

SOPHOS

simple + secure

Sophos SafeGuard Disk Encryption, Sophos SafeGuard Easy **Startup guide**

Product version: 5.60

Document date: April 2011



Contents

1 About this guide.....	3
2 About Sophos SafeGuard.....	4
3 Can I upgrade from earlier versions?.....	6
4 What do I install?.....	7
5 What are the key steps?.....	8
6 Install SafeGuard Policy Editor.....	9
7 Carry out first-time configuration.....	10
8 Copy of the default policy for editing.....	12
9 Configure endpoint computers for post-installation service tasks	13
10 Publish the policy into a configuration package.....	14
11 Install encryption software and configuration package on endpoint computers.....	15
12 Recover a forgotten password.....	22
13 Get help with common tasks.....	24
14 Technical support.....	25
15 Legal notices.....	26

1 About this guide

This guide tells you how to set up Sophos SafeGuard to protect your company's computers against unauthorized access.

It is valid for the following products:

- Sophos SafeGuard Disk Encryption (SDE) 5.6x available with the Endpoint Security and Data Protection (ESDP) bundle.
- Sophos SafeGuard Easy (SGE) 5.6x. From version 5.50, SGE is the new product name for the SafeGuard Enterprise Standalone solution.

Whenever features or settings differ between the two products, this is stated in this guide.

Additional information is available in the SDE/SGE Administrator Help and SDE/SGE User Help.

2 About Sophos SafeGuard

Sophos SafeGuard encrypts data transparently: users do not need to decide which data is to be encrypted. Encryption and decryption is performed in the background. Encryption effectively prevents data from being read or changed by unauthorized persons. Sophos SafeGuard encryption cannot be bypassed by connecting storage media to another system.

Sophos SafeGuard lets you:

- Implement quickly.
- Protect the confidentiality of data.
- Encrypts data using technology that is FIPS 140 compliant.

Computers protected by Sophos SafeGuard run the SafeGuard Power-on Authentication (POA) in the pre-boot phase of the computer, before the operating system starts. After the user has been properly authenticated at the POA, the operating system starts and the user is logged on to Windows.



The POA provides highly secure and user friendly features such as:

- Tamper protection for Sophos SafeGuard Disk Encryption.
- Logon delays on false entries.
- Customizable Windows-like graphical user interface.
- Passthrough to Windows.
- Multiple language and unicode support.

Convenient access for IT operations

Sophos SafeGuard offers several features that aid IT operations on endpoint computers:

- The Power-on Authentication can be configured for use with Wake on LAN, for example to facilitate patch management.
- Service accounts enable members of the IT team to log on to endpoint computers for post-installation tasks without activating the Power-on Authentication.

- POA access accounts enable members of the IT team to log on to encrypted endpoint computers for administrative tasks after the Power-on Authentication has been activated.

Recovery scenarios in Sophos SafeGuard

For recovery, Sophos SafeGuard offers different options that are tailored to different recovery scenarios:

■ Logon recovery using Local Self Help

Local Self Help enables users who have forgotten their password to log on to their computers without the assistance of a help desk. Even in situations where neither telephone nor network connections are available (for example aboard an aircraft), users can regain access to their computers. To log on, they answer a predefined number of questions in the Power-on Authentication.

Local Self Help reduces the number of calls concerning logon recovery, thus freeing the help desk staff from routine tasks and allowing them to concentrate on more complex support requests.

■ Recovery using Challenge/Response

The Challenge/Response recovery mechanism involves the assistance of the help desk. It helps users who cannot log on to their computers or access encrypted data. During the Challenge/Response procedure, the user provides a challenge code generated on the endpoint computer to the help desk officer who in turn generates a response code that authorizes the user to perform a specific action on the computer. With recovery through Challenge/Response, Sophos SafeGuard offers different workflows for typical recovery scenarios requiring help desk assistance.

■ System recovery

Sophos SafeGuard offers different methods and tools for system recovery, such as a Sophos SafeGuard customized Windows PE and Lenovo Rescue and Recovery. Problems with Windows system and Sophos SafeGuard components can be addressed using these tools.

Recovery is based on a key recovery file created for each Sophos SafeGuard encrypted computer and typically stored on a network share. This recovery key ensures that the recovery process is not exploited to bypass data protection and is encrypted for additional security. The network share for storing these files well as the required access rights to this share are automatically created during first-time configuration.

3 Can I upgrade from earlier versions?

There are significant enhancements available within Sophos SafeGuard 5.6x.

■ Upgrade from version 5.5x:

Computers that have already been encrypted with SDE 5.5x or SGE 5.5x can be upgraded to version 5.6x.

■ Upgrade from version 4.x:

Computers that have been encrypted with SDE 4.6x or SGE 4.3x to 4.5x can be upgraded to Sophos SafeGuard 5.6x.

From version 5.5x, Sophos SafeGuard uses a different administration tool, SafeGuard Policy Editor, which is not backward compatible with SDE 4.x or SGE 4.x. Encrypted volumes remain encrypted and the encryption keys are converted to a format compatible with version 5.5x.

With Sophos SafeGuard 5.6x, a valid licence file is required that needs to be imported into SafeGuard Policy Editor. You receive the file from your sales partner.

Before upgrading to Sophos SafeGuard 5.6x, a new configuration package should be created using SafeGuard Policy Editor and deployed alongside the Sophos SafeGuard 5.6x software.

For further information, see the Administrator Help, chapter *Upgrading SafeGuard Easy 4.x/ Sophos SafeGuard Disk Encryption 4.x to Sophos SafeGuard 5.6x* and see <http://www.sophos.com/support/knowledgebase/article/108561.html>.

4 What do I install?

You install the following components:

- SafeGuard Policy Editor. This is the Sophos SafeGuard management tool. It enables you to manage encryption software on endpoint computers and to carry out recovery tasks.

Microsoft SQL Server 2005 Express used to store Sophos SafeGuard policy settings is automatically installed during the SafeGuard Policy Editor setup if an SQL server instance is unavailable.

Note:

First install the SafeGuard Policy Editor on a Windows server. Later, you can install it on multiple administrator computers, all connecting to the central Sophos SafeGuard database on the server.

- Sophos SafeGuard encryption software. This encrypts data on endpoint computers and protects them from unauthorized access.

Note:

We recommend that you do not install the encryption software on the administrator computer used for Sophos SafeGuard management.

5 What are the key steps?

You carry out these steps:

- Install SafeGuard Policy Editor.
- Carry out first-time configuration creating a default policy and important requirements for help desk tasks.
- Copy the default policy for editing.
- Configure the endpoint computer for post-installation service tasks.
- Publish the edited policy into a configuration package.
- Install the encryption software and configuration package on the endpoint computers.

6 Install SafeGuard Policy Editor

Before you start:

- Check if .NET Framework 3.0 Service Pack 1 is installed on the computer where you want to install SafeGuard Policy Editor. You can download it for free from:
<http://www.microsoft.com/downloads>.
- Check the system requirements:
<http://www.sophos.com/support/knowledgebase/article/112891.html>.
- Make sure that you have Windows administrator rights.

To install SafeGuard Policy Editor:

1. Log on to your computer as an administrator.
2. Using the web address and download credentials provided by your system administrator, go to the Sophos website and download the installers.
3. From the product's install folder, double-click one of the following, depending on your product. A wizard guides you through the necessary steps.

Sophos SafeGuard Disk Encryption	SafeGuard Easy
SDEPolicyEditor.msi.	SGNPolicyEditor.msi.

4. Accept the defaults on the subsequent dialogs.

If prompted to install Microsoft SQL Server 2005 Express, click **Yes**. In this case, your Windows credentials are used for the SQL user account.

5. Click **Finish** to complete the installation.

SafeGuard Policy Editor is installed. You now carry out first-time configuration within SafeGuard Policy Editor.

7 Carry out first-time configuration

Make sure that you have Windows administrator rights.

1. Start SafeGuard Policy Editor from the **Start** menu. The configuration wizard is launched and guides you through the necessary steps.
2. On the **Welcome** page, click **Next**.
3. On the **Database** page, click **Next**. The SQL database for storing SafeGuard settings and policies is created.
4. On the **Security Officer** page, enter and confirm a password that you need to access the SafeGuard Policy Editor. Click **Next**. The security officer certificate is created.

Keep this password in a safe place. If you lose it, you are not able to access the SafeGuard Policy Editor any more. Access to the account is needed to enable IT help desk staff to carry out recovery tasks.

The security officer name is displayed.

Sophos SafeGuard Disk Encryption	SafeGuard Easy
The security officer name is always Administrator .	The current user name is displayed.

5. On the **Company** page, click **Next**. The company certificate is created to secure policy settings in the database and on the endpoint computers.
6. On the **Security officer and company certificate backup** page, specify a safe storage location for the certificate backups. Then click **Next**.

If you save the certificates to the default storage location now, make sure that you export them to a safe location that can be accessed in cases of recovery, for example a USB flash drive, right after first-time configuration. You need them to restore a broken SafeGuard Policy Editor installation or a corrupt database.

7. On the **Recovery Keys** page, click **Next**. A network share with sufficient permissions for IT help desk staff is created. The share is used to collect key recovery files from the endpoint computers that are needed for recovery.

Note:

The Sophos SafeGuard software attempts to connect to the network share for about 4 minutes and if unsuccessful, tries again to connect to it after each Windows logon until the connection is established or until the recovery key files are backed up manually.

8. On the **License** page, click [...] to browse for the valid license file to run SafeGuard Policy Editor in a productive environment. You receive the license file from your sales partner. Select the file and click **Open**. Click **Next**.
9. Click **Finish**.

First-time configuration is completed.

- A default policy has been created to implement a company-wide security policy on the endpoint computers:

- Power-on Authentication is enabled.

- Volume-based-encryption for all internal hard disks is enabled.

- The user can recover a forgotten password with Local Self Help by answering predefined questions.

- The help desk can recover passwords using Challenge/Response.

- For SafeGuard Easy customers only, file-based encryption is enabled.

- All necessary requirements for the help desk to carry out recovery tasks have been set.

- A valid license file is imported to run Sophos SafeGuard in a productive environment.

SafeGuard Policy Editor starts once the configuration wizard has closed.

8 Copy of the default policy for editing

1. In the SafeGuard Policy Editor navigation area, click **Policies**.
2. In the **Policies** navigation window under **Policy Groups**, right-click **Default Policy** and click **Backup Policy**.
3. Enter a file name and storage location for the copy (XML) and click **Save**.
4. In the navigation window, right-click **Policy Groups** and click **Restore Policy**.
5. Select the newly created copy of the policy (XML) and click **Open**.

A copy of the default policy with all individual policy items is imported back into the SafeGuard Policy Editor.

Next customize the default policy copy to configure a service account list for post-installation tasks on endpoint computers. This ensures that service staff can access and pre-configure computers after installation of the encryption software without becoming the computer's "owner".

9 Configure endpoint computers for post-installation service tasks

Service staff might need to access and pre-configure the endpoint computer once the encryption software is installed, for example with a central rollout. However, the first user to log on to the computer after installation of the encryption software, activates the POA and is added as a Sophos SafeGuard user to the computer. To avoid this, you can include them on a service account list. Service staff included on this list can then log on to the operating system of the computer after installation and carry out the necessary tasks without activating the POA and without being added as a Sophos SafeGuard user.

To configure a service account list:

1. In the SafeGuard Policy Editor navigation area, click **Policies**.
2. In the **Policies** navigation window, right-click **Service Account Lists**, click **New** and then **Service Account List**.
3. Enter a name for the list and click **OK**.
4. In the navigation window, under **Service Account Lists**, select the new list.
5. Right-click in the action area on the right-hand side and select **Add** from the context-menu. A new user line is added.
6. Enter the Windows **User Name** and the **Domain Name** in the respective columns and press ENTER. To add further users, repeat this step. For further information, see the Administrator Help, chapter *Additional information for entering user and domain names*.
7. Click the **Save** icon in the toolbar to save your changes to the database.

The service account list is now registered. In the next steps you assign it to the policy.

8. In the navigation window, under **Policy Items**, select the copied **Authentication** policy item.
9. Under **Logon Options**, select **Service Account List** and select the newly created list.
10. Click the **Save** icon in the toolbar to save your changes.

The service account list is configured. The **Authentication** policy item and the policy group it is part of are updated accordingly. Next publish the edited policy to a configuration package.

Note:

You can edit further policy settings to your needs, for example to customize the POA, to configure encryption or to enable Wake-On-LAN. For further information, see the Administrator Help, chapter *Policy Settings*.

10 Publish the policy into a configuration package

To make policies available on the endpoint computer, they must first be published into a configuration package.

1. In the SafeGuard Policy Editor, on the **Tools** menu, click **Configuration Package Tool**.
2. Click **Add Configuration Package**.
3. Enter a name of your choice for the configuration package.
4. Select the **Policy Group** edited in the previous step to be applied to the endpoint computers.
5. Specify a storage location for the configuration package.
6. Click **Create Configuration Package**.
7. Click **Close**.

The policy is published into a configuration package (MSI) in the specified location. Next install the Sophos SafeGuard encryption software and the configuration package on the endpoint computers.

11 Install encryption software and configuration package on endpoint computers

1. Prepare endpoint computer for encryption.
2. To get to know Sophos SafeGuard, install the encryption software on a trial computer first. Use a different computer than the one SafeGuard Policy Editor is installed on.
3. Log on for the first time.
4. Use your own tools to create and distribute the installation and configuration packages to centrally set up the encryption software on endpoint computers.

11.1 Prepare endpoint computers for encryption

- Check if a user account is set up and active. The user needs to have a password.
- Create a full backup of the data.
- Close all open applications.
- Make sure that you have Windows administrator rights.
- Make sure that there is enough free hard disk space.
- Sophos provides a hardware configuration list to minimize the risk of conflicts between the POA and your computer hardware. The list is contained within the encryption software installation package.

We recommend that you install an updated version of the hardware configuration list on the endpoint computer before any significant deployment of Sophos SafeGuard. The file is updated on a monthly basis and made available to download from:

<ftp://POACFG:POACFG@ftp.ou.utimaco.de>

For further information, see the Administrator Help, chapter *Supported hotkeys in the POA*. See also: <http://www.sophos.com/support/knowledgebase/article/65700.html>.

- Check the hard disk(s) for errors with this command:

```
chkdsk %drive% /F /V /X
```

In some cases you might be prompted to restart the computer and run **chkdsk** again. For further information, see: <http://www.sophos.com/support/knowledgebase/article/107081.html>.

You can check the results (log file) in the Windows Event Viewer:

Windows XP: Select **Application, Winlogon**.

Windows 7, Windows Vista: Select **Windows Logs, Application, Wininit**.

- Use the Windows built-in **defrag** tool to locate and consolidate fragmented boot files, data files, and folders on local volumes.

defrag %drive%

For further information, see: <http://www.sophos.com/support/knowledgebase/article/109226.html>

- Uninstall third party boot managers, such as PRONetworks Boot Pro and Boot-US.
- We recommend that you clean the master boot record (MBR). To install Sophos SafeGuard you need a clean, unique MBR. If you have used an imaging/cloning tool on the endpoint computer, it might no longer be clean.

Start the computer from a Windows DVD and use the command **FIXMBR** within the Windows Recovery Console. For further information, see:

<http://www.sophos.com/support/knowledgebase/article/108088.html>

- If the boot partition on the endpoint computer has been converted from FAT to NTFS and the computer has not been restarted since, restart the computer once before Sophos SafeGuard is installed. Otherwise the installation might not be completed because the file system was still FAT at the time of installation while NTFS was found when it was activated.

11.2 Carry out a trial installation

Carry out the trial installation of the encryption software on a different computer than the one SafeGuard Policy Editor is installed on.

1. Prepare for installation on the endpoint computers, *see Prepare endpoint computers for encryption* (page 15).
2. Log on to the endpoint computer as an administrator.
3. Install the pre-installation package **SGxClientPreinstall.msi** that provides the endpoint computer with the necessary requirements for a successful installation of the encryption software.
4. Install the encryption software on the endpoint computer: Double-click one of the following packages (MSI) to start the encryption software installation wizard. It guides you through the necessary steps.

Sophos SafeGuard Disk Encryption	Sophos SafeGuard Easy
SDEClient.msi for the 32 bit variant or SDEClient_x64.msi for the 64 bit variant.	SGNClient.msi for the 32 bit variant. SGNClient_x64.msi for the 64 bit variant.

5. Accept the defaults on the subsequent dialogs.
6. If prompted, select the install type **Complete**.

Sophos SafeGuard Easy: SafeGuard Device Encryption and additionally SafeGuard Data Exchange are installed. For information on further available "Client" installation packages, see the Administrator Help, chapter *Installation*.

Sophos SafeGuard Disk Encryption: SafeGuard Device Encryption is installed. SafeGuard Data Exchange is not available.

7. Accept the defaults on all subsequent dialogs to complete the installation wizard.
8. Go to the location where you have saved the previously created configuration package (MSI).
9. Install this configuration package on the endpoint computer. Make sure that you delete all outdated configuration packages on the endpoint computer.

Sophos SafeGuard is installed and configured according to the previously created policies on the endpoint computer. Next log on to the computer for the first time after installation, either for post-installation tasks (using a service account) or to take ownership of the computer (as a normal user).

Additional configuration may be required to ensure that the POA functions correctly on each hardware platform. Most hardware conflict issues can be resolved using the **Hotkeys** feature built into the POA. Hotkeys can be configured after installation in the POA or using an additional configuration setting passed to the msixec deployment tool. For further information, see the Administrator Help, section *Supported hotkeys in the POA*. Also see:

<http://www.sophos.com/support/knowledgebase/article/107781.html>

<http://www.sophos.com/support/knowledgebase/article/107785.html>

11.3 Log on for the first time using a service account

Log on with a service account if you want to carry out post-installation tasks on the computer.

1. Restart the endpoint computer after installation. The Windows logon is displayed.

On Windows Vista and Windows 7 you first have to press CTRL+ALT+DEL to start 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).

2. Log on to Windows using the service account: Enter the domain and credentials as previously defined in the service account list in SafeGuard Policy Editor.

You are logged on to Windows as a guest user. The Power-on Authentication is not activated and you are not assigned as owner to this computer. You can carry out post-installation tasks as required.

11.4 Log on for the first time without a service account

1. Restart the computer. The Sophos SafeGuard Autologon is displayed, then the Windows logon is displayed.

On 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).

2. Enter your Windows user name and password.
3. Restart the computer for a second time. The Sophos SafeGuard Power-on Authentication is activated.
4. Enter your Windows user name and password. You are automatically logged on to Windows.

The Power-on Authentication is now activated. You are registered as a Sophos SafeGuard user. A balloon tool tip confirming this is displayed. Next time you log on you only need to enter your Windows credentials at the Power-on Authentication.

Initial encryption starts automatically. You may continue working and do not need to restart the computer after encryption is completed. Encryption and decryption work transparently without any user interaction. For further information, see the User Help (chapters *First logon after Sophos SafeGuard installation*, and *Data Encryption*).

11.5 Install the encryption software and configuration packages with a script

1. Prepare for installation on the endpoint computers, [see *Prepare endpoint computers for encryption* \(page 15\)](#).
2. Log on to the administrator computer as an administrator.
3. Create a folder called **Software** to use as a central store for all applications.

- Use a software deployment tool such as Microsoft System Center Configuration Manager, IBM Tivoli, or Enteo Netinstall to carry out central installation on the endpoint computers. The following must be included in the order mentioned:

Option	Description
Package	Description
Pre-installation package SGxClientPreinstall.msi	The package provides the endpoint computers with the necessary requirements for a successful installation of the encryption software. Note: If this package is not installed, installation of the encryption software is aborted.
Encryption software installation package <Client>*.msi	Depending on your product and operating system, different installation packages are available. For Windows 7 and Windows Vista, for example you may install the *_x64.msi package variant. You will find all available <Client> installation packages in your product delivery. Note: For information on all available <Client> installation packages, see the Administrator Help, chapter <i>Installation</i> .
Configuration package for endpoint computers	Use the configuration package created before in SafeGuard Policy Editor. Make sure that you delete all outdated configuration packages.
Script with commands for pre-configured installation	We recommend that you use the Windows Installer command-line tool msiexec to create the script. For further information, see the Administrator Help, chapter <i>Command for central installation</i> or see: http://msdn.microsoft.com/en-us/library/aa367988(VS.85).aspx

- To create the script, open a command prompt, and then type the scripting commands. For further information, *see Scripting command sample* (page 20).
- Distribute the pre-install, "Client" package and configuration package and the script to the endpoint computers using company software distribution mechanisms.

The packages are executed on the endpoint computers.

Sophos SafeGuard is installed and configured according to the previously created policy configuration on the endpoint computers. A key recovery file needed for recovery is created for each endpoint computer in the location defined during SafeGuard Policy Editor first-time configuration.

Additional configuration may be required to ensure that the Power-on Authentication (POA) functions correctly on each hardware platform. Most hardware conflict issues can be resolved using the **Hotkeys** built into the POA. Hotkeys can be configured after installation in the POA or by an additional configuration setting passed to the Windows Installer command msiexec. For further information, see the Administrator Help, section *Supported hotkeys in the POA*. Also see:

<http://www.sophos.com/support/knowledgebase/article/107781.html>

<http://www.sophos.com/support/knowledgebase/article/107785.html>

11.6 Scripting command sample

```
msiexec /i F:\Software\Sophos\SafeGuard\SGxClientPreinstall.msi  
/qn
```

```
msiexec /i F:\Software\Sophos\SafeGuard\SDEClient.msi /qn
```

```
/L*VX G:\Temp\Sophos\SafeGuard\%computername%_SDEClient_inst.log
```

```
InstallDir=C:\Program Files\Sophos\Sophos SafeGuard
```

```
msiexec /i F:\Software\Sophos\SafeGuard\SDEClientConfig.msi /qn
```

The command has the following effect:

```
■ msiexec /i F:\Software\Sophos\SafeGuard\SGxClientPreinstall.msi
```

Installs the Sophos SafeGuard pre-installation package from the specified storage location to the default installation directory **C:\Program Files\Sophos\Sophos SafeGuard**. The endpoint computers are provided with the necessary requirements for successful installation of the encryption software.

```
■ msiexec /i F:\Software\Sophos\SafeGuard\SDEClient.msi
```

```
InstallDir=C:\Program Files\Sophos\Sophos SafeGuard
```

Installs encryption software, in this case SafeGuard Device Encryption with Power-on Authentication from the specified storage location to the default installation directory **C:\Program Files\Sophos\Sophos SafeGuard**.

```
■ msiexec /i F:\Software\Sophos\SafeGuard\SDEClientConfig.msi
```

Installs the configuration package from the specified storage location to the default installation directory.

```
■ /L*VX  
G:\Temp\Sophos\SafeGuard\%computername%\_SDEClient_inst.log
```

Logs all warnings and error messages in the specified log file on the network and creates a log file to review the encryption process from a central location that can be analyzed using the Windows Installer tool **wilogutl.exe**.

```
■ /qn
```

Installs without user interaction and does not display a user interface.

12 Recover a forgotten password

If the user has forgotten their password, there are two ways to recover it:

- The user may recover it themselves using Local Self Help. This is the recommended method.
- The help desk may recover it using a Challenge/Response procedure.

12.1 Recover a forgotten password using Local Self Help

1. On the endpoint computer in the Power-on Authentication, the user enters their user name.
The **Recovery** button becomes active.

2. The user clicks **Recovery**.

- If only Local Self Help is activated for logon recovery on the endpoint computer, it is then started automatically.
- If both Local Self Help and Challenge/Response are displayed for logon recovery, the user clicks **Local Self Help**.

3. In the following five dialogs, the user answers a defined number of questions randomly selected from the questions stored on the endpoint computer. After answering the last one, the user confirms the answers with **OK**.

4. In the next dialog, the user can view the password by pressing ENTER or SPACEBAR, or by clicking the blue display box.

The password is displayed for 5 seconds at the maximum. Afterwards, the startup process continues automatically. The user can hide the password immediately by pressing ENTER, or SPACEBAR, or by clicking the blue display box again.

5. After reading the password, the user clicks **OK**.

The user is logged on at the Power-on Authentication and to Windows and can use the password for future logon.

12.2 Recover a forgotten password using Challenge/Response

Prerequisites:

The key recovery file created for each endpoint computer during installation of the Sophos SafeGuard encryption software must be accessible to the help desk and the name of the file must be known. Challenge/Response must be enabled using a policy for the endpoint computer.

Note:

We recommend that you primarily use Local Self Help to recover a forgotten password. Local Self Help allows the user 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.

1. On the endpoint computer in the Power-on Authentication, the user enters their user name. The **Recovery** button becomes active.
2. The user clicks **Recovery**.
 - If only Challenge/Response is activated for logon recovery, it is then started automatically.
 - If both Challenge/Response and Local Self Help are displayed for logon recovery, the user clicks **Challenge/Response**.

A dialog is displayed indicating the name of the key recovery file required.

3. The user clicks **Next**. A random challenge code is displayed.
4. The user contacts the help desk and provides the name of the required key recovery file as well as the challenge code to the help desk.
5. In SafeGuard Policy Editor, the help desk launches the **Recovery Wizard**.
6. The help desk selects recovery of type **Sophos SafeGuard Client**, confirms the key and the challenge code and selects the required recovery action **Booting without user logon**.

A response code in the form of an ASCII character string is generated and displayed.

7. The help desk provides the user with the response code, for example by phone or text message.
8. On the endpoint computer in the Challenge/Response Wizard, the user clicks **Next** to enter the response code provided. The computer is enabled to start through Power-on Authentication.
9. In the Windows logon dialog, the user does not know the correct password and needs to change password at Windows level. This requires further recovery actions outside the scope of Sophos SafeGuard, using standard Windows means. We recommend that you use the following methods to reset the password at Windows level.
 - Using a service or administrator account available on the endpoint computer with the required Windows rights.
 - Using a Windows password reset disk on the endpoint computer.

10. The user enters the new password at Windows level that the help desk has provided. The user then changes this password immediately to a value only known to them.
11. Sophos SafeGuard detects that the newly chosen password does not match the current Sophos SafeGuard password used in the POA. The user is therefore prompted to enter the old Sophos SafeGuard password and, since the user has forgotten this password, needs to click **Cancel**.
12. In Sophos SafeGuard, a new certificate is needed in order to set a new password without providing the old one. The user has to confirm this procedure.
13. A new user certificate is created based on the newly chosen Windows password.

The user can log on to the computer and log on at the Power-on Authentication again with the new password and can use the password for future logon.

13 Get help with common tasks

This section tells you where to find information on how to carry out common tasks. Refer to the Sophos SafeGuard Administrator Help, User Help or Tools Guide for all further information.

Task	Manual/Help
Configure additional instances of the SafeGuard policy Editor.	Administrator Help, Configure additional instances of the SafeGuard Policy Editor.
Ensure correct functioning of the Power-on Authentication	Administrator Help/User Help, Supported Hotkeys in the Power-on Authentication
Display Sophos SafeGuard specific information on the endpoint computer.	User Help, System Tray icon and balloon tool tip
Create and group policies.	Administrator Help, Working with policies
Export certificates.	Administrator Help, Exporting the company and security officer certificates.
Create administrative access to endpoint computers (POA access accounts).	Administrator Help, Administrative access to endpoint computers
Recover access to encrypted data	Administrator Help, Challenge/Response using Virtual Clients
Recover a corrupt Master Boot Record	Tools Guide, Restoring a corrupted MBR
Upgrade SDE 4.6x / SGE 4.3x -4.5x to Sophos SafeGuard	Administrator Help, Upgrading SafeGuard Easy 4.x/Sophos Disk Encryption 4.x to Sophos SafeGuard 5.6x

14 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.

15 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.