

SOPHOS

simple + secure

Sophos SafeGuard Disk Encryption, Sophos SafeGuard Easy User help

Product version: 5.60

Document date: April 2011



Contents

1 About Sophos SafeGuard.....	3
2 Key backup for recovery.....	5
3 Power-on Authentication.....	6
4 Power-on Authentication under Windows Vista and Windows 7.....	18
5 Logging on to Windows Vista and Windows 7.....	21
6 Logging on with the Lenovo Fingerprint Reader.....	23
7 Recovery options.....	30
8 Recovery with Local Self Help.....	31
9 Recovery with Challenge/Response.....	40
10 System Tray icon and balloon tool tip.....	44
11 Accessing functions via Explorer extensions.....	47
12 Data Encryption.....	49
13 SafeGuard Data Exchange.....	52
14 Sophos SafeGuard and self-encrypting, Opal-compliant hard drives.....	64
15 Sophos SafeGuard and Lenovo Rescue and Recovery.....	65
16 Technical support.....	70
17 Legal notices.....	71

1 About Sophos SafeGuard

Sophos SafeGuard uses a policy-based encryption strategy to protect information on endpoint computers. Data encryption and protection against unauthorized access are its main security functions. 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 with 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 in a configuration package created with the SafeGuard Policy Editor. The configuration package can be distributed with company distribution tools or 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 user help.

The following modules are available for Sophos SafeGuard protected computers:

■ SafeGuard Device Encryption

Power-on Authentication

User logon is performed immediately after you switch on the computer. After successful Power-on Authentication you are automatically logged on to the operating system. You can also deactivate Power-on Authentication. In this case user authentication is performed by the operating system.

Volume-based encryption

All data on volumes (including 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.

SafeGuard Data Exchange offers 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:

Some features described in this user help may not be available on your computer. This is because the features available depend on the policies set by your security officer.

1.1 Sophos SafeGuard features

Sophos SafeGuard offers the following features:

■ Recovery options in the Power-on Authentication

For recovery (for example, if 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 help desk. 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 in situations where neither telephone nor network connections are available (for example aboard an aircraft). For further information, [see *Recovery with Local Self Help*](#) (page 31).

Challenge/Response is a secure and efficient help desk assisted recovery system that helps you if you cannot log on to your computer or access encrypted data. For further information, [see *Recovery with Challenge/Response*](#) (page 40).

■ Sophos SafeGuard System Tray icon

You can access all important functions from the Sophos SafeGuard System Tray icon. The System Tray Icon is in the Windows task bar. For further information, [see *System Tray icon and balloon tool tip*](#) (page 44).

■ Sophos SafeGuard Explorer extensions

You can access encryption-related functions from the corresponding entries in Windows Explorer context menus, [see *Accessing functions via Explorer extensions*](#) (page 47).

Note:

Some features described in this user help may not be available on your computer. This is because the features available depend on the policies set by your security officer.

2 Key backup for recovery

For logon recovery, Sophos SafeGuard offers a Challenge/Response procedure ([see Recovery with Challenge/Response](#) (page 40)) that allows information to be exchanged confidentially.

To enable recovery with 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).

When the Sophos SafeGuard configuration is applied to your computer 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 are 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 is 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 are 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 make sure that the help desk has access to it. The file is encrypted and can be saved to any external media, which you then can provide to the help desk. You can also send the file by e-mail. If you do not save the file, you are prompted to do so every time you restart your computer.

You can create a new key backup from 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

Power-on Authentication (POA) requires you to authenticate before the computer's operating system is started. After you do this, Windows starts and you are logged on automatically. The procedure is the same when the computer is switched back on from hibernation (Suspend to Disk).



POA look and feel

The look and feel of the POA can be customized according to your company's requirements. Your security officer does this in 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 by 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 Sophos SafeGuard is installed. After installation, you can change the POA dialog text by changing the default language in the Windows Regional and Language Options. The dialog text can also be specified by the security officer in a policy.

3.1 First logon after Sophos SafeGuard installation

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

When you log on for the first time after installation, you must first successfully log on to Windows as usual. 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.

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 by using 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 in policy files.

3.2 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 POA logon dialog. You are logged on to Windows automatically.

Note:

You can deactivate the automatic logon to Windows by clicking the **Options >>** button in the logon dialog and deactivating **Pass through to Windows**. Deactivating the automatic logon is, for example, necessary to enable other users to use Power-on Authentication on that computer ([see Import further users](#) (page 8)). 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.

Make sure that you enter characters case-sensitive when logging on at the POA.

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.

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 with Challenge/Response](#) (page 40).

3.2.1 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. Switch on your computer.

The **POA Autologon** dialog is displayed.

2. The Windows logon dialog is then displayed. Log on to Windows.

You are now the "owner". There is one owner per computer. By default, the first user to log on is the owner.

3. If your policies, certificate, and key are all on the endpoint computer, an entry is created for you in the Sophos SafeGuard system core.
4. Once the computer has restarted, you 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.

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

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.

3.3 Import further users

To allow another Windows user to log on to your computer:

1. Switch on the computer.

The POA logon dialog is displayed. The second Windows user cannot log on at the POA because they do not have the necessary keys and certificates.

2. For the second user to log on at the POA, the computer's owner must allow it.

Note: The default setting specifies that the first user to log on after installation is registered as the owner of the computer. The security officer can also define the owner of a computer with a policy setting.

3. In the POA logon dialog, click **Options** and clear the **Pass through Windows** check box.

The Windows logon dialog is displayed, prompting the second user to log on.

4. The second user enters their Windows credentials.
5. An entry for the second user is created in the Sophos SafeGuard system core.

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

3.4 Temporary password in POA

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

Example: You start your notebook in a public place, for example at the airport. You think that somebody watched you enter 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 are automatically prompted to change the temporary password.

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

Note: If you do not enter the existing password before you press **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**.

Note: 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 you do 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 you log on to Windows, Sophos SafeGuard automatically prompts you 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.

3.5 Logging on at the Power-on Authentication using smartcards or tokens

Note:

Token logon is not available with ESDP (Endpoint Security and Data Protection).

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

- Logon is *only allowed with smartcards or tokens*.
- Logon on is *allowed either with user name and password or with smartcard or token*.

The security officer defines the allowed logon type in a policy.

Note: From Sophos SafeGuard's perspective, smartcards and tokens are treated in the same way. So the terms "token" and "smartcard" mean the same in the product and the manual. In the following sections, the term "token" is used.

3.5.1 First token logon after installation

The first logon with a token is identical to the logon procedure without a token.

If a token with your user credentials is available, you can use it to log on to Windows by entering the token PIN.

Note: We recommend that you configure your token with Windows user credentials ([see Store Windows user credentials on your token](#) (page 10)) before you restart the computer. The security policies that apply to you may require using a token at POA. If your token does not contain your credentials, you cannot log on at the Power-on Authentication.

3.5.2 Store Windows user credentials on your token

If your token does not contain your Windows user credentials, you can store them on the token yourself.

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

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

If the system detects an empty token, the **Issue Token** dialog is displayed automatically.

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

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

You are logged on to Windows.

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

To do so, click **Options** in the POA logon dialog and clear the **Pass through to Windows** check box. The Windows logon dialog is displayed, and you can store your credentials on the token as described.

3.5.3 POA logon with token

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

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

The dialog for token logon is displayed.

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

3. Enter your token PIN.

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

3.5.4 Change the PIN

You can change your token PIN in the Windows logon dialog.

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

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

1. In the **PIN** dialog for Windows logon, select the **Change PIN** check box.
2. Enter your token PIN and click **OK**.

The **PIN Change** dialog is displayed.

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

The token PIN is changed and Windows logon continues.

3.5.5 Token logon recovery

If you have forgotten your PIN, you can regain access to your computer with one of the following recovery methods:

- Recovery with Local Self Help, [see *Recovery with Local Self Help*](#) (page 31).
- Recovery with Challenge/Response, [see *Recovery with Challenge/Response*](#) (page 40).

The recovery methods available on your computer depend on the settings specified by the security officer.

To initiate recovery, click the **Recovery** button in the token logon dialog.

3.5.6 Unblock tokens

If you enter your PIN incorrectly several times, your token is blocked. The security officer can configure Sophos SafeGuard to display the **Unblock Token** dialog in this case.

The security officer has to provide you with the administrator PIN defined for your token.

1. In the **Unblock Token** dialog, enter the administrator PIN.
2. Enter a new PIN and confirm it.

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

3. Click **OK**.

The token is unblocked and logon continues.

Note:

If this function is not available on your computer, you can regain access to your computer with Challenge/Response. With Challenge/Response you can regain access to your computer, but you cannot change the PIN or your user credentials.

3.5.7 Remote Desktop Connection

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

Remote capture is not possible in this case.

3.6 Logon recovery

For logon recovery for example, if you have forgotten your password, Sophos SafeGuard offers different options that are tailored to different recovery scenarios. The recovery methods available on your computer depend on the settings specified by the security officer. For further information, [see Recovery options](#) (page 30).

3.7 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 security officer has activated the display of the virtual keyboard by policy.

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 that are used for changing the POA keyboard layout ([see Change the keyboard layout](#) (page 14)).

3.8 Keyboard layout

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

By default, Sophos SafeGuard adopts the keyboard layout which is set in Windows' Regional and Language Options for the Windows default user at the time that 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, you can also use the US keyboard layout (English).

3.8.1 Change the keyboard layout

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

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 restarts of the endpoint computer. If the previous keyboard layout is deselected in the **Regional and Language Options**, it is still maintained unless you select a different one.

Note:

You must also 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 restart 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 by using the mouse or keyboard (**Alt+Shift**).

To see which languages are installed and available on your system, select **Start > Run > regedit: HKEY_USERS\DEFAULT\Keyboard Layout\Preload**.

3.9 Supported hotkeys/function keys in the Power-on Authentication

Certain hardware functionality and settings can lead to problems when starting 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 greylist of hardware settings and functionalities that are known to cause these problems is integrated in the .msi file installed on the computer.

We recommend that you install an updated version of the POA configuration file before 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 you define a customized file, this will be used instead of the one integrated in the .msi file. Only when no POA configuration file is defined or found will the default file 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 <http://www.sophos.com/support/knowledgebase/article/65700.html>.

The Power-on Authentication also supports a number of function keys.

3.9.1 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 - F3	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 startup 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**.

The POA may use the USB keyboard via BIOS SMM. There is 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.

When you change hardware settings by 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**. When you restart your computer, the new settings become active. If you click **No**, your changes are not saved, and the old configuration remains active when you restart your computer.

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

3.9.2 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 start 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** to change to the POA dialog for logging on with a user name and password. For further information on fingerprint logon, [see Logging on with the Lenovo Fingerprint Reader](#) (page 23).

3.10 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 happen if the Windows password has been changed through 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 and Windows 7

The Power-on Authentication for Windows Vista and Windows 7 has the same look and feel and behavior as that for Windows XP. Differences only occur when you log on to the operating system itself.

Note: This section only describes the differences regarding Windows Vista and Windows 7. If differences are not explicitly stated, the procedures/processes described in the Power-on Authentication section apply (*see Power-on Authentication* (page 6)).

4.1 First logon after Sophos SafeGuard installation under Windows Vista and Windows 7

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

Note: Under Windows Vista and Windows 7, 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** (for interactive logon, **Ctrl + Alt + Del** is not required).

When you log on for the first time after installation, you must first log on successfully to 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 by using your 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 in policy files.

4.1.1 First logon procedure

This section describes the procedure for the first logon to your computer after Sophos SafeGuard has been installed. The procedure 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/Windows 7 logon dialog is displayed.
Under Windows Vista/Windows 7, Sophos SafeGuard offers the Sophos SafeGuard and the Windows Vista/Windows 7 authentication method.
3. Windows Vista/Windows 7 provides two icons for each authentication method:
 - Click **Other User** to you open a dialog for entering credentials.
 - Click the second icon (with a user name displayed below it) to 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 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.

You must restart the computer to activate Power-on Authentication fully. After the restart, POA protects your computer against unauthorized access.

4.2 Logging on at the Power-on Authentication under Windows Vista and Windows 7

After successful activation of the Power-on Authentication (initial synchronization and restart), you log on by entering your Windows user credentials in the POA logon dialog. You are 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 computer (*see [Import further users](#) (page 8)*). 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.

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.

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 with Challenge/Response*](#) (page 40).

5 Logging on to Windows Vista and Windows 7

Under Windows Vista and Windows 7, 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/Windows 7 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 Log on with 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 functionality after you log on to Windows Vista or Windows 7.

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

5.2 Log on with the Windows Vista/Windows 7 authentication method

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

If you use the Windows Vista/Windows 7 authentication method, the logon to Sophos SafeGuard is performed after the logon to the operating system.

After logging on to Windows Vista/Windows 7, the Sophos SafeGuard authentication application is started automatically, if necessary, to achieve full Sophos SafeGuard functionality.

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 and Windows 7

Sophos SafeGuard automatically detects when the Windows password has been changed and no longer corresponds to the stored one. This may happen if the Windows password has been changed through 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.

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.

Note:

- 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 fingerprint logon:

General requirements

- Lenovo hardware.
- Lenovo Fingerprint Reader in the notebook or a USB keyboard with a fingerprint reader.
- The latest BIOS (recommended).
- Sophos SafeGuard
- The recommended vendor-specific software version must be installed before Sophos SafeGuard:
 - ThinkVantage Fingerprint for AuthenTec
 - or
 - ThinkVantage Fingerprint for UPEK.
- The security officer must have activated fingerprint logon by policy.

System requirements

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

Supported hardware

For information on supported fingerprint logon hardware, refer to <http://www.sophos.com/support/knowledgebase/article/108789.html>.

Supported software

For information on supported fingerprint software, refer to <http://www.sophos.com/support/knowledgebase/article/111626.html>.

6.2 Enroll 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 fingerprint with your credentials (user name and password).

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

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. Restart your PC/notebook.
4. To test your enrolled fingerprint, swipe your finger over the fingerprint reader after restarting the computer.

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

6.3 Log 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. Restart your computer.

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

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

If the software 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 25)).

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

Note:


- 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, although this does not pass you 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 [Log 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.

	<p>Prompts you to swipe your finger over the fingerprint reader.</p>
---	--

	<p>Indicates that fingerprint logon is not currently enabled. This can occur, for example, if the fingerprint logon module has not yet been initialized.</p>
	<p>Indicates that the fingerprint reader is working and is busy.</p>
	<p>Indicates that the fingerprint was read successfully and a match was found.</p>
	<p>Indicates that the fingerprint was read successfully, but no match was found.</p>
	<p>Indicates that the fingerprint could not be read. Swipe your finger across the fingerprint reader again.</p>
	<p>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.</p>

	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 Log 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.

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.

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 Change your password

1. If a fingerprint logon is enabled in Power-on Authentication, you can change your password in Windows by pressing **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 Synchronize your password

If your Windows password no longer matches the password stored on the fingerprint reader, for example in cases where you changed your password, but the new password was not transferred to the fingerprint reader, you can synchronize your password:

1. Restart your computer.

2. Press the **Esc** key or **Ctrl+Alt+Del** in the POA dialog for logging on with a fingerprint. This switches you to the POA dialog for logging on with a user name and password.
3. Click **Options**, and disable **Pass-through to Windows**.

Note: 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 rejects the password linked to the fingerprint. This is not viewed as a failed logon attempt, however, so no logon delay goes into effect.

A message indicating that the password was changed is displayed, and the system prompts you to enter your current Windows password.

7. Enter the correct Windows password.

Note:

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 Fingerprint logon recovery

If fingerprint logon does not work and you have forgotten the password required to log on, Sophos SafeGuard offers the following recovery methods:

- Recovery with Local Self Help, *see [Recovery with Local Self Help](#)* (page 31).
- Recovery with Challenge/Response, *see [Recovery with Challenge/Response](#)* (page 40).

The recovery methods available on your computer depend on the settings specified by the security officer.

To initiate recovery, click the **Recovery** button in the fingerprint logon dialog.

Note:

Due to a recovery procedure, you may be invited to change your password, when you start your computer, for example, to enable recovery if you have forgotten your password. In this case, the system also offers to update your fingerprint credentials.

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 with 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 help desk. 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 further information, [see *Recovery with Local Self Help*](#) (page 31).

■ Recovery with 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 further information, [see *Recovery with Challenge/Response*](#) (page 40).

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

8 Recovery with 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 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 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. The Local Self Help Wizard helps you provide the initial answers and edit the questions. You can open the Local Self Help Wizard by clicking the Sophos SafeGuard System Tray icon on the Windows taskbar.

Recovery with Local Self Help is available for the following logon methods in the Power-on Authentication:

- Logon with user ID and password
- Logon with fingerprint
- Logon with non-cryptographic token, provided that logon with user ID and password has also been enabled as a possible logon mode by policy.

Note:

Fingerprint and token logon is not available with ESDP (Endpoint Security and Data Protection).

Prerequisites

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

- The security officer has enabled Local Self Help by policy and has defined the settings for this function (for example, the right to define your own questions).
- You have activated Local Self Help on your computer (*see [Activate Local Self Help](#)* (page 31)).

8.1 Activate 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 a predefined number of questions. The security officer specifies how many questions you have to

answer. The Local Self Help Wizard guides you through the process and shows how many answers are required. Depending on the policy settings, these are the possible scenarios:

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

Answer and save the predefined questions received. The Local Self Help Wizard shows, how many answers are required.

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

Answer and save the required number of 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 the required number of questions.

Note: To log on at the Power-on Authentication with Local Self Help, you have to answer questions randomly selected from the questions answered in the Local Self Help Wizard. The security officer specifies how many questions you have to answer in the POA.

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

To activate Local Self Help:

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

The **Local Self Help Wizard Welcome** dialog is displayed.

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

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

The **Status Overview** dialog is displayed.

This dialog tells you how to activate Local Self Help. It also 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 with 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.

8.2 Edit 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.

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 tells you how to activate Local Self Help. It also 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, select 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.

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 [Activate Local Self Help](#) (page 31)*).

8.3 Changes of question parameters

The security officer can define the following parameters that apply to Local Self Help questions:

- The number of questions you have to answer in the Local Self Help Wizard to activate Local Self Help on your computer. The number of questions specified must be available with answers for Local Self Help to remain active.
- The number of questions you have to answer in the POA to log on with Local Self Help. The questions displayed in the POA are selected randomly from the questions you have answered in the Local Self Help Wizard.

If these two parameters change due to a new policy deployed to your computer, the following scenarios may occur:

Condition	LSH action	User action required
The number of questions you have to answer in the LSH Wizard changes, but there are enough questions available for Local Self Help to remain active on your computer.	Local Self Help remains active on your computer.	None
The number of questions you have to answer in the LSH Wizard changes and there are not enough questions available for Local Self Help to remain active on your computer.	A message is displayed stating that your Local Self Help settings have changed. The questions available on your computer are no longer valid. Local Self Help is no longer active on your computer.	To reactivate Local Self Help, open the Local Self Help Wizard and follow the Wizard instructions.

Condition	LSH action	User action required
The number of questions you have to answer in the POA to log on with Local Self Help changes.	A message is displayed stating that your Local Self Help settings have changed. The questions available on your computer remain valid. The ratio between available questions and valid answers has changed.	Open the Local Self Help Wizard and follow the Wizard instructions.

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

Local Self Help parameters may change while you are defining or editing questions in the Local Self Help Wizard. 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 through 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 (for example minimum length of answers, right to define your own questions, the number of questions to be answered) 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 (for example	The Local Self Help Wizard shows a message stating that Local Self Help	To activate Local Self Help, rerun the Local

Condition	LSH Wizard action	Result
minimum length of answers, right to define your own questions, the number of questions to be answered) by a 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.	parameters have changed. Local Self Help will not be active on your computer. You are advised to rerun the wizard. The wizard closes.	Self Help Wizard and define questions and answers again. Afterwards, you can use Local Self Help for logon recovery.

8.5 Log on at the POA with Local Self Help

1. In the POA logon dialog, click the **Recovery** button.
 - 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**.

Note:

If you usually log on to the Power-on Authentication with a PIN or smartcard, you first have to remove the PIN/smartcard from your computer. After that the POA logon dialog for logging on with user name and password is displayed. Enter your user ID and click the **Recovery** button.

Note:

Token logon is not available with ESDP (Endpoint Security and Data Protection).

The **Local Self Help Welcome** dialog is displayed.

This dialog provides a short description of the next steps.

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

The first question is displayed.
3. 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.
4. After answering the question, click **Next**.

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

5. Answer the remaining questions. After answering the last one, click **OK**.

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

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

Note:

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

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

Note:

Make sure that no unauthorized person can view the contents of your screen, by chance or on purpose. You can immediately hide your password by pressing the **Spacebar**, **Enter**, or by clicking the blue display box.

7. You can read the password and use it for logging on at the Power-on Authentication and to Windows again.
8. After reading the password, click **OK**. Otherwise, the startup 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 with Local Self Help again, questions are randomly selected again.

9 Recovery with Challenge/Response

For recovery, Sophos SafeGuard offers a **Challenge/Response procedure** that allows information to be exchanged confidentially.

Note:

We recommend using Local Self Help to recover a forgotten password. Local Self Help allows you to have the current password displayed and to continue using it. This avoids the need to reset the password or to involve the help desk.

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 generates a response code that authorizes you to perform a specific action on your computer.

Recovery with Local Self Help is available for the following logon methods in the Power-on Authentication:

- Logon with user ID and password
- Logon with fingerprint

Note:

Fingerprint logon is not available with ESDP (Endpoint Security and Data Protection).

9.1 Prerequisites

A prerequisite for logon recovery with Challenge/Response is that the help desk can access the key recovery file. These files have to be provided to the help desk by 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 with Challenge/Response, a password reset is required.

Note:

Local Self Help allows you to have the current password displayed and to continue using it. This avoids the need to reset the password or to involve the help desk. For further information, [see *Recovery with Local Self Help*](#) (page 31).

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. You need to change password at Windows level. This requires further recovery actions outside the scope of Sophos SafeGuard using standard Windows means.

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

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

The help desk officer tells 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, you need a new certificate in order to set a new password without providing the old one. 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.

SafeGuard Data Exchange is not available with ESDP (Endpoint Security and Data Protection).

9.4 You cannot access your computer any more

If you cannot access your computer any more, the Power-on Authentication might be corrupted. Even in this critical situation Sophos SafeGuard 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 through a WinPE environment. When encountering such a critical situation, we recommend that you contact your Sophos SafeGuard 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. This means that it will be restored automatically from its backup. In this case, no Challenge/Response procedure is required to repair the local cache. However, logon recovery can be activated by policy, if the local cache is to be repaired explicitly with a Challenge/Response procedure. In this case, you are prompted automatically to initiate a Challenge/Response procedure, if the local cache is corrupted.

Note:

When you generate the challenge, a time period of 30 minutes is available within which to enter the response generated by the help desk. 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. Tell the help desk officer the challenge code. (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 by 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 from 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 with 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 with Challenge/Response.

- **Local Self Help**

- If Local Self Help is activated for your computer in 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, [see *Recovery with Local Self Help*](#) (page 31).

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

Field	Information
Last policy received	Shows the date and time when the computer has last received a new policy.
Last key received	Shows the date and time when the computer has last received a new key.
Last certificate received	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, this means 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 in a 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.

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

11 Accessing functions via Explorer extensions

You can access encryption-related functions from the 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 50)) from 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 from 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 from the context menu.

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

Note: The functions displayed depend on the settings defined in the policies. They also 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 state:** 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 state 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, *see [Volume-based encryption](#)* (page 49).

12 Data Encryption

Sophos SafeGuard encrypts data on a computer either in a volume-based or a file-based manner.

Note:

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

In 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 do not see any prompts for encryption or decryption when opening, editing, and saving files. When you open the files, they are decrypted and you can edit them. When you close or save the files, they will be encrypted again.

If you copy or move files (also with **Save as**) from an encrypted drive to an unencrypted file location on your computer, they are decrypted. The files are stored in the new file location in plaintext.

12.2 Initial encryption

After the first encryption policy has been deployed to your computer, initial encryption is performed according to the policy received. Depending on the encryption policy settings, initial encryption is started automatically or you have to start it manually.

12.3 Volume-based encryption

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

If a policy specifying 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 of the volume to be encrypted. If available, it also shows existing encrypted volumes. The Encryption Viewer is shown in minimized view on the Windows taskbar. You can open it by clicking 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 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.

Note:

If a new policy is applied to your computer that allows decryption, the following applies: After a complete volume-based encryption, you must restart the computer at least once before decryption can be started.

12.4 File-based encryption

Note:

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

If a policy specifying 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** from the Sophos SafeGuard Explorer extensions.
2. When encryption starts, a dialog prompts you to select a local key.
3. If the dialog for key selection does not contain any keys, 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.

12.4.1 Define 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 using the context menu of a file on a volume, or the context menu of the removable storage 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.

12.4.2 Encryption state

On volumes encrypted in a file-based manner, the individual files are marked with 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 has not been encrypted yet.
- **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 from its context menu. By selecting **File encryption > Show Encryption state** you can open a window showing the encryption state.

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

12.5 Volume access restrictions

Sophos SafeGuard denies access to volumes in the following cases:

Volumes with failed encryption

If a policy exists that specifies 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.

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 specifies 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 by ESDP (Endpoint Security and Data Protection).

SafeGuard Data Exchange allows you to encrypt data stored on removable media that are 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 can read the contents of the encrypted data. All subsequent encryption processes are run transparently. Transparent encryption means that 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 in a 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. The security officer can also specify that you are not allowed to access unencrypted files, and they remain unencrypted.

There are two ways to exchange 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 Settings for handling removable media

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 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 on removable media starts 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 are asked to select a key, or a predefined key will be used.
- **You are allowed to cancel initial encryption:** When initial encryption starts, a dialog is displayed that allows you to cancel initial encryption.
- **You are not allowed to access unencrypted data:** In this case, SafeGuard Data Exchange only accepts 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 storage 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 are not be encrypted by SafeGuard Data Exchange.
- **You are allowed to decide about encryption:** When you connect removable media to your computer, a message box is displayed asking you whether you want to encrypt the files on the attached media.

13.2 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 entering only one media passphrase. The media passphrase is bound to the computers.

A media passphrase is useful in the following scenarios:

- You want to use encrypted data on removable media 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.

Supported media

SafeGuard Data Exchange supports the following removable media:

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

13.3 Encrypting removable media

13.3.1 Initial encryption

Encryption of unencrypted data on removable media either starts automatically as soon as you connect the media to the system, or you have to start the process manually. If you are entitled to decide whether files on removable media should be encrypted, you are prompted to do so when you attach removable media to your computer.

To start the encryption process manually:

1. Select **File encryption > Start encryption** from the context menu in Windows Explorer. If no specific key has been defined, a dialog is displayed for key selection.
2. Select a key.

If the dialog for key selection does not contain any keys, close the dialog and first create one or more keys (**System Tray Icon > Create new key**).

3. Click **OK**.

All data contained on the removable media is encrypted.

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.

Initial encryption for users with media passphrase

If the usage of a media passphrase has been defined in a policy, you are prompted to enter the media passphrase before 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.

13.3.2 Transparent encryption

If the settings defined for your computer specify 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 plaintext. If a different encryption policy applies to the new file location, the data is encrypted accordingly.

Media passphrase

If specified by a 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, 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.

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 passphrases 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.

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 your removable media with your computer. This ensures that the new media passphrase is used on all your devices immediately (synchronization).

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 from the context menu of a file on removable media, or from 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 storage 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.

13.4 Exchanging data using SafeGuard Data Exchange

The following are typical examples of secure data exchange with 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 storage 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 storage medium. As SafeGuard Portable is a self-sufficient application, no additional software needs to be installed on the computer in order to access encrypted data.

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

13.4.1 Import 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.

13.4.2 Create local keys

To create a user-defined local key:

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. 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 storage medium from now on is encrypted using this key.

Local keys are not backed up and cannot be used for recovery.

For the recipient to be able to decrypt all data contained on the removable storage medium, you may have to re-encrypt the data on the removable storage 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.

13.5 Writing files to CDs 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 **Statistics**, the following information is displayed:

- how many files are selected to be written to CD
- how many of the selected files are encrypted
- how many of the selected files are plain files

Under **Status**, the keys used for encrypting previously 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.

Encrypt files on CD

If you want to encrypt the files when writing them to CD, click **(Re)Encrypt all files**.

If necessary, previously 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.

Write files to CD in plain

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

Copy SafeGuard Portable to optical media

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

13.5.1 Writing CDs/DVDs with Windows Vista and Windows 7

Windows Vista and Windows 7 provide 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.

13.6 SafeGuard Portable

Note:

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

Using SafeGuard Portable, you can exchange encrypted data on removable media with recipients who do not have SafeGuard Data Exchange installed on their machines. Data encrypted with 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 local key was used for encrypting them. 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 with SafeGuard Data Exchange for encryption, or create a new key with SafeGuard Portable (for example, for new files).

SafeGuard Portable does not have to be installed on or copied to your communication partner's computer. 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.

13.6.1 Edit 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 **SGPortable.exe**.

Using SafeGuard Portable, you can decrypt the encrypted data 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 key used is displayed.

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

- To edit files on the removable media, select the file with a left-click, and choose the relevant command from the context menu (with 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 with 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. 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** with the icons shown on the toolbar.

13.6.1.1 Set encryption keys

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

- From the context menu or from the **File** menu, select **Set Encryption Key**.

The **Enter Key** dialog is displayed.

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

The passphrase has to correspond to the company policies. If it does not, a warning message is displayed.

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

13.6.1.2 Encrypt files 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 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.

13.6.1.3 Decrypt files 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 local 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.

13.6.1.4 Encrypt new files using SafeGuard Portable

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

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

13.6.1.5 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.

13.6.2 Other operations using SafeGuard Portable

The following operations are also available:

- **Open:** This menu command is only available from the SafeGuard Portable **File** menu.
When you open 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 self-encrypting, Opal-compliant hard drives

Self-encrypting hard drives offer hardware-based encryption of data when they are written to the hard disk. The Trusted Computing Group (TCG) has published the vendor-independent Opal standard for self-encrypting hard drives. Different hardware vendors offer Opal-compliant hard drives. Sophos SafeGuard supports the Opal standard.

14.1 Encryption of Opal-compliant hard drives

Opal-compliant hard drives are self-encrypting. Data are encrypted automatically when they are written to the hard disk.

Opal-compliant hard drives are locked by an AES 128/256 key used as an Opal password. This password is managed by Sophos SafeGuard through an encryption policy. Your security officer defines this encryption policy in the SafeGuard Policy Editor and deploys it to your computer.

14.2 System Tray Icon and Explorer extensions on endpoint computers with Opal-compliant hard drives

When Sophos SafeGuard is installed on your computer, the Sophos SafeGuard product icon is displayed in the system tray of the computer taskbar. You can centrally access all important functions provided by Sophos SafeGuard on your computer. Note that the features available depend on the settings defined by the security officer.

If the security officer has enabled you by policy to decrypt Opal-compliant hard drives, the Sophos SafeGuard **Decrypt** command is available in the Windows Explorer context menu.

15 Sophos SafeGuard and Lenovo Rescue and Recovery

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

You can restore complete operating system backups on an encrypted partition without decrypting the hard disk first. This saves 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 starts, Rescue and Recovery saves data through an emergency environment (WinPE). You can access the rescue tools from the Microsoft Windows Desktop or by pressing the blue "ThinkVantage" key integrated in Lenovo systems.

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

15.1 Overview

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:

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

15.2 Requirements

- Latest BIOS for the PC/notebook.
- For information on compatibility of Rescue and Recovery versions with Sophos SafeGuard versions, see: <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.

15.3 Installation

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

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

In the sections that follow, note the sequence in which Rescue and Recovery and Sophos SafeGuard are installed. We recommend that you install Lenovo Rescue and Recovery first, and Sophos SafeGuard afterwards.

15.3.1 Install 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.

15.3.2 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).

15.4 Upgrade

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

Upgrade Sophos SafeGuard

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

15.5 Uninstallation

When uninstalling the software products:

- We recommend 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, start 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.

15.6 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 Rescue and Recovery is started 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.

15.7 Creating a backup

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

15.8 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 restart your machine after the restore is completed, you can work with your files immediately.

15.9 Restore 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 startup 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 starting up, press **F11** to start the Rescue and Recovery environment.

The user interface for Rescue and Recovery is displayed. The welcome screen is displayed.
3. Click **Next**.
4. On the left-hand side menu, select **Restore Backup**.

A dialog is displayed in which you can select the backup.
5. Select the backup and restore it.

15.10 Service and factory recovery partitions

Lenovo supplies new computers with special pre-installed partitions:

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

These partitions are visible in Windows under separate drive letters.

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

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

15.11 Disabled POA and Lenovo Rescue and Recovery

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

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

16 Technical support

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

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

17 Legal notices

Copyright © 1996 - 2011 Sophos Group. All rights reserved. SafeGuard is a registered trademark of Sophos Group.

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

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

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