

**SOPHOS**

Security made simple.

# SafeGuard Easy startup guide

Product version: 6.1

Document date: February 2014



# Contents

1 About this guide.....	3
2 About Sophos SafeGuard (SafeGuard Easy).....	4
3 Can I upgrade from earlier versions?.....	9
4 What do I install?.....	10
5 What are the key steps?.....	11
6 Install SafeGuard Policy Editor.....	12
7 Carry out first-time configuration.....	13
8 Copy the default policy for editing.....	15
9 Give administrators access to endpoints .....	16
10 Publish the policy into a configuration package.....	17
11 Install encryption software and configuration package on endpoints.....	18
12 Recover a forgotten password.....	24
13 Get help with common tasks.....	26
14 Technical support.....	27
15 Legal notices.....	28

## **1 About this guide**

This guide tells you how to set up Sophos SafeGuard (SafeGuard Easy 6.1) to protect your company's endpoints against unauthorized access.

Further information is available in the *SafeGuard Easy administrator help* and *SafeGuard Easy user help*.

## 2 About Sophos SafeGuard (SafeGuard Easy)

Sophos SafeGuard (SafeGuard Easy) 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.
- Encrypt data using technology that is FIPS 140 compliant.

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



The SafeGuard 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 administrative access

Sophos SafeGuard offers several features that aid IT operations on endpoints:

- The SafeGuard 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 endpoints for post-installation tasks without activating the SafeGuard Power-on Authentication.
- POA users are predefined local accounts that enable users (for example members of the IT team) to log on to encrypted endpoints for administrative tasks after the SafeGuard Power-on Authentication has been activated.

## Recovery options

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 endpoints without the assistance of a helpdesk. Even in situations where neither telephone nor network connections are available (for example aboard an aircraft), users can regain access to their endpoints. To log on, they answer a predefined number of questions in the SafeGuard Power-on Authentication.

Local Self Help reduces the number of calls concerning logon recovery, thus freeing the helpdesk 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 helpdesk. It helps users who cannot log on to their endpoints or access encrypted data. During the Challenge/Response procedure, the user provides a challenge code generated on the endpoint to the helpdesk officer who in turn generates a response code that authorizes the user to perform a specific action on the endpoint. With Challenge/Response, Sophos SafeGuard offers different workflows for typical recovery scenarios that require helpdesk 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 endpoint 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 as well as the required access rights to this share are automatically created during first-time configuration.

## 2.1 About Sophos SafeGuard (SafeGuard Easy) 6.1

Sophos SafeGuard provides powerful data protection through encryption and additional logon authentication.

This version of Sophos SafeGuard (SafeGuard Easy) Easy supports Windows 7 and Windows 8 on endpoints with BIOS or UEFI.

- For BIOS platforms you can choose between SophosSafeGuard full disk encryption and BitLocker encryption managed by Sophos SafeGuard. The BIOS version comes with the BitLocker native recovery mechanism.

**Note:** If SafeGuard Power-on Authentication or SafeGuard full disk encryption is mentioned in this manual, it refers to Windows 7 BIOS endpoints only.

- For UEFI platforms, use BitLocker managed by Sophos SafeGuard (SafeGuard Easy) for disk encryption. For these endpoints Sophos SafeGuard offers enhanced Challenge/Response capabilities. For details on the supported UEFI versions and restrictions to SafeGuard BitLocker Challenge/Response support, please see the Release Notes at [http://downloads.sophos.com/readmes/readseasy\\_61\\_eng.html](http://downloads.sophos.com/readmes/readseasy_61_eng.html).

**Note:** Whenever the description only refers to UEFI, it is mentioned explicitly.

The table shows which components are available.

	SafeGuard full disk encryption with SafeGuard Power-on Authentication (POA)	BitLocker with pre-boot authentication (PBA) managed by SafeGuard	SafeGuard C/R recovery for BitLocker pre-boot authentication (PBA)
Windows 7 BIOS	YES	YES	
Windows 7 UEFI		YES	YES
Windows 8 UEFI		YES	YES
Windows 8 BIOS		YES	
Windows 8.1 UEFI		YES	YES
Windows 8.1 BIOS		YES	

**Note:** SafeGuard C/R recovery for BitLocker pre-boot authentication (PBA) is only available on 64-bit systems.

**SafeGuard full disk encryption with SafeGuard Power-on Authentication (POA)** is the Sophos module for encrypting volumes on endpoints. It comes with a Sophos implemented pre-boot

authentication named SafeGuard Power-on Authentication (POA) which supports logon options like smartcard and fingerprint and a Challenge/Response mechanism for recovery.

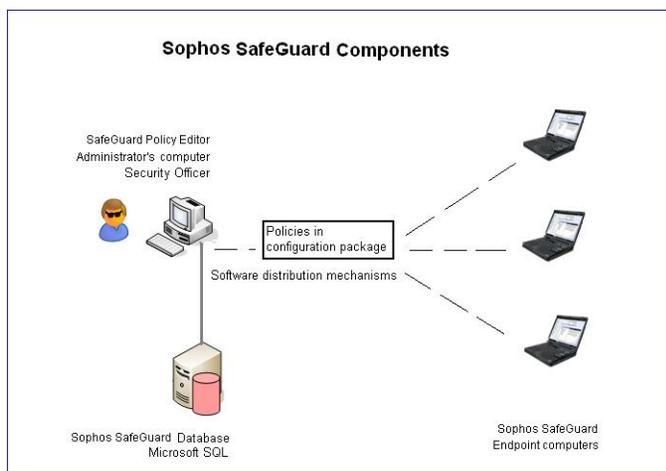
**BitLocker with pre-boot authentication (PBA) managed by SafeGuard** is the component that enables and manages the BitLocker encryption engine and the BitLocker pre-boot authentication.

It is available for BIOS and UEFI platforms:

- The UEFI version additionally offers an SafeGuard Challenge/Response mechanism for BitLocker recovery in case users forget their PINs. The UEFI version can be used when certain platform requirements are met. For example the UEFI version must be 2.3.1. For details, see the Release Notes.
- The BIOS version does not offer the recovery enhancements by the SafeGuard Challenge / Response mechanism and serves also as fallback option in case the requirements for the UEFI version are not met. The Sophos installer checks whether the requirements are met, and if not automatically installs the BitLocker version without Challenge/Response

Sophos SafeGuard (SafeGuard Easy) uses a policy-based encryption strategy to protect information on endpoints.

Administration is carried out with the SafeGuard Policy Editor, which is used to create and manage security policies and to provide recovery functions. Policies are deployed to endpoints in configuration packages. On the user side, the main security functions are data encryption and protection against unauthorized access. Sophos SafeGuard can be seamlessly integrated into the user's normal environment and is easy and intuitive to use. The Sophos SafeGuard authentication system, SafeGuard Power-on Authentication (POA), provides powerful access protection and offers user-friendly support when recovering credentials.



## Sophos SafeGuard components

Sophos SafeGuard consists of the following components:

Component	Description
SafeGuard Policy Editor	<p>Sophos SafeGuard management tool used to create encryption and authentication policies.</p> <p>SafeGuard Policy Editor creates a default policy during first-time configuration.</p> <p>SafeGuard Policy Editor also provides recovery functions to allow users to regain access to their computers, if they have forgotten their password, for example.</p>
Sophos SafeGuard Database	Sophos SafeGuard Database holds all policy settings for the endpoints.
Sophos SafeGuard software on endpoints	Encryption software on endpoints.

### Product names

The following product names are used in this help:

Product name	Description
Sophos SafeGuard Easy (SGE)	Sophos SafeGuard standalone encryption software. From versions 5.x, SafeGuard Policy Editor is used for policy configuration and helpdesk tasks.
Sophos SafeGuard Disk Encryption (SDE) up to 5.60	Sophos SafeGuard standalone encryption software available with the Endpoint Security and Data Protection (ESDP) bundle up to version 10.
Sophos Disk Encryption 5.61	Managed full disk encryption through Sophos Enterprise Console 5.1 and above.
SafeGuard Enterprise	Comprehensive, modular SafeGuard encryption suite with central, role-based management that protects data on endpoints from being read or changed by unauthorized persons.
Sophos Enterprise Console	Sophos console that manages and updates Sophos security software. With version 5.1 it also manages encryption on endpoints (Sophos Disk Encryption 5.61).

### 3 Can I upgrade from earlier versions?

Endpoints that have already been encrypted with SafeGuard Easy/Sophos SafeGuard Disk Encryption 5.60.x or above can be upgraded to SafeGuard Easy 6.1.

A valid license file is required that you need to import into SafeGuard Policy Editor. You receive the file from your sales partner.

For further information, see the *SafeGuard Easy administrator help*, sections *About upgrading* and *About migrating*.

## 4 What do I install?

You install the following components:

- **SafeGuard Policy Editor.** This is the Sophos SafeGuard management console. It enables you to manage encryption software on endpoints and to carry out recovery tasks.

Microsoft SQL Server 2012 SP1 Express Edition is used to store Sophos SafeGuard policy settings. It is automatically installed during SafeGuard Policy Editor setup if a Microsoft 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 endpoints and protects them from unauthorized access.

**Note:** We recommend that you do not install the encryption software on computers with SafeGuard Policy Editor installed.

## **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 helpdesk tasks.
- Copy the default policy for editing.
- Give administrators access to endpoints after installation.
- Publish the edited policy into a configuration package.
- Install the encryption software and configuration package on the endpoints.

## 6 Install SafeGuard Policy Editor

Before you start:

- Make sure that .NET Framework 4 is installed on the computer where you want to install SafeGuard Policy Editor. It is provided in your product delivery.
- If you want to install Microsoft SQL Server 2012 SP1 Express Edition automatically during SafeGuard Policy Editor installation, make sure that Microsoft Windows Installer 4.5 is installed.
- Check the system requirements in the current release notes version.
- 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 installer and documentation.
3. Store them in a location where you can access them for installation.
4. From the product's install folder, double-click the SafeGuard Policy Editor package SGNPolicyEditor.msi. A wizard guides you through the necessary steps.
5. Accept the defaults on the subsequent dialogs.

If prompted to install Microsoft SQL Server 2012 SP1 Express Edition, click **Yes**. In this case, your Windows credentials are used for the SQL user account.

6. 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 helpdesk staff to carry out recovery tasks.

The security officer 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 endpoints.
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 helpdesk staff is created. The share is used to collect key recovery files from the endpoints that are needed for recovery.
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 endpoints:
  - SafeGuard Power-on Authentication is enabled.
  - SafeGuard full disk encryption for all internal hard disks is enabled.
  - File-based encryption for data on removable media is enabled.
  - The user can recover a forgotten password with Local Self Help by answering predefined questions.

- The helpdesk can recover passwords using Challenge/Response.
  - The necessary requirements for the helpdesk 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 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 SafeGuard Policy Editor.

Next customize the default policy copy to configure a service account list for administrative access on endpoints after installation. This ensures that service staff can access and pre-configure endpoints after installation of the encryption software without being registered.

## 9 Give administrators access to endpoints

Service staff might need to access and pre-configure endpoints once the encryption software is installed, for example with a central rollout. However, the first user who logs on after installation of the encryption software, activates the SafeGuard POA and is added as a Sophos SafeGuard user to the endpoints. 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 endpoint after installation and carry out the necessary tasks without activating the SafeGuard 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**, select **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 *SafeGuard Easy 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 SafeGuard POA, to configure encryption or to enable Wake On LAN. For further information, see the *SafeGuard Easy administrator help*, chapter *Secure Wake On LAN*.

## 10 Publish the policy into a configuration package

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

1. In 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 endpoints.
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 endpoints.

## 11 Install encryption software and configuration package on endpoints

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 endpoints.

### 11.1 Prepare endpoints for encryption

- Check if a user account is set up and active. The user needs to have a password.
- Make sure that you have Windows administrator rights.
- Create a full backup of the data.
- Drives to be encrypted must be completely formatted and have a drive letter assigned to them.
- Sophos provides a hardware configuration list to minimize the risk of conflicts between the SafeGuard POA and your endpoint hardware. The list is contained within the encryption software installation package.

We recommend that you install an updated version of this configuration file before any significant deployment of Sophos SafeGuard. The file is updated on a monthly basis and made available to download from: <http://www.sophos.com/en-us/support/knowledgebase/65700.aspx>.

- 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 endpoint and run **chkdsk** again. For further information, see: <http://www.sophos.com/en-us/support/knowledgebase/107081.aspx>.

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

Windows 7: 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/en-us/support/knowledgebase/109226.aspx>.

- 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, it might no longer be clean.

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

<http://www.sophos.com/en-us/support/knowledgebase/108088.aspx>.

- If the boot partition on the endpoint has been converted from FAT to NTFS and the endpoint has not been restarted since, restart the endpoint once. Otherwise the installation might not be completed successfully.

## 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.

### Prerequisites:

Endpoints must have been prepared for encryption, see *Prepare endpoints for encryption* (section 11.1).

1. Log on to the endpoint as an administrator.
2. Install the current pre-installation package **SGxClientPreinstall.msi** that provides the endpoint with the necessary requirements for a successful installation of the current encryption software.
3. Double-click the encryption software package **SGNClient.msi** or the 64 bit variant if appropriate. A wizard guides you through the necessary steps.
4. Accept the defaults on the subsequent dialogs.
5. If prompted, select the install type **Complete**.

SafeGuard full disk encryption and SafeGuard file-based encryption are installed. For information on available encryption packages and features, see the *SafeGuard Easy administrator help*, section *Installation*.

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

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

Additional configuration may be required to ensure that the SafeGuard POA functions correctly on each hardware platform. Most hardware conflict issues can be resolved using the **Hotkeys**

feature built into the SafeGuard POA, see the *SafeGuard Easy administrator help*, section *Supported hotkeys in SafeGuard Power-on Authentication*. Also see:

<http://www.sophos.com/en-us/support/knowledgebase/107781.aspx> and

<http://www.sophos.com/en-us/support/knowledgebase/107785.aspx>.

### 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 endpoint.

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

You may 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. SafeGuard Power-on Authentication is not activated and you are not registered on the endpoint. You can carry out post-installation tasks as required.

### 11.4 Log on for the first time as a normal user

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

You may 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 endpoint for a second time. The SafeGuard Power-on Authentication is activated.
4. Enter your Windows user name and password. You are automatically logged on to Windows.

SafeGuard 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 SafeGuard Power-on Authentication.

Initial encryption starts automatically. You may continue working and do not need to restart the endpoint after encryption is completed. Do not shut down or hibernate the endpoint until initial encryption is completed. Encryption and decryption work transparently without any user interaction. For further information, see the *SafeGuard Easy user help*.

## 11.5 Install the encryption software and configuration packages with a script

1. Prepare for installation on the endpoints, see [Prepare endpoints for encryption](#) (section 11.1).
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.
4. 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. The following must be included in the order mentioned:

**Note:** When carrying out the installation through Active Directory, use a separate group policy object (GPO) for each package and sort them in the order mentioned below to guarantee a successful installation.

When the endpoint language is not set to German, additionally do the following: in the Group Policy Editor, select the respective group object and then **Computer Configuration > Software Settings > Advanced**. In the **Advanced Deployment Options** dialog, select **Ignore language when deploying this package** and click **OK**.

Package	Description
<b>Pre-installation package</b> <b>SGxClientPreinstall.msi</b>	The mandatory package provides the endpoints with the necessary requirements for a successful installation of the current encryption software.  <b>Note:</b> If this package is not installed, installation of the encryption software is aborted.
<b>Encryption software package</b>	Depending on your license and operating system, different installation packages are available. You find all available packages (<*Client*>.MSI) in your product delivery.  <b>Note:</b> For a list of available packages, see the <i>SafeGuard Easy administrator help</i> , chapter <i>Installation</i> .
<b>Configuration package for endpoints</b>	Use the configuration package created before in SafeGuard Policy Editor. Make sure that you delete any outdated ones first.
<b>Script with commands for pre-configured installation</b>	We recommend that you use the Windows Installer command-line tool <b>msiexec</b> to create the script. For further information, see the <i>SafeGuard Easy administrator help</i> , chapter <i>Command for central installation</i> or see: <a href="http://msdn.microsoft.com/en-us/library/aa367988(VS.85).aspx">http://msdn.microsoft.com/en-us/library/aa367988(VS.85).aspx</a>

5. To create the script, open a command prompt, and then type the scripting commands. For further information, see [Scripting command sample](#) (section 11.6).
6. Distribute the pre-install, encryption software package and configuration package, as well as the script to the endpoints using company software distribution mechanisms.

The packages are executed on the endpoints.

7. After installation, make sure that endpoints are restarted twice to activate SafeGuard Power-on Authentication. They must be restarted for a third time to perform a backup of the kernel data on every Windows boot.

Make sure that endpoints are not suspended or hibernated before the third restart to successfully complete the kernel backup.

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

**Note:** Additional configuration may be required to ensure that the SafeGuard Power-on Authentication (POA) functions correctly on each hardware platform. Most hardware conflict issues can be resolved using the **Hotkeys** built into the SafeGuard POA. For further information, see the *SafeGuard Easy administrator help*, section *Supported hotkeys in SafeGuard the Power-on Authentication*. Also see:

<http://www.sophos.com/en-us/support/knowledgebase/107781.aspx> and

<http://www.sophos.com/en-us/support/knowledgebase/107785.aspx>.

## 11.6 Scripting command sample

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

```
msiexec /i F:\Software\Sophos\SafeGuard\SGNClient.msi /qn /L*VX  
G:\Temp\Sophos\SafeGuard\%computername%\SGNClient_inst.log  
InstallDir=C:\Program Files\Sophos\Sophos SafeGuard
```

```
msiexec /i F:\Software\Sophos\SafeGuard\SGNClientConfig.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 endpoints are provided with the necessary requirements for successful installation of the current encryption software.

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

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

Installs encryption software, in this case SafeGuard full disk encryption with SafeGuard 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\SGNClientConfig.msi
```

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

```
■ /L*VX  
G:\Temp\Sophos\SafeGuard\%computername%\_SGNClient_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 **wilogut1.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 helpdesk may recover it using a Challenge/Response procedure.

### 12.1 Recover a forgotten password using Local Self Help

1. On the endpoint in the SafeGuard 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, 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. 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 SafeGuard 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 during installation of the Sophos SafeGuard encryption software must be accessible to the helpdesk and the name of the file must be known. Challenge/Response must be enabled using a policy for the endpoint.

#### 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 helpdesk.

1. On the endpoint in the SafeGuard 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 helpdesk and provides the name of the required key recovery file as well as the challenge code to the helpdesk.
5. In SafeGuard Policy Editor, the helpdesk launches the **Recovery Wizard**.
6. The helpdesk selects recovery of type **Sophos SafeGuard Client**, confirms the key and the challenge code and selects the required recovery action **Boot SGN Client without user logon**.

A response code in the form of an ASCII character string is generated and displayed.
7. The helpdesk provides the user with the response code, for example by phone or text message.
8. On the endpoint in the Challenge/Response Wizard, the user clicks **Next** to enter the response code provided. The endpoint is enabled to start through SafeGuard Power-on Authentication.
9. In the Windows logon dialog, the user does not know the correct password and needs to change the 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 with the required Windows rights.
  - Using a Windows password reset disk on the endpoint.

10. The user enters the new password at Windows level that the helpdesk has provided. The user then changes this password immediately to a value only known to them.

A new user certificate for use in Sophos SafeGuard will be created automatically based on the newly chosen Windows password. This enables the user to log on to the computer again and to log on at the SafeGuard Power-on Authentication with the new password.

The user can log on to the endpoint and log on at the SafeGuard 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 *SafeGuard Easy administrator help*, *user help* or *tools guide* for all further information.

Task	Manual/Help
Configure additional instances of SafeGuard Policy Editor.	Administrator help, Configure additional instances of SafeGuard Policy Editor.
Ensure correct functioning of the SafeGuard Power-on Authentication	Administrator help/user help, Supported hotkeys keys in SafeGuard Power-on Authentication
Display Sophos SafeGuard specific information on the endpoint.	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 endpoints (POA access accounts).	Administrator help, Administrative access to endpoints
Recover access to encrypted data	Administrator help, Regain access to encrypted data with Challenge/Response
Recover a corrupt Master Boot Record	Tools guide, Restoring a corrupted MBR
Migrate SGE/SDE 5.60.x or above to SafeGuard Easy 6.1	Upgrade and migration guide, About upgrading

## 14 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/en-us/support.aspx/>.
- Download the product documentation at <http://www.sophos.com/en-us/support/documentation/>.
- Send an email to [support@sophos.com](mailto:support@sophos.com), including your Sophos software version number(s), operating system(s) and patch level(s), and the text of any error messages.

## 15 Legal notices

Copyright © 1996 - 2014 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.