon procedure

This section describes the procedure of the first logon to your computer after Sophos SafeGuard 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.

1. The endpoint computer starts, and the Sophos SafeGuard Autologon dialog is displayed.



An autouser is logged on.

2. The Windows Vista logon dialog is displayed.

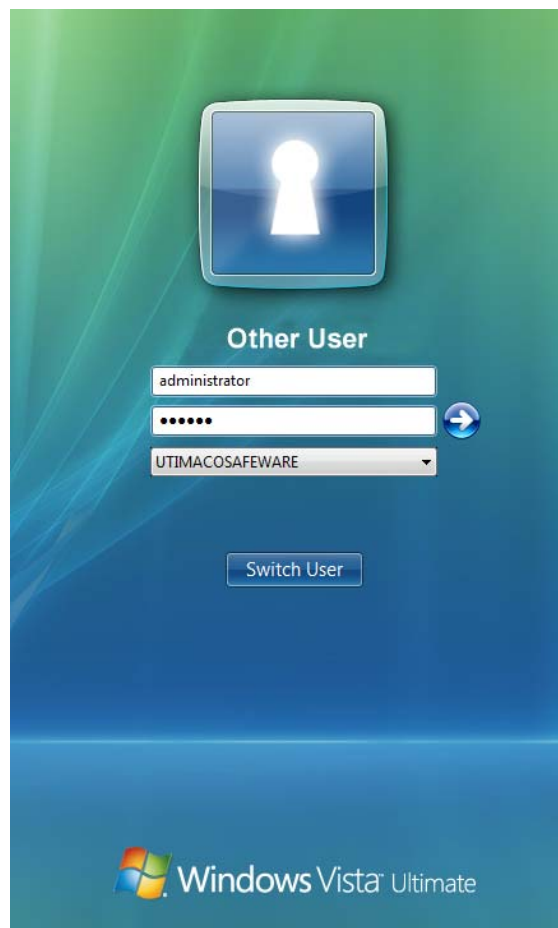


Under Windows Vista, Sophos SafeGuard offers an additional authentication method. The example shows the Sophos SafeGuard authentication method, and the icons for the Vista authentication method.

3. 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 Sophos SafeGuard icon, select the relevant icon. If this is not the case, select the Sophos SafeGuard icon **Other User**.



4. Enter your Windows user credentials as usual.

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.

4.2 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.

4.2.1 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.

4.2.2 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 43.

5 Logging on to Windows Vista

Under Windows Vista, Sophos SafeGuard 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 Sophos SafeGuard is inactive on your computer. In this case, the logon at Sophos SafeGuard is not done during the Windows logon but after the Windows Vista logon.

5.1 Logging on via Sophos SafeGuard

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 Sophos SafeGuard method for logging on to Windows, Sophos SafeGuard 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.

5.2 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 Sophos SafeGuard authentication method.

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

After logging on to Windows Vista, the Sophos SafeGuard 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 Sophos SafeGuard functionality is available and you can, for example, access encrypted data, if you have the necessary key.

5.3 Password synchronization under Windows Vista

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

Password synchronization takes place in two situations:

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

6 Logging on with the Lenovo Fingerprint Reader

Note: This function is not available with ESDP (Endpoint Security and Data Protection).

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.

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.

Sophos SafeGuard 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.
- Remote fingerprint logon is not supported.

6.1 Requirements

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

6.1.1 General requirements

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

6.1.2 System requirements

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

6.1.3 Supported hardware

- AuthenTec AES2810
- UPEK TCS3C/TCD42A

6.1.4 Supported software

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

6.2 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 Sophos SafeGuard 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.

6.3 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 26).

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 28).

6.3.1 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.



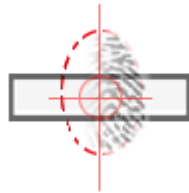
Indicates that the fingerprint was read successfully and a match was found.



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.

6.3.2 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.

6.3.3 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 30).

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.

6.4 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.

6.4.1 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.

6.5 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 Sophos SafeGuard 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 43.

7 Recovery options

For recovery (for example, if you have forgotten your password), Sophos SafeGuard 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 32.

■ 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 43.

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

8 Recovery via Local Self Help

If you have forgotten your password and you cannot contact the help desk for assistance, Sophos SafeGuard 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, Sophos SafeGuard offers the Local Self Help Wizard. You can open the Local Self Help Wizard by clicking the Sophos SafeGuard System Tray icon on the Windows taskbar.

8.1 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 32).

8.2 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 Sophos SafeGuard 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.

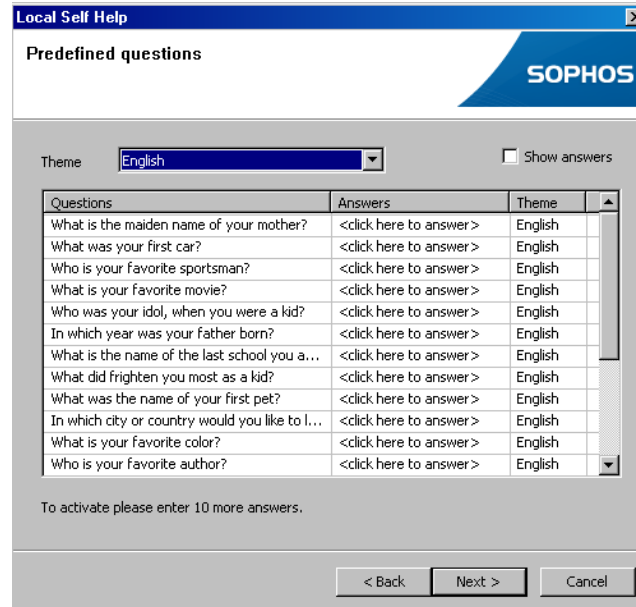
3. Enter your password, and click **Next**.

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.



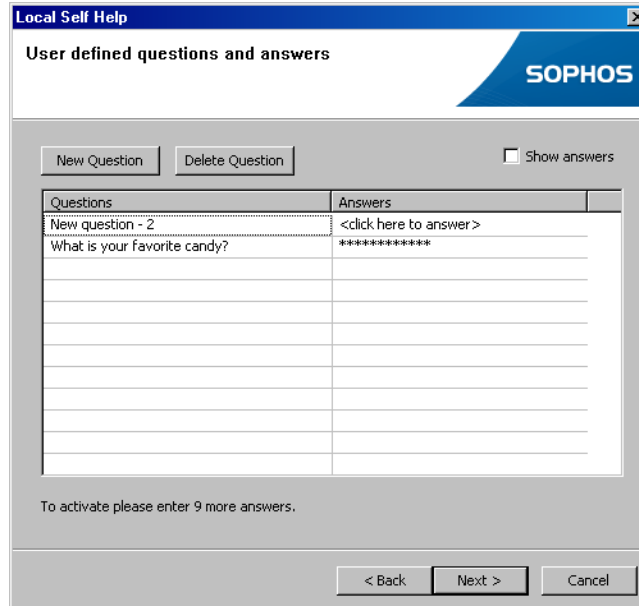
- If you have received several different question themes, you can choose from the question themes displayed in the drop-down list of the **Theme** field.
- To display all themes in a continuous list, select the **All Themes** option (default) from the drop-down list.
- To answer the questions, click 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.



- 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.

8.3 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 Sophos SafeGuard 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 32).

8.4 Changes of 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 may change. For example, 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 your company-specific distribution 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.
Local Self Help parameters have been changed (e.g., minimum length of answers, right to define your own questions) by new policy. Local Self Help has not been disabled. 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.	The Local Self Help Wizard shows a message stating that 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.

8.5 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.



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.

8.6 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.

9 Recovery via Challenge/Response

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

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.

9.1 Prerequisites

A prerequisite for logon recovery via Challenge/Response is that the help desk can access the key recovery file. These files have to be provided to the help desk via shared path, e-mail, or different media.

If you have forgotten your password, another account has to be available on the computer to reset the password. Alternatively, you can use a password reset disk.

The Challenge/Response procedure lets you log on at the Power-on Authentication. You are also allowed to log on to Windows, even if the Windows password needs to be reset.

9.2 You have entered the password incorrectly too often

If you have entered your password incorrectly too often and your computer is locked at POA level, the Challenge/Response procedure enables your computer to boot through the Power-on Authentication. Then, the Windows logon dialog is displayed. You can enter your Windows password in this dialog and you will be logged on.

The counter of the maximum number of password entry attempts allowed is reset.

9.3 You have forgotten your password

When recovering the password via Challenge/Response a password reset is required.

Note: We therefore recommend primarily using Local Self Help to recover a forgotten password. With recovery via Local Self Help you can have the current password displayed 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. For further information, see [Recovery via Local Self Help](#), page 32.

1. Start a Challenge/Response procedure and follow the instructions of the help desk. Your computer will be enabled to boot through the Power-on Authentication.
2. In the Windows logon dialog, you do not know the correct password either and you therefore need to be change it at Windows level. This requires further recovery actions outside the scope of Sophos SafeGuard, via standard Windows means.

There are two possible methods to reset the password at the Windows level.

- Via a service or administrator account available on your computer with the required Windows rights.
- Via a Windows password reset disk.

The help desk officer informs you which procedure should be used, and either provides the additional Windows credentials or the required disk.

3. Enter the new password the help desk has provided at Windows level and immediately change it again to a value that is only known to you.

Sophos SafeGuard detects that the newly chosen password does not match the current Sophos SafeGuard password. You are prompted to enter the old password.

4. If you have changed the Windows password yourself and you still know the old password, you can also perform the password change for Sophos SafeGuard by entering the old password here. If this is not the case, click **Cancel**.

In Sophos SafeGuard, the definition of a new password without providing the old one requires a new certificate. You have to confirm this procedure. A new user certificate will be created based on the newly chosen Windows password. This enables you to log on to the computer again and to log on at the Power-on Authentication with the new password.

5. Log on at the POA with the new password

Note:

Keys for SafeGuard Data Exchange

If you have forgotten the Windows password and it has been reset, you will not be able to use the keys already created for SafeGuard Data Exchange without the corresponding passphrases. To continue using the already-generated user keys for SafeGuard Data Exchange, you have to remember the SafeGuard Data Exchange passphrases needed to reactivate these keys.

Note: Please note that SafeGuard Data Exchange is not available with ESDP (Endpoint Security and Data Protection).

9.4 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 Policy Editor 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 Policy Editor 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.

9.5 The Challenge/Response procedure

The Challenge/Response procedure must be initiated:

- if you have entered the password incorrectly too often.
- if you have forgotten your password.
- to repair a corrupted cache.

Note: 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.

Note: 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.

1. In the POA logon dialog, click **Recovery**.
 - If only Challenge/Response is activated for logon recovery, the Challenge/Response procedure is started.
 - If Challenge/Response and Local Self Help are available for logon recovery, a dialog with both recovery methods is displayed. Click the **Challenge/Response** button to start the Challenge/Response procedure.

A dialog is displayed, indicating the name of the file required for the Challenge/Response procedure.



2. Call your help desk. Tell the help desk officer the name of the file.

3. Click **Next**.

Your user data and a random Challenge code are displayed. To enhance readability, the code is subdivided into blocks of five characters each. (If you need help stating the challenge code, you can click the **Spelling Aid** button).

4. Click **Next**.

The Challenge/Response - Step 3 out of 3 dialog is displayed.

The help desk officer provides you with the response code via phone or SMS.

5. Enter the response code in the input fields of the Challenge/Response - Step 3 out of 3 dialog.

If you have entered the response code incorrectly, the character block containing the error is marked in red.

6. Click **OK**.

You are logged on at the Power-on Authentication.

10 System Tray icon and balloon tool tip

The following functionality is available via the System Tray icon:

- **Show**

- **Key ring**

- Shows all keys available to you.

Note: The Sophos SafeGuard Client uses a defined computer key for volume-based encryption and file-based encryption of drives. This key will *not* be displayed in the dialog. Only keys created locally on the computer will be displayed. If you have not created any keys, none is displayed in the dialog. Note that file-based encryption is not available with ESDP (Endpoint Security and Data Protection).

- **Certificate**

- Shows information concerning your certificate.

- **Create new key**

- Opens a dialog to create a new key that is used for data exchange via removable media.

Note: This function is not available with ESDP.

- **Key backup**

- Using this function, you can create a backup of the key file. This key file is necessary for logon recovery via Challenge/Response.

- **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 4.

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

Field	Information
Last policy receipt	Shows the date and time when the computer has last received a new policy.
Last key receipt	Shows the date and time when the computer has last received a new key.
Last certificate receipt	Shows the date and time when the computer has last received a new certificate
SGN user state	<p>Shows the status of the user who is logged on to the computer (Windows logon):</p> <ul style="list-style-type: none"> ■ Pending The user is being assigned to the Sophos SafeGuard installation as a Sophos SafeGuard user. Please wait until the user data has been processed. Afterwards, the user status will be automatically set to SGN user, i.e., Sophos SafeGuard user. ■ SGN user The user has been assigned to the Sophos SafeGuard installation as a Sophos SafeGuard user. ■ SGN guest The user logged on to Windows is a Sophos SafeGuard guest user. The user is allowed to log on to Windows without being assigned to this Sophos SafeGuard protected computer as a Sophos SafeGuard user. ■ SGN guest (service account) The user logged on to Windows is a Sophos SafeGuard guest user who has logged on using a service account for administrative tasks. ■ Unknown Indicates that the user status could not be determined.
Local Self Help (LSH) State Enabled Active	Indicates whether Local Self Help has been enabled via policy and whether it has been activated by the user on the computer.

- **Help**

Starts the Sophos SafeGuard Online Help.

- **About Sophos SafeGuard**

Shows information about your Sophos SafeGuard version.

The tool tip for the System Tray icon indicates that the computer is a Sophos SafeGuard Client (standalone).

Note: A balloon tool tip indicates successful completion of initial synchronization.

Note: Restart your computer after successful completion of initial synchronization. Only after you restart your computer are all Sophos SafeGuard functions available.

11 SafeGuard Explorer extensions

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

11.1 Explorer extensions for file-based encryption

Note: File-based encryption is not available with ESDP (Endpoint Security and Data Protection).

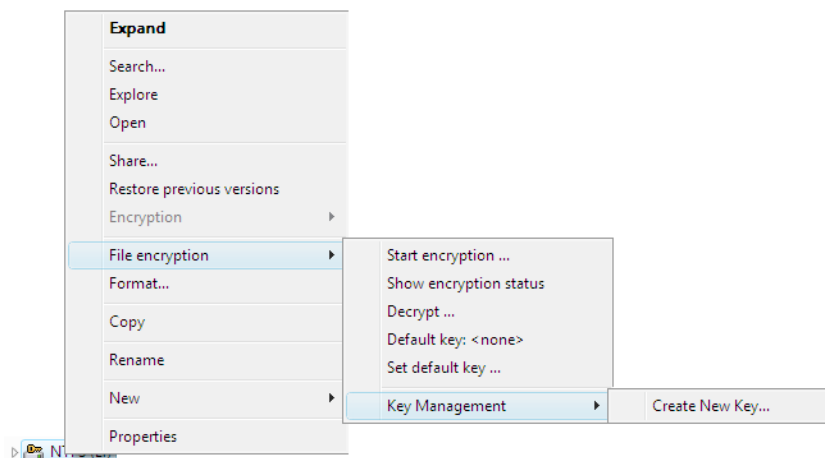
You can access the functions for file-based encryption (see [File based encryption](#), page 53) via the corresponding entries in Windows Explorer context menus. The functions are available in the context menus of

- 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.

11.2 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.

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.

For further information on volume based encryption, see [Volume based encryption](#), page 52.

12 Data Encryption

Sophos SafeGuard 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.

12.1 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.

12.2 Volume based encryption

On a Sophos SafeGuard protected computer, an automatically generated computer key is used for volume based data encryption.

If a policy defining an encryption of this type applies to your computer, the data is encrypted automatically. No further keys can be added to the volume.

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 Sophos SafeGuard.

12.3 File based encryption

Note: File-based encryption is not available with ESDP (Endpoint Security and Data Protection).

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.

For file based encryption keys you create locally will be used. 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** via the Sophos SafeGuard Explorer extensions.
2. Upon encryption start a dialog will be displayed for selection of a local key.
3. If the dialog for key selection does not contain any key, close the dialog and first create one or more keys (**System Tray Icon > Create new key**).
4. Log on to your computer again.

Encryption starts again and the keys are now displayed in the dialog for initial encryption.

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

All data on the relevant volume is encrypted.

12.3.1 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.

12.3.2 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.

12.4 Volume access restrictions

Sophos SafeGuard denies access to volumes in the following cases:

12.4.1 Volumes with failed encryption

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

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

12.4.2 Unidentified File System Objects

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

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.

13 SafeGuard Data Exchange

Note: SafeGuard Data Exchange and SafeGuard Portable are not supported with ESDP (Endpoint Security and Data Protection).

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 defined via policy by the security officer.

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:

- **Sophos SafeGuard 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.
- **Sophos SafeGuard is *not* installed on the recipient's computer:** Sophos SafeGuard 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.

13.1 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 the computers.

A media passphrase makes sense in the following scenarios:

- You want to use encrypted data on removable media also on computers where Sophos SafeGuard 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. 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.

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 be asked to select a key.
- **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

13.1.1 Supported media

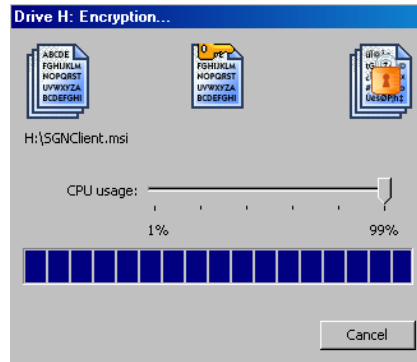
SafeGuard Data Exchange supports the following removable media:

- 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)

13.2 Encrypting removable media

13.2.1 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.
3. If the dialog for key selection does not contain any key, close the dialog and first create one or more keys (**System Tray Icon** > **Create new key**).
4. Click **OK**.
5. All data contained on the removable media is encrypted.

6. 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.

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.

13.2.1.1 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.

13.2.2 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.

13.2.2.1 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.

13.2.2.2 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.

13.2.2.3 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).

13.2.2.4 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.

13.3 Exchanging data using SafeGuard Data Exchange

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

- Exchanging data with Sophos SafeGuard 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 Sophos SafeGuard. 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 Sophos SafeGuard

For users who do not have Sophos SafeGuard 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.

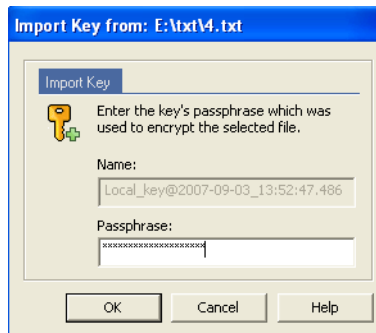
Note: The security officer determines whether SafeGuard Portable is copied to removable media via the security policy that applies to you.

13.3.1 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**.

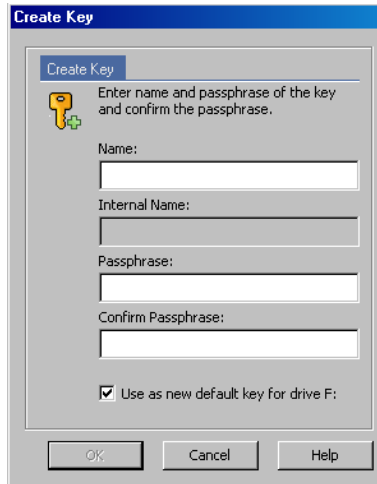


Enter the passphrase in the dialog that is displayed. The key is imported, and you can access the file.

13.3.2 Creating local keys

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

1. Right-click the Sophos SafeGuard 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**.

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.

13.4 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.

13.4.1 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.

13.4.2 Writing files to CD in plain

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

13.4.3 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.

13.4.4 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.

13.5 SafeGuard Portable

Note: SafeGuard Portable is not available with ESDP (Endpoint Security and Data Protection).

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.

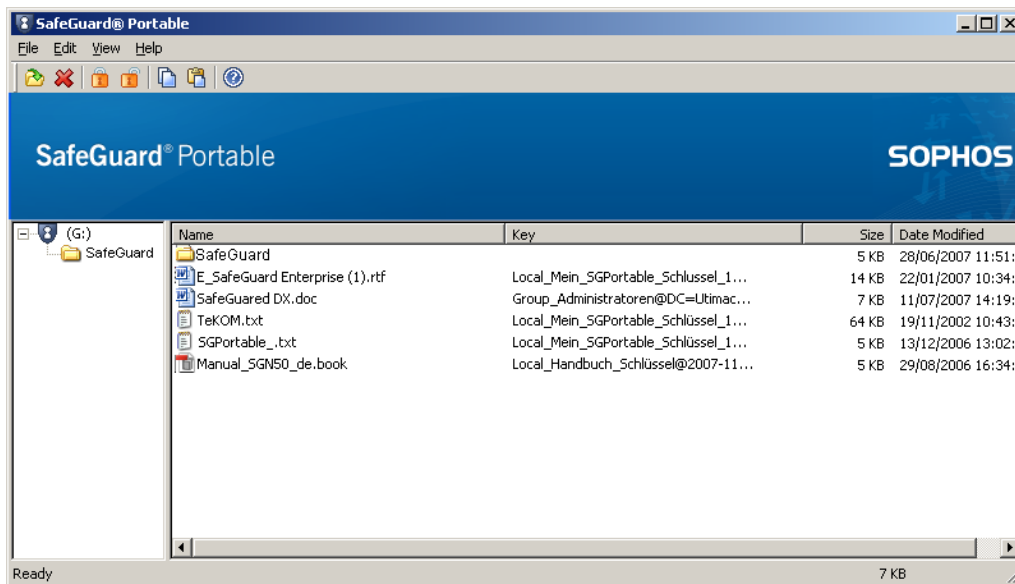
Note: As a Sophos SafeGuard user, you usually do not need SafeGuard Portable. The following description assumes that users do not have Sophos SafeGuard installed on their computer and therefore have to use SafeGuard Portable to edit encrypted data.

13.5.1 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:

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

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

13.5.1.1 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.

13.5.1.2 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.

13.5.1.3 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 again when you close SafeGuard Portable.

13.5.1.4 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.

13.5.1.5 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.

13.5.2 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.

14 Sophos SafeGuard and Lenovo Rescue and Recovery

For information on the Lenovo Rescue and Recovery (RnR) versions supported by Sophos SafeGuard, see the knowledgebase: <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. Sophos SafeGuard 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.

14.1 Overview

Sophos SafeGuard 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 Sophos SafeGuard encrypted operating system partitions. Backups from encrypted Sophos SafeGuard 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.

Sophos SafeGuard 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 Sophos SafeGuard 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.

14.2 Requirements

- Latest BIOS for the PC/notebook.
- For information on compatibility of Rescue and Recovery versions with Sophos SafeGuard versions, see the knowledgebase: <http://www.sophos.com/support/knowledgebase/article/108383.html>
- Lenovo Rescue and Recovery can be used to recover Sophos SafeGuard 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.

14.3 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 Sophos SafeGuard are installed. It is recommended that you install Lenovo Rescue and Recovery first, and Sophos SafeGuard afterwards.

14.3.1 Installing both Rescue and Recovery and Sophos SafeGuard

The following installation sequence is recommended:

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

Sophos SafeGuard 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 Sophos SafeGuard.

14.3.2 Sophos SafeGuard 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 Sophos SafeGuard settings are carried out for the RnR WinPE environment. You must start a Sophos SafeGuard tool named `SetupWinPE.exe` to setup RnR WinPE for use with Sophos SafeGuard. 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.

14.3.3 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 Sophos SafeGuard Device Encryption module (`SGNClient.msi`).

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

14.4 Upgrade

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

14.4.1 Upgrade Sophos SafeGuard

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

14.4.2 Upgrade Rescue and Recovery

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

14.5 Uninstallation

When uninstalling the software products:

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

14.6 Boot environment and recovery options

Sophos SafeGuard 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 Sophos SafeGuard 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: Sophos SafeGuard 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. Sophos SafeGuard will be removed during the restore process. To secure the system again, Sophos SafeGuard must be reinstalled.

14.7 Creating a backup

You create backups using Rescue and Recovery in Windows. On computers on which Rescue and Recovery is already installed, and Sophos SafeGuard 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.

Sophos SafeGuard 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.

14.8 Restoring file backups

Rescue and Recovery can restore files or folders from backups in which Sophos SafeGuard 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.

14.9 Restoring the Sophos SafeGuard system

To restore a system backup that includes Sophos SafeGuard, 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 Sophos SafeGuard credentials.

2. If you do not use a Lenovo computer:

- a) Log in at the POA with your Sophos SafeGuard 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.

14.10 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 Sophos SafeGuard. For further information, refer to the Lenovo documentation.

14.11 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.

15 Technical support

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

- Visit the SophosTalk forum at <http://community.sophos.com/> and search for other users who are experiencing the same problem.
- Visit the Sophos support knowledgebase at <http://www.sophos.com/support/>
- Download the product documentation at <http://www.sophos.com/support/docs/>

Send an email to support@sophos.com, including your Sophos software version number(s), operating system(s) and patch level(s), and the text of any error messages

16 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.