## Contents

1 About Sophos SafeGuard..........................................................................................................................3

2 Security best practices ..............................................................................................................................4

3 Power-on Authentication...........................................................................................................................6

4 Power-on Authentication under Windows Vista and Windows 7........................................................13

5 Logging on to Windows Vista and Windows 7......................................................................................16

6 Logging on with the Lenovo Fingerprint Reader..................................................................................18

7 System Tray icon and balloon tool tip...................................................................................................25

8 Remove users from POA.........................................................................................................................27

9 Accessing functions via Explorer extensions.........................................................................................28

10 Data Encryption....................................................................................................................................29

11 Sophos SafeGuard and self-encrypting, Opal-compliant hard drives................................................31

12 Recovery options...................................................................................................................................32

13 Recovery with Local Self Help..............................................................................................................33

14 Recovery with Challenge/Response......................................................................................................41

15 Technical support..................................................................................................................................45

16 Legal notices..........................................................................................................................................46
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. The Sophos SafeGuard authentication system, Power-on Authentication (POA), provides powerful access protection and offers user-friendly support when recovering credentials.

1.1 Sophos SafeGuard features

Sophos SafeGuard offers the following features:

■ **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.

■ **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 33).

**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 41).

■ **Full disk 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.

■ **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 25).
2 Security best practices

By following the simple steps described here, you can keep data on your computer secure and protected at all times.

**Shut down or hibernate your computer when it is not in use.**

On Sophos Disk Encryption protected computers, encryption keys might be accessible to attackers in certain sleep modes where the computer’s operating system is not shut down properly and background processes are not terminated. Protection is enhanced when the operating system is always shut down or hibernated properly.

When your computer is not in use or left unattended:

- Avoid sleep (stand-by/suspend) mode. On Windows Vista and Windows 7, also avoid Hybrid sleep mode. Hybrid sleep mode combines hibernation and sleep.
- Do not lock the desktop and then switch off your monitor or only close the lid of your mobile computer as modes of protection when not followed by a proper shut down or hibernation. Setting an additional password prompt after resume does not provide sufficient protection.
- Instead, shut the computer down properly or put it into hibernation mode.

*Note:* It is important that the hibernation file resides on an encrypted drive. Typically it resides on C:.  

Follow these steps in particular when you use a computer in public locations like airports.  

When the computer is hibernated or shut down properly, Power-on Authentication is always activated when it is used the next time, thus providing full protection.

**Choose strong passwords.**

Strong passwords are a vital part of protecting your data. Use strong passwords, especially for securing the logon to your computer.

A strong password follows these rules:

- It is long enough to be secure: minimum 10 characters.
- It contains a combination of letters (upper and lower case), numbers and special characters/symbols.
- It does not contain a commonly used word or name.
- It is hard to guess but easy for you to remember and type accurately.

Change your passwords at regular intervals. Do not share them with anyone nor write them down.

**Ensure that all drives have a drive letter assigned.**

Only drives that have a drive letter assigned are considered for disk encryption. Consequently, drives without a drive letter assigned may be abused to leak confidential data in plain text.
To mitigate this threat:

- Do not change drive letter assignments.
- If you find a drive without a drive letter assigned on your computer, contact your system administrator.
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).

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. 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.

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 SEC administrator, 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.
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 7)).

**Note:**

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

When entering credentials at the POA in Japanese, you have to use Romaji (Roman) characters to successfully log on at the POA. Your Windows credentials must consist of Romaji characters.

**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**

Your computer will be locked after 16 failed logon attempts. To unlock your computer, initiate a Challenge/Response procedure, see **Recovery with Challenge/Response** (page 41).

### 3.2.1 First POA 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.
   
   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.

### 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. Enter your POA credentials.
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 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 SEC administrator. For further information, see Recovery options (page 32).

3.6 Virtual keyboard

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

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 10)).

3.7 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).
3.7.1 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.

3.8 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 file of hardware settings and functionalities (POA configuration file) that are known to cause these problems is installed with the encryption software on the computer.

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

For further information, see: http://www.sophos.com/support/knowledgebase/article/117142.html

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

3.8.1 Hotkeys

Shift-F3 = USB Legacy Support (on/off)
**Shift-F4** = VESA graphic mode (off/on)
**Shift-F5** = USB 1.x and 2.0 support (off/on)
**Shift-F6** = ATA Controller (off/on)
**Shift-F7** = USB 2.0 support only (off/on) USB 1.x support remains as set by **Shift-F5**.
**Shift-F9** = ACPI/APIC (off/on)

Hotkeys dependency matrix

<table>
<thead>
<tr>
<th>Shift - F3</th>
<th>Shift - F3</th>
<th>Shift - F7</th>
<th>Legacy</th>
<th>USB 1.x</th>
<th>USB 2.0</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>off</td>
<td>off</td>
<td>off</td>
<td>on</td>
<td>on</td>
<td>on</td>
<td>3.</td>
</tr>
<tr>
<td>on</td>
<td>off</td>
<td>off</td>
<td>off</td>
<td>on</td>
<td>on</td>
<td>Default</td>
</tr>
<tr>
<td>off</td>
<td>on</td>
<td>off</td>
<td>on</td>
<td>off</td>
<td>off</td>
<td>1., 2.</td>
</tr>
<tr>
<td>on</td>
<td>on</td>
<td>off</td>
<td>on</td>
<td>off</td>
<td>off</td>
<td>1., 2.</td>
</tr>
<tr>
<td>off</td>
<td>off</td>
<td>on</td>
<td>on</td>
<td>on</td>
<td>off</td>
<td>3.</td>
</tr>
<tr>
<td>on</td>
<td>off</td>
<td>on</td>
<td>off</td>
<td>on</td>
<td>off</td>
<td></td>
</tr>
<tr>
<td>off</td>
<td>on</td>
<td>on</td>
<td>on</td>
<td>off</td>
<td>off</td>
<td></td>
</tr>
<tr>
<td>on</td>
<td>on</td>
<td>on</td>
<td>on</td>
<td>off</td>
<td>off</td>
<td>2.</td>
</tr>
</tbody>
</table>

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.

### 3.8.2 Function keys in the logon dialog

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

- **F2** = abort Autologon.
- **F5** = displays a dialog showing the hotkey configuration used to 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 18).

### 3.9 Password synchronization

Sophos SafeGuard automatically detects when the Windows password has been changed and no longer corresponds to the one stored in the Sophos SafeGuard database. This may 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 SEC administrator 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.

3. Windows Vista/Windows 7 provides two icons for each authentication method:
   ■ Click Other User to 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 7)).
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

Your computer will be locked after 16 failed logon attempts. To unlock your computer, initiate a Challenge/Response procedure, see *Recovery with Challenge/Response* (page 41).
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.

A dialog for entering user credentials is displayed.

1. Enter your credentials 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

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 SEC administrator must have activated fingerprint logon by policy.

**System requirements**

- Windows XP, 32 bit
- Windows Vista, 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 SEC administrator 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 20)).

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.

### 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.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Prompt Icon" /></td>
<td>Prompts you to swipe your finger over the fingerprint reader.</td>
</tr>
<tr>
<td><img src="image" alt="Not Enabled Icon" /></td>
<td>Indicates that fingerprint logon is not currently enabled. This can occur, for example, if the fingerprint logon module has not yet been initialized.</td>
</tr>
<tr>
<td><img src="image" alt="Busy Icon" /></td>
<td>Indicates that the fingerprint reader is working and is busy.</td>
</tr>
<tr>
<td>Image</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td><img src="image" alt="Checkmark" /></td>
<td>Indicates that the fingerprint was read successfully and a match was found.</td>
</tr>
<tr>
<td><img src="image" alt="X" /></td>
<td>Indicates that the fingerprint was read successfully, but no match was found.</td>
</tr>
<tr>
<td><img src="image" alt="Question Mark" /></td>
<td>Indicates that the fingerprint could not be read. Swipe your finger across the fingerprint reader again.</td>
</tr>
<tr>
<td><img src="image" alt="Left Arrow" /></td>
<td>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.</td>
</tr>
<tr>
<td><img src="image" alt="Skewed" /></td>
<td>Indicates that your finger swipe was too skewed. Swipe your finger across the fingerprint reader again.</td>
</tr>
<tr>
<td><img src="image" alt="Fast" /></td>
<td>Indicates that you moved your finger too fast. Swipe your finger across the fingerprint reader again.</td>
</tr>
</tbody>
</table>
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.
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 33).
- Recovery with Challenge/Response, see *Recovery with Challenge/Response* (page 41).

The recovery methods available on your computer depend on the settings specified by the SEC administrator.

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 System Tray icon and balloon tool tip

The following functionality is available from the System Tray icon:

- **Show**
  - **Certificate**
  
  Shows information concerning your certificate.

- **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 33).

- **User Machine Assignments**

  Shows a list of users who can log on at the Power-on Authentication. In the dialog displayed, users can be removed from the list. After users have been removed, they can no longer log on at the Power-on Authentication.

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last policy received</td>
<td>Shows the date and time when the computer has last received a new policy.</td>
</tr>
<tr>
<td>Last key received</td>
<td>Shows the date and time when the computer has last received a new key.</td>
</tr>
<tr>
<td>Last certificate received</td>
<td>Shows the date and time when the computer has last received a new certificate.</td>
</tr>
<tr>
<td>SGN user state</td>
<td>Shows the status of the user who is logged on to the computer (Windows logon):</td>
</tr>
</tbody>
</table>
  - **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 after installation and before Power-on Authentication is activated.

- **Unknown**
  Indicates that the user status could not be determined.

<table>
<thead>
<tr>
<th>Local Self Help (LSH) State</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Indicates whether Local Self Help has been enabled in a policy and whether it has been activated by the user on the computer.</td>
</tr>
<tr>
<td>Active</td>
<td></td>
</tr>
</tbody>
</table>

- **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.

**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.
8 Remove users from POA

As an SGN user or as an SGN guest with a service account, you can remove other SGN users. A SGN guest user can carry out administrative tasks after installation before Power-on Authentication is activated.

After you have removed an SGN user they can no longer log on at the Power-on Authentication.

All SGN users are managed in a list called "User Machine Assignment".

Note:

The user currently logged on and the last user in the list cannot be removed.

To remove an SGN user:

1. Right-click the System Tray Icon.
2. From the context menu of the System Tray Icon, select User Machine Assignments. The User Machine Assignments dialog shows all users who can log on at the Power-on Authentication.
3. Select a user and click Remove selected user.
4. Click OK.

The user can no longer log on at the Power-on Authentication.
9 Accessing functions via Explorer extensions

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

9.1 Explorer extensions for full disk 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.
10 Data Encryption

Sophos SafeGuard encrypts data on a computer with full disk encryption.

The SEC administrator defines the volumes (drives) that are to be encrypted.

10.1 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.

10.2 Initial encryption

After the first encryption policy has been deployed to your computer, initial encryption is performed according to the policy received.

Initial encryption runs in the background and you can continue working with your computer.

Note: During initial encryption of the system partition (i.e. the partition, where the hiberfil.sys file is located) do not hibernate the computer. After initial encryption of the system partition is completed, restart the computer to make sure that hibernation works properly again.

10.3 Full disk encryption

On a Sophos SafeGuard protected computer, an automatically generated computer key is used for full disk encryption.

If a policy specifying encryption applies to your computer, the data is encrypted automatically.

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.
10.4 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 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 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.
11 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.

11.1 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 SEC administrator defines this encryption policy and deploys it to your computer.
12 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 33).

- **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 41).

Both recovery options are enabled for use on your computer by the SEC administrator in policies.
13 Recovery with Local Self Help

If you have forgotten your password, Sophos SafeGuard offers Local Self Help. Using Local Self Help you can regain access to your computer without the assistance of the help desk.

You can log on to your computer by answering a specified number of predefined questions in the Power-on Authentication.

If you are entitled by policy, you can define your own questions. 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

Prerequisites

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

- The SEC administrator 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 33)).

13.1 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 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).
**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 SEC administrator 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 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**.
   
   The **Predefined questions** dialog is displayed.

5. 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.

6. After you have finished answering the predefined questions, click **Next**.
   
   If you are entitled to define your own questions, the **User defined questions and answers** dialog is displayed.

7. In the **User defined questions and answers** dialog, you can add your own questions:
   
   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. 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.

8. 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. A message indicates whether the prerequisites for activating Local Self Help have been met.

9. Click Finish.

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

10. 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 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.

13.2 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**.

   The **Predefined Questions** dialog is displayed, containing the answered questions. By default, the answers are not shown as text.

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

6. To change the answers, click the relevant questions and enter your new answer in the **Answers** column.

7. 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.

8. 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**.

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

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

10. 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.

11. 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 33)).

13.3 Changes of question parameters

The SEC administrator 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:

<table>
<thead>
<tr>
<th>Condition</th>
<th>LSH action</th>
<th>User action required</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td>Local Self Help remains active on your computer.</td>
<td>None</td>
</tr>
<tr>
<td>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.</td>
<td>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.</td>
<td>To reactivate Local Self Help, open the Local Self Help Wizard and follow the Wizard instructions.</td>
</tr>
</tbody>
</table>
Open the Local Self Help Wizard and follow the Wizard instructions.

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.

### 13.4 Changes of conditions and 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 may be transferred to your computer.

If such changes occur during the editing process, 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:

<table>
<thead>
<tr>
<th>Condition</th>
<th>LSH Wizard action</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Self Help has been disabled globally by a new policy.</td>
<td>The Local Self Help Wizard shows a message stating that Local Self Help has been disabled globally and closes.</td>
<td>Local Self Help can no longer be used.</td>
</tr>
<tr>
<td>Local Self Help parameters have been changed (for example the 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 sufficient for Local Self Help on your computer.</td>
<td>The Local Self Help Wizard shows a message stating that Local Self Help parameters have changed, saves your changes and closes.</td>
<td>Local Self Help is active on your computer and can be used for logon recovery.</td>
</tr>
<tr>
<td>Local Self Help parameters have been changed (for example the right to define your own questions, the number of questions to be answered) by a new policy. Local Self Help has</td>
<td>The Local Self Help Wizard shows a message stating that Local Self Help parameters have changed. Local Self Help will not be active on your computer. You are advised to rerun the wizard. The wizard closes.</td>
<td>To activate Local Self Help, rerun the Local Self Help Wizard and define questions and answers again.</td>
</tr>
<tr>
<td>Condition</td>
<td>LSH Wizard action</td>
<td>Result</td>
</tr>
<tr>
<td>--------------------------------------------------------------------------</td>
<td>----------------------------------------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td>not been disabled. However, there are not enough questions for Local Self Help to be active on your computer.</td>
<td></td>
<td>Afterwards, you can use Local Self Help for logon recovery.</td>
</tr>
</tbody>
</table>

**13.5 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**.

   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.

### 13.6 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.
14 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 Challenge/Response is available for the following logon methods in the Power-on Authentication:
- Logon with user ID and password
- Logon with fingerprint

**Note:** Challenge/Response cannot be used to allow a computer to be booted from external media. The option **Continue Booting from ... Floppy Disk/External Media** in the POA logon dialog has no effect. If you want to start the computer from external media, use the boot option provided in the BIOS. The BIOS default option already is to boot from CD/DVD when one is inserted.

14.1 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.

14.2 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.
14.3 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 33).

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.

14.4 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.

14.5 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.
15 Technical support

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

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

Copyright © 1996 - 2012 Sophos Group. All rights reserved. SafeGuard is a registered trademark of Sophos Group.

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 license terms or you otherwise have the prior permission in writing of the copyright owner.

Sophos, Sophos Anti-Virus and SafeGuard are registered trademarks 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.

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