

# SOPHOS

## Sophos SafeGuard Disk Encryption 5.50 Sophos SafeGuard Easy 5.50 Startup guide

Document date: April 2010



# Content

1	About this guide .....	2
2	Introduction.....	3
3	Upgrading from Sophos SafeGuard Disk Encryption 4.60 .....	6
4	Upgrading from SafeGuard Easy 4.x.....	7
5	What are the key steps? .....	8
6	Check the system requirements .....	9
7	Prepare for installation.....	11
8	Install the SafeGuard Policy Editor .....	14
9	Carry out initial configuration .....	15
10	Carry out additional configuration of the encryption software .....	17
11	Configure administrative access on endpoint computers.....	27
12	Install the encryption software and encryption configuration on endpoint computers.....	30
13	Recover a forgotten password .....	36
14	Recover access to the system .....	39
15	Get help with common tasks .....	41
16	Technical support.....	42
17	Copyright .....	43

# 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) 5.50 available with the Endpoint Security and Data Protection (ESDP) bundle.
- Sophos SafeGuard Easy (SGE) 5.50. 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 clearly stated in this guide.

Additional information is available within the Sophos SafeGuard Administrator help and Sophos SafeGuard User help documents which accompany this Startup guide.

## 2 Introduction

Sophos SafeGuard encrypts data transparently. This means that users do not need to decide which data is to be encrypted and decryption takes place unnoticed. 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.

The benefits of Sophos SafeGuard are:

- Simply but effectively protects the confidentiality of data
- Can be implemented quickly
- Based on market leading encryption technology certified FIPS 140 compliant

Computers protected by Sophos SafeGuard run the SafeGuard Power-on Authentication (POA) before the operating systems starts.



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

- Tampering 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

## **2.1 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.

## 2.2 Recovery scenarios in Sophos SafeGuard

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

### ■ Logon recovery via 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 via Challenge/Response

The Challenge/Response recovery mechanism is a secure and efficient recovery system that 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 via 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.

### ■ Key recovery file

Recovery via Challenge/Response as well as system 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 as well as the required access rights to this share are automatically created during initial configuration.

## **3 Upgrading from Sophos SafeGuard Disk Encryption 4.60**

There are significant enhancements available within Sophos SafeGuard Disk Encryption (SDE) 5.5x. This includes support for encrypting computers running Windows Vista and Windows 7 (32 and 64 bit).

Computers that have already been encrypted using SDE 4.60 can be upgraded to SDE 5.50. Encrypted volumes remain encrypted and the encryption keys are automatically converted to a format compatible to version 5.50.

Before upgrading encrypted computers to Sophos SafeGuard 5.50 a new configuration package should be created using SafeGuard Policy Editor and deployed alongside the Sophos SafeGuard 5.50 software.

For further information see the Administrator help, chapter *Upgrading SafeGuard Easy 4.x/ Sophos SafeGuard Disk Encryption 4.x to Sophos SafeGuard 5.5x* as well as the following knowledgebase article: <http://www.sophos.com/support/knowledgebase/article/108561.html>.

## **4 Upgrading from SafeGuard Easy 4.x**

There are significant enhancements available within SafeGuard Easy (SGE) 5.50. This includes support for encrypting computers running Windows Vista and Windows 7 (32 and 64 bit).

Computers that have already been encrypted using SGE 4.3x to 4.5x can be upgraded to SGE 5.5x. Encrypted volumes remain encrypted and the encryption keys are automatically converted to a format compatible to version 5.50.

SGE 5.50 also uses a different administration tool, the SafeGuard Policy Editor, which is not backwards compatible with SGE 4.x. Before upgrading encrypted computers to Sophos SafeGuard 5.50 a new configuration package should be created using SafeGuard Policy Editor and deployed alongside the Sophos SafeGuard 5.50 software.

For further information see the Administrator help, chapter *Upgrading SafeGuard Easy 4.x/ Sophos SafeGuard Disk Encryption 4.x to Sophos SafeGuard 5.5x* as well as the following knowledgebase article: <http://www.sophos.com/support/knowledgebase/article/108561.html>.

## **5 What are the key steps?**

We recommend installing SafeGuard Policy Editor on a Windows Server and then deploying the encryption software to computers using a software deployment tool such as Microsoft System Center Configuration Manager. The key steps are:

- Check the system requirements.
- Prepare for installation.
- Install the SafeGuard Policy Editor used for policy configuration and help desk tasks.
- Carry out initial configuration.
- Carry out additional configuration of the encryption software.
- Install the encryption software and encryption configuration on endpoint computers.

## **6 Check the system requirements**

### **6.1 Administration tools requirements**

#### **Hardware**

- Intel or AMD X86 CPU
- 1 GB RAM
- 1 GB free hard disk space (recommended)

#### **Software**

The 32 bit and 64 bit versions of the following operating systems are supported unless otherwise mentioned. Latest service packs are recommended:

- Microsoft Windows XP Professional (32 bit)
- Microsoft Windows 2003 Server
- Microsoft Windows 2003 Server R2
- Microsoft Windows Vista
- Microsoft Windows 2008 Server
- Microsoft Windows 2008 Server R2
- Microsoft Windows 7

Microsoft ASP.net: .NET Framework 3.0 SP1

### **6.2 Database requirements**

The following 32 bit and 64 bit versions are supported:

- Microsoft SQL Server 2005 SP2, SP3
- Microsoft SQL Server 2005 Express SP2, SP3
- Microsoft SQL Server 2008
- Microsoft SQL Server 2008 Express

## 6.3 Requirements for Sophos SafeGuard protected computers

### Hardware

- Intel or AMD X86 CPU
- 512 MB RAM (minimum), 1024 MB (recommended for Windows Vista)
- The installation needs at least 300 MB free hard disk space of which at least 100 MB must be one contiguous area. Please defragment your system before installation if you have below 5 GB free hard disk space and your operating system is not freshly installed to increase the chance that this contiguous area is available. Otherwise, installation may fail due to insufficient free contiguous space and cannot be supported.

### Software

The 32 bit and 64 bit versions of the following operating systems are supported unless otherwise mentioned. Latest service packs are recommended:

- Microsoft Windows XP Professional (32 bit only)
- Microsoft Windows Vista Enterprise, Ultimate, Business or Home Premium. (Vista without SP1 is not supported.)
- Microsoft Windows 7

### Restrictions

- If using Intel Advanced Host Controller Interface (AHCI) on the computer, the boot hard disk must be in Slot 0 or Slot 1. You can insert up to 32 hard disks. Sophos SafeGuard only runs on the first two slot numbers.
- Dynamic and GUID partition table (GPT) disks are not supported. In such cases, the installation will be terminated. If such disks can be found on the computer at a later point in time, they will not be supported.
- The Sophos SafeGuard Device Encryption module does not support systems that are equipped with hard disks attached via a SCSI bus.

## 7 Prepare for installation

Before deploying Sophos SafeGuard it is recommended to carry out the following preparations.

### 7.1 General considerations

- If you would like to install Sophos SafeGuard via a central rollout we recommend configuring a service account list. Once an IT administrator is added to the service account list they can log on to computers after the installation of Sophos SafeGuard without activating the Power-on Authentication. This is recommended because normally the first user to log on to an endpoint computer after installation is added to the POA as the primary account. For further information see [Configure Service Account Lists](#), page 27.
- Central deployment of Sophos SafeGuard can be achieved using a wide range of system management/deployment tools including Microsoft SCCM/SMS, IBM Tivoli, Enteo Netinstall.
- Decide if you want to use the recommended default policy configuration supplied with Sophos SafeGuard. For a summary of the default policies see [Carry out additional configuration of the encryption software](#), page 17. For a detailed breakdown of the default policies see the Administrator help, chapter *Default Policies*.
- If you wish to use Wake-On-LAN you need to configure it in advance via a policy of the type **Specific Machine Settings**. For further information see the Administrator help, chapter *Policy settings*.
- Sophos SafeGuard can be configured to save encryption/installation logs into a network location (UNC path). This enables the administrator to review the encryption process from a central location. For further information, see [Install the encryption software and encryption configuration with a script](#), page 33.

## 7.2 General preparations

- To install the encryption software and to operate the Sophos SafeGuard administration tools you need Windows administrator rights.
- Read the release notes carefully.

## 7.3 Prepare computers for encryption

- A user account must be set up and active on the computer. The user needs to have a password.
- Close all open applications.
- Ensure that there is enough free hard disk space.
- Create a full backup of the data on the computer.
- 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 you install an updated version of the hardware configuration file prior to any significant deployment of Sophos SafeGuard. The file is updated on a monthly basis and made available to download from here: <ftp://POACFG:POACFG@ftp.ou.utimaco.de>

For further information see the Administrator help, chapter *Supported hotkeys in the POA* as well as the following knowledgebase article: <http://www.sophos.com/support/knowledgebase/article/65700.html>.

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

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

In some cases you might be prompted to restart the computer and run chkdsk again. For further information see the following knowledgebase article:

<http://www.sophos.de/support/knowledgebase/article/107081.html>.

- 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 the following knowledgebase article:

<http://www.sophos.com/support/knowledgebase/article/109226.html>

- Uninstall third party boot managers, such as "PRONetworks Boot Pro" and "Boot-US".
- If you have used an imaging/cloning tool, we recommend to "rewrite" the MBR. To install Sophos SafeGuard you need a clean, unique master boot record. By using image/cloning tools the master boot record might no longer be clean.

You can clean the master boot record by booting from a Windows CD and using the command FIXMBR within the Windows Recovery Console.

For further information see the following knowledgebase article:

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

- If the boot partition has been converted from FAT to NTFS and the system has not been restarted since, you should not install Sophos SafeGuard. 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. In this case you have to restart the computer once before Sophos SafeGuard is installed.

## 8 Install the SafeGuard Policy Editor

Before you deploy the encryption software on endpoint computers, 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. The same account is used to access each SafeGuard Policy Editor instance.

**Prerequisites:** .NET Framework 3.0 Service Pack 1 must be installed on the Windows server. You may download it for free from <http://www.microsoft.com/downloads>.

1. Log on to your computer as an administrator.
2. From the product's install folder, install either of the following. A wizard will guide you through the necessary steps.

Sophos SafeGuard Disk Encryption	SafeGuard Easy
Double-click SDEPolicyEditor.msi.	Double-click SGNPolicyEditor.msi.

3. Accept the default on the next dialogs.

Database installation: An SQL database instance is used to store Sophos SafeGuard policy settings. You may be prompted to install Microsoft SQL Server 2005 Express during the SafeGuard Policy Editor installation if an existing SQL database instance is unavailable. In this case, your Windows credentials will be used as the SQL user account.

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

The SafeGuard Policy Editor is installed. Next you carry out initial configuration within SafeGuard Policy Editor.

## 9 Carry out initial configuration

You need to have Windows administrator rights to carry out the initial configuration within SafeGuard Policy Editor.

1. Start the SafeGuard Policy Editor. The Configuration Wizard will be launched and guides you through the necessary steps.
2. Confirm the **Welcome** page with **Next**.
3. On the **Database** page, the SQL database instance selected or created during the SafeGuard Policy Editor installation will be displayed. Confirm the defaults with **Next**. The database will be created.
4. On the **Security Officer** page, the security officer name is already displayed. Enter and confirm a password that you will need to access the SafeGuard Policy Editor. Confirm the defaults with **Next**. The security officer certificate will be created.

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

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

5. On the **Company** page, enter a **Company name**. Confirm the default with **Next**. The company certificate will be created.  
For a reinstallation you may also import the certificate.
6. On the **Certificate Backup** page, confirm the default with **Next**.  
Ensure to export the certificates to a location that can be accessed for recovery purposes, for example to a memory stick, right after initial configuration. Keep them in a safe place. You will need them to restore a broken installation or corrupt database. For further information see the Administrator help.
7. On the **Default Policy** page, confirm the defaults with **Next**. Recommended default policies as well as a configuration package (standard-packet.msi) will be created containing these default policies.

The recommended default policies include the encryption of internal hard disk volumes, activated Power-on Authentication, and settings that enable local and remote recovery. For details see [Carry out additional configuration of the encryption software](#), page 17 and the Administrator help, chapter *Default Policies*. The default policies can only be created during the initial configuration in the SafeGuard Policy Editor Configuration Wizard. You may change the default policies later on or create new user-defined policies as required.

8. On the **Recovery Keys** page, accept the default **Create network share**. Confirm with **Next** to accept the default permissions.

This will create a network share SafeGuardRecoveryKeys\$ and a directory on the server or local computer where the recovery keys will be saved automatically. It will grant the help desk sufficient access rights to the recovery key share. If **Create network share** is not enabled, the end user will be prompted for a location to save the recovery key files once encryption has been completed.

**Note:** The Sophos SafeGuard software will attempt to connect to the network share for about 4 minutes. If it fails to connect, a balloon message will be displayed on the computer and an error logged. Additional attempts to connect to the network share will occur after each Windows logon until connection is established or a manual backup of the recovery key files is carried out on the computer.

9. Click **Next**. Then click **Finish** to complete initial configuration. SafeGuard Policy Editor will launch once the configuration wizard has closed.

You have now completed initial configuration. You have created a configuration package with a set of default policies as well as a key recovery share with the required access rights for the help desk. We recommend reading the remaining chapters within the Startup guide prior to deploying Sophos SafeGuard and the default policy configuration package on the endpoint computers. For information on deployment see [Install the encryption software and encryption configuration with a script](#), page 33.

## 10 Carry out additional configuration of the encryption software

The Sophos SafeGuard policies include all settings to implement a companywide security policy on the endpoint computers. They incorporate settings for the following areas (policy types):

Policy type	Content	SDE	SGE
General settings	Settings for logon recovery, POA customization etc.	✓	✓
Authentication	Settings for logon mode, number of logon attempts etc.	✓	✓
Passwords	Settings for user passwords, such as length, forbidden characters.	✓	✓
Device protection	Settings for encryption, such as volume selection	Settings for volume-based encryption	Settings for volume- and file based encryption, SafeGuard Data Exchange and SafeGuard Portable
Specific machine settings	Settings for the computer such as Power-on Authentication (activate/deactivate), Secure Wake On LAN, display options	✓	✓
Logging	Defines events to be logged.	✓	✓
Passphrase	Settings for SafeGuard Data Exchange passphrases		✓

With the default policies configuration your endpoint computers are well protected:

- Power-on Authentication is enabled.
- Volume-based-encryption for all internal hard disks is enabled.
- Recovering a forgotten password via Local Self Help is enabled and configured.
- Additionally, password recovery via Challenge/Response with help desk assistance is enabled.
- The key recovery file needed is automatically generated on each Sophos SafeGuard protected computer and stored in a network share created during initial configuration. Access permissions to this share are set by default.
- For SafeGuard Easy 5.50: File based encryption of removable media is enabled.

The default policies configuration does not cover the following areas which you should consider prior to deploying it on the endpoint computers:

- To cater for special access requirements for post-installation and administrative tasks on endpoint computers, create administrative access options: service accounts and POA access accounts.
- Define further advanced settings, e.g. define your own questions for Local Self Help.
- For recovering data in cases where the POA is corrupt, create special files (Virtual Clients) that are needed in a Challenge/Response procedure via a WinPE environment.
- Customize the Power-on Authentication to your company's preferences.

## 10.1 Creating policies

To create a new policy, do the following:

1. Log on to the SafeGuard Policy Editor with the password set during initial configuration.
2. Click **Policies** in the navigation area.
3. In the navigation window, right-click **Policy Items** and select **New**.
4. Select the policy type. A dialog for naming the policy of the selected policy type is displayed.
5. Enter a name and optionally a description for the new policy.

Policies for Device Protection:

When creating a policy for device protection, you also have to specify the target for device protection in this dialog. Possible targets are:

- Mass storage (boot volumes/other volumes)
- Removable media (Only supported for SafeGuard Easy installations.)
- Optical drives (Only supported for SafeGuard Easy installations.)

For each target, a separate policy has to be created. Later on you can combine the individual policies in a policy group named *Encryption*, for example.

6. Click **OK**.

The new policy is displayed in the **Policies** navigation area, below **Policy Items** on the left. In the action area on the right, all settings for the selected policy type are displayed and may be changed as required.

## 10.2 Combining policies into groups

### **Prerequisites:**

The individual policies of different types must have been created beforehand.

Sophos SafeGuard policies need to be combined to policy groups to be transferred inside a configuration package. A policy group may contain different policy types.

To group policies, do the following:

1. Click **Policies** in the navigation area.
2. In the navigation window, right-click **Policy Groups** and select **New**.
3. Click **New Policy Group**. A dialog for naming the policy group is displayed.
4. Enter a unique name and optionally a description for the policy group. Click **OK**.
5. The new policy group is displayed in the **navigation window** below **Policy Groups**.
6. Select the policy group. The action area shows all elements required for grouping the policies.
7. To add the policies to the group, drag them from the list of available policies to the policy area.
8. You can define a **priority** for each policy by arranging the policies in order using the context menu.

If you sum up policies of the same type in a group, the settings will be merged automatically. In this case, you can define priorities for utilizing the settings. The settings of a policy with a higher priority overwrite the settings of a policy with a lower priority. If an option is set to **not configured**, the setting will **not be overwritten** in a policy of a lower priority.

### **Exception concerning device protection:**

Policies for device protection will only be merged, if they were defined for the same target (e.g. boot volume). If they are pointed at different targets, the settings will be added.

9. Save the policy via **File > Save**.

The policy group now contains the settings of all individual policies. Next create a configuration package containing the policy group.

## 10.3 Creating a Sophos SafeGuard configuration package

**Note:** Policies are transferred to the endpoint computers inside a configuration package. After creating a new policy or editing an existing one, ensure to carry out the following steps. When using the default policies only, a configuration package is automatically created during initial configuration. In this case, you do not need to carry out the following steps.

To create a configuration package do the following:

1. In the SafeGuard Policy Editor, select the **Configuration Package Tool** from the **Tools** menu.
2. Click **Add Configuration Package**.
3. Enter a name of your choice for the configuration package.
4. Specify a **Policy Group** which must have been created beforehand in the SafeGuard Policy Editor, to be applied to the computers.
5. Under **Key Backup Location**, specify a shared network path for storing the key recovery file. Enter the share path in the following form: \\networkcomputer\, e.g. "\\mycompany.edu\". If you do not specify a path here, the end user will be prompted to name a storage location for this file when first logging on to the endpoint computer after installation.

The key recovery file is needed to enable recovery of Sophos SafeGuard protected computers and is generated on each Sophos SafeGuard protected computer.

Make sure to save this key recovery file at a file location accessible to the help desk, for example a shared network path. Alternatively the files can be provided to the help desk via different mechanisms. This file is encrypted by the company certificate. It can therefore be saved to any external media or to the network to provide it to the help desk for recovery purposes. It can also be sent by e-mail.

6. Under **POA Group**, you can select a POA access account group to be assigned to the endpoint computer. POA access accounts offer access for administrative tasks on the endpoint computer after the Power-on Authentication has been activated. To assign POA access accounts, the POA group must have been created beforehand in the **Users** area of the SafeGuard Policy Editor.
7. Specify an output path for the configuration package (MSI).
8. Click **Create Configuration Package**.

The configuration package (MSI) has now been created in the specified directory. You now need to distribute this package to the Sophos SafeGuard endpoint computers and deploy it to them.

## 10.4 Configure Local Self Help

With Local Self Help, users who have forgotten their password may even recover it without the assistance of a help desk. To do so, they simply answer a predefined number of questions in the Power-on Authentication. You can define the set of questions to be answered in the SafeGuard Policy Editor. A predefined question theme is also available. You can also grant the users the right to define their own questions.

**Note:** Local Self Help is already configured in the default policies with predefined questions. If you use the default policies, you do not have to carry out the following configuration steps.

To configure special Local Self Help settings, do the following:

1. In the navigation area of the SafeGuard Policy Editor, click **Policies**.
2. Create a new policy of the type **General Settings**.
3. Define the settings for Local Self Help under **Local Self Help (LSH)**:
  - a) In the **Enable Local Self Help** field, select **Yes**.
  - b) In the **Minimal length of answers** field, define the minimum number of characters the user has to enter when initially answering the questions.
  - c) In the **Welcome Text under Windows** field you can specify an individual information text to be displayed in the first dialog when launching the Local Self Help Wizard on the endpoint computer. Prior to selecting the text here, it has to be created and registered. For a detailed description of creating and registering information texts, refer to the Administrator help, *Registering welcome texts*.
  - d) To entitle users to define their own questions, select **Yes** in the **Users can define their own questions** field.

After defining the policy settings for enabling Local Self Help on the endpoint computers, you now define a question theme to be deployed with the policy.

In the **Policies** navigation area under **Local Self Help questions**, a predefined question theme is available. You can use it as is, edit it or delete it. The following steps describe how to create a new question theme and add questions.

4. In the **Policies** navigation area, select **Local Self Help questions**.
5. Right-click **Local Self Help questions** and select **New > Question Theme**.
6. Enter a name for the question theme and click **OK**.

7. In the **Policies** navigation area, select the new question theme under **Local Self Help questions**.
8. Right-click in action area to open the context menu for the question theme. In the context menu, select **Add**.

A new question line is added.

9. Enter your question and press **Enter**. To add further questions repeat this step.

The question theme must contain at least 10 questions.

10. To save your changes, click the **Save** icon in the toolbar.

Your question theme is registered and will be automatically deployed with the policy of the type **General Settings** enabling Local Self Help on the endpoint computers.

11. Add the policy to the policy group that is to be deployed in the configuration package to the endpoint computers.

The policy group with the **General Settings** policy is available for selection when creating a configuration package (via **Tools > Configuration Package Tool**), to be deployed on the endpoint computers. Via this policy group, Local Self Help is enabled on the endpoint computer. To be able to use Local Self Help, the user first has to activate this function by answering at least ten questions (see [Activate Local Self Help on the endpoint computer](#), page 23).

### 10.4.1 Activate Local Self Help on the endpoint computer

For Local Self Help to become active on endpoint computers, the user has to answer and store at least 10 questions.

1. After the policy has become effective on the endpoint computer, a balloon tool tip indicates that there are unanswered Local Self Help questions. The user restarts the computer.

The command **Local Self Help** is added to the context menu of the System Tray Icon in the Windows taskbar.

2. The user right-clicks the Sophos SafeGuard System Tray Icon and selects **Local Self Help**.

The Local Self Help Wizard **Welcome** dialog is displayed. The Local Self Help Wizard guides the user through the process of answering and storing questions.

After completing the wizard, Local Self Help is active on the endpoint computer.

## 10.5 Configure Challenge Response for data recovery

Easy recovery for encrypted volumes can be achieved when using specific files called Virtual Clients in cases where Challenge/Response would usually not be supported, for example when the POA is corrupted. They can be used by different computers and for several Challenge/Response sessions.

The Virtual Client files need to be created and must be available to the help desk prior to the Challenge/Response procedure.

1. In the SafeGuard Policy Editor, select the **Virtual Clients** area.
2. In the left-hand navigation window, click **Virtual Clients**.
3. In the toolbar, click **Add Virtual Client**.
4. Enter a unique name for the Virtual Client and click **OK**. Virtual Clients are identified in the database by these names.
5. Click the **Save** icon in the toolbar to save your changes to the database.
6. Select the respective Virtual Client in the action area and click **Export Virtual Client** in the toolbar. Select a storage location for the Virtual Client file recoverytoken.tok and confirm with **OK**.

The Virtual Client has been exported to the file recoverytoken.tok.

7. Copy the Virtual Client file recoverytoken.tok to a removable medium. We recommend using a memory stick.

Make sure to keep the storage medium in a safe place. Make the files available to the help desk and in the endpoint computer environment as they are needed for a Challenge/Response with Virtual Clients.

## 10.6 Customize the Power-on Authentication

You may customize the look of the POA to suit your preferences, for example background/logon image, information text, keyboard, dialog language. Create images and texts beforehand and register them in the SafeGuard Policy Editor. All further configuration is done via policies.

The POA can be customized as follows:

### ■ **Background and logon image**

By default the background and logon images that appear in the POA are in SafeGuard design. You can customize these images to show, for example, your company's logo.

Background and logon images are configured via a policy of the type **General Settings**.

For a detailed description, refer to the Administrator help, section *Background and logon image*.

### ■ **Customized information texts**

You can define customized information texts to be displayed in the POA, for example, information to be shown upon initiating a Challenge/Response procedure for logon recovery, legal notices or additional information to be displayed after logging on to the POA.

Depending on their type, these texts are configured via policies of the types **General Settings** or **Specific Machine Settings**.

For a detailed description refer to the Administrator help, section *User defined information text in the POA*.

### ■ **Language for the POA dialog text**

After installation of the Sophos SafeGuard encryption software, the POA dialog text is displayed in the default language which is set in Windows' Regions and Language Options on the endpoint computer when installing Sophos SafeGuard.

You can change the POA dialog text via a policy of the type **General Settings**.

For a detailed description, refer to the Administrator help, section *Language for POA dialog text*.

### ■ **Keyboard Layout**

As the default, Sophos SafeGuard adopts the keyboard layout in the POA which is set in the Windows **Regional and Language Options** at the time it is installed.

You can change the keyboard layout via the **Regional and Language Options**.

For a detailed description, refer to the Administrator help, section *Keyboard Layout*.

■ **Virtual keyboard**

Sophos SafeGuard provides a virtual keyboard for entering credentials by clicking the on-screen keys.

You can define whether the virtual keyboard should be available via a policy of the type **Specific Machine Settings**.

For a detailed description, refer to the Administrator help, section *Virtual keyboard*.

## 11 Configure administrative access on endpoint computers

To cater for access requirements for administrative tasks after the installation of Sophos SafeGuard on endpoint computers, you can configure the following administrative access options:

### ■ Service accounts for Windows Logon

With service accounts, users (for example, rollout operators, members of the IT team) can log on (Windows logon) to endpoint computers after the installation of Sophos SafeGuard without activating the Power-on Authentication and without being added as users to the computers.

### ■ POA access accounts for POA logon

POA access accounts are predefined accounts that enable users (for example members of the IT team) to log on (POA logon) to endpoint computers after the Power-on Authentication has been activated to perform administrative tasks.

For detailed descriptions of these options, see the Sophos SafeGuard Administrator help, sections *Service accounts for Windows Logon* and *POA access accounts for POA logon*.

### 11.1 Configure Service Account Lists

Do the following:

1. In the navigation area of the SafeGuard Policy Editor, click **Policies**.
2. In the policy navigation window, select **Service account lists**.
3. In the context menu of **Service account lists**, click **New > Service account list**.
4. Enter a name for the service account list and click **OK**.
5. Select the new list under **Service account lists** in the policy navigation window.
6. Right-click in the action area on the right-hand side to open the context menu for the service account list. In the context menu, select **Add**.
7. A new user line is added. Enter the **User Name** and the **Domain Name** in the respective columns and press **Enter**. To add further users, repeat this step.
8. Save your changes by clicking the **Save** icon in the toolbar.

The service account list is now registered. In the next steps you select it for assignment via policy.

9. Create a policy of the type **Authentication**.
10. Under **Logon Options**, select the service account list from the drop-down list of the **Service Account List** field.
11. Save your changes by clicking the **Save** icon in the toolbar.
12. Add the policy to the policy group that is to be deployed in the configuration package to the endpoint computers.

The policy group with the **Authentication** policy is available for selection when creating a configuration package (via **Tools > Configuration Package Tool**) to be deployed on the endpoint computers. Via this policy group, the service account list assigned to the endpoint computer.

## 11.2 Configure POA access accounts

Do the following:

1. Click **Users** in the navigation area of the SafeGuard Policy Editor.
2. In the **Users** navigation window under **POA**, select **POA Users**.
3. In the context menu of **POA Users**, click **New > Create new user**.

The **Create new user dialog** is displayed.

4. In the **Full name** field, enter a name, i.e. the logon name, for the new POA user. Optionally, enter a description for the new POA user.
5. Enter a password for the new POA access account and confirm it.

**Note:** To enhance security, the password should adhere to certain minimum complexity requirements, e.g., minimal length of 8 characters, mixture of numerical and alphanumerical characters etc. If the password you have entered is too short, a warning message will be displayed.

6. Click **OK**.

The new POA access account is created and the POA user (i.e. the POA access account) is displayed under **POA users** in the **Users** navigation area.

Repeat these steps to create further POA users.

In the next steps, you create a POA group that can be selected when creating configuration packages, and add the users to the group.

7. In the **Users** navigation window under **POA**, select **POA Groups**.

8. In the context menu of **POA Groups**, click **New > Create new group**.

The **Create new group** dialog is displayed.

9. In the **Full name** field, enter a name for the new POA group. Optionally, enter a description for the new POA group.

10. Click **OK**.

11. In the **Users** navigation window under **POA, POA Group**, select the new POA group.

In the action area of the SafeGuard Policy Editor on the right-hand side, the **Members** tab is displayed.

12. In the SafeGuard Policy Editor toolbar, click the **Add** icon (green plus sign).

13. Select the user, i.e. POA access account, you want to add to the group and click **OK**. Repeat this step for adding further users.

The POA Group is available for selection when creating a configuration package (via **Tools > Configuration Package Tool**) to be deployed on the endpoint computers.

## 12 Install the encryption software and encryption configuration on endpoint computers

Do the following:

1. Before you install the encryption software, prepare for installation on the endpoint computer, see [Prepare for installation](#), page 11.
2. To get to know Sophos SafeGuard, install the encryption software on a trial computer first.
3. Log on for the first time.
4. Then use your own tools to create and distribute an installation package to centrally set up the encryption software on the endpoint computers.

### 12.1 Carry out a trial installation

Before you install the encryption software, prepare for installation on the endpoint computer, see [Prepare for installation](#), page 11.

1. Log on to the computer as an administrator.
2. Install the MSI package SGxClientPreinstall.msi that provides the endpoint computer with the necessary requirements for a successful installation of the encryption software, for example the required DLLs.
3. Double-click the relevant “Client” MSI package to start the encryption software installation wizard. It guides you through the necessary steps. Install either of the following:

Sophos SafeGuard Disk Encryption	SafeGuard Easy
SDEClient.msi for the 32bit variant or SDEClient_x64.msi for the 64bit variant.	SGNClient.msi for the 32bit variant. SGNClient_x64.msi for the 64bit variant. For further Client MSI packages see the Administrator help, chapter <i>Installation</i> .

4. Accept the defaults on the next dialogs.

5. If prompted, select the install type. Customers installing SGNClient.msi or SGNClient\_x64.msi do either of the following:
  - Select **Complete** to install both Device Protection (volume based encryption) and Data Exchange (file based encryption).
  - Select **Typical** to install Device Protection only.
  - Select **Custom** and activate the features to your needs.

The feature **Data Exchange** is not available with SDE.

6. Accept the defaults on all further dialogs to complete the installation wizard.
7. Go to the location where you have saved the default configuration package (MSI) created during initial configuration in the SafeGuard Policy Editor.
8. Install this configuration package on the computer.

Sophos SafeGuard is installed with a default configuration on the endpoint computer. Next log on to the computer for the first time after installation.

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” functionality built into the POA. Hotkeys can be configured post installation from within the POA or via an additional configuration setting passed to the msixec deployment tool. For further information, see *Supported hotkeys in the POA* in the Administrator help as well as the following knowledgebase articles:

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

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

## **12.2 Logging on to an endpoint computer for the first time (without a service account)**

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

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 (Interactive logon: CTRL+ ALT+ DEL 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 will be displayed. Next time you log on you only need to enter your Windows credentials at the Power-on Authentication.

Initial encryption will start automatically. With default policies all internal disks will be encrypted. You may continue working and do not need to restart the computer after encryption is completed. Disks will be encrypted and decrypted transparently for editing without any user interaction. For further information see the User help (chapters *First logon after Sophos SafeGuard installation*, *First POA user logon example* and *Data Encryption*) for the behavior of the computer after Sophos SafeGuard installation.

## **12.3 Logging on to an endpoint computer using a service account**

At the first Windows logon after rebooting the computer, a user included on a service account list logs on to the respective machine as a Sophos SafeGuard guest user. This first Windows logon to the machine neither kicks off a pending Power-on Authentication nor adds the user to the computer. The Sophos SafeGuard System Tray icon balloon tool tip "Initial user synchronisation completed" will not be displayed.

### **12.3.1 Service account status display on the endpoint computer**

In addition, the guest user logon status can also be displayed via the System Tray Icon. For further information the System Tray Icon refer to the Sophos SafeGuard User help, chapter *System Tray icon and balloon tool tip* (description of the user state field).

## 12.4 Install the encryption software and encryption configuration with a script

Before you deploy the encryption software, prepare for installation on the endpoint computers, see [Preparing for installation](#), page 4.

Use your own tools to create a package to be installed on the endpoint computers. The package must include the following:

- **a script with the commands for the pre-configured installation**

We recommend using the Windows Installer command-line tool `msiexec` to create the script. For more information on `msiexec` see the Administrator help, chapter *Command for central install* or [http://msdn.microsoft.com/en-us/library/aa367988\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/aa367988(VS.85).aspx).

- **Sophos SafeGuard preparatory installation package**

Use `SGxClientPreinstall.msi`. The package provides the endpoint computers with the necessary requirements for a successful installation of the encryption software, for example the required DLL `MSVCR80.dll`, version 8.0.50727.4053.

**Note:** If this package is not installed, installation of the encryption software will be aborted.

- **Sophos SafeGuard encryption software installation package**

You will find it in the product folder that you downloaded from the Sophos website or on the product CD.

- **Configuration package(s)**

The configuration package(s) created beforehand in the SafeGuard Policy Editor. They contain the policies with the encryption configuration of the endpoint computers. Use the configuration package with predefined default policies created during initial configuration, for quick and easy policy deployment, or use the ones you created yourself.

1. Create a folder `Software` on the administrator computer to use as a central store for all applications.
2. To create the script, enter the commands at the command prompt with the command-line parameters as shown in the following example.

**Script example:**

```
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
```

```
■ msiexec /i F:\Software\Sophos\SafeGuard\SGxClientPreinstall.msi
msiexec /i F:\Software\Sophos\SafeGuard\SDEClient.msi
InstallDir=C:\Program Files\Sophos\Sophos SafeGuard
```

Installs the Sophos SafeGuard preparatory installation package and the encryption software from the specified storage location to the default installation directory C:\Program Files\Sophos\Sophos SafeGuard. Installs Sophos SafeGuard Device Encryption (volume based encryption) and Power-on Authentication.

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

Installs the Sophos SafeGuard 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 useful log file that can be analyzed automatically by using the Windows Installer tool wilogutl.exe.

```
■ /qn
```

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

3. Distribute the installation and configuration package via company software distribution mechanisms to the endpoint computers.

The encryption software and the configuration package(s) will be installed on the endpoint computers and the computers will be encrypted.

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” functionality built into the POA. Hotkeys can be configured post installation from within the POA or via an additional configuration setting passed to the Windows Installer command `msiexec`. For further information, see the Administrator help, chapter *Supported hotkeys in the POA* as well as the following knowledgebase articles:

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

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

## 13 Recover a forgotten password

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

- The user may recover it themselves via Local Self Help (recommended).
- The help desk may recover it via a Challenge/Response procedure.

### 13.1 Recover a forgotten password via 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, 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. The user clicks **Local Self Help**.

The Local Self Help Welcome dialog is displayed.

3. In the following five dialogs, the user answers five 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 display the password by pressing Enter, the spacebar or by clicking the blue display box.

The password will be shown for 5 seconds at the maximum. Afterwards the boot process will continue automatically. The user can hide the password immediately by pressing Enter, the spacebar or by clicking the display box again.

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

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

## 13.2 Recover a forgotten password via 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. The help desk needs the relevant permissions to perform recovery actions. Challenge/Response must be enabled via policy for the endpoint computer.

**Note:** We recommend to primarily use Local Self Help to recover a forgotten password. With recovery via Local Self Help the user can have the current password displayed in a confidential way in the Power-on Authentication and may continue using this password. This will avoid that the password has to be reset at all and will also avoid help desk assistance.

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 available for logon recovery, the user selects **Challenge/Response**.

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

3. The user clicks **Next**. A random challenge code will be 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. The help desk launches the Recovery Wizard in the SafeGuard Policy Editor.
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 form of an ASCII character string will be generated and displayed.

7. The help desk provides the user with the response code e.g. via 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 boot through Power-on Authentication.

9. In the Windows logon dialog, the user does not know the correct password either and therefore needs to change it at Windows level. This requires further recovery actions outside the scope of Sophos SafeGuard, via standard Windows means. We recommend using the following methods to reset the password at Windows level.
  - Via a service or administrator account available on the endpoint computer with the required Windows rights.
  - Via 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 the user.
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, the definition of a new password without providing the old one requires a new certificate. The user has to confirm this procedure.
13. A new user certificate will be created based on the newly chosen Windows password. This enables the user to log on to the computer again and to log on at the Power-on Authentication with the new password.

The user may resume working.

## 14 Recover access to the system

Sophos SafeGuard offers several convenient recovery options in critical situations, for example when the POA is corrupt and the user can no longer access encrypted data or when the Master Boot Record is damaged.

### 14.1 Recover data via Challenge/response using Virtual Clients

Data recovery using Virtual Clients is based on a Challenge/Response procedure. This recovery type can be applied when under special circumstance the operating system cannot be started any more. This might be due to a corrupt driver configuration, for example.

In this case, access to the encrypted data can be regained by booting the computer via a Windows PE recovery disk customized for Sophos SafeGuard and by initiating a Challenge/Response procedure using Virtual Clients. For further information see the Administrator help, chapter *Recover access to the system*.

To regain access to encrypted data on the computer, do the following:

1. Obtain the Sophos SafeGuard recovery disk from technical support.

The help desk may download the Windows PE recovery disk with the latest Sophos SafeGuard filter drivers from the Sophos support site. For further information see the knowledgebase: <http://www.sophos.com/support/knowledgebase/article/108805.html>.

2. Configure the Virtual Client in the SafeGuard Policy Editor.
3. Boot the computer from the recovery disk.
4. Import the Virtual Client file into the KeyRecovery Tool.
5. Initiate the Challenge in the KeyRecovery Tool.
6. Confirm the Virtual Client in the SafeGuard Policy Editor.
7. Enter the challenge code in the SafeGuard Policy Editor.
8. Generate the response code in the SafeGuard Policy Editor.
9. Enter the response code into the KeyRecovery Tool.

Access to the data stored on this partition is recovered.

## 14.2 Recover data by booting from an external medium

This recovery type can be applied when the user can still log on at the POA, but cannot access the encrypted volume any more. In this case, access to the encrypted data can be regained by booting the computer via a Windows PE recovery disk customized for Sophos SafeGuard.

### Prerequisites:

- The user booting from the external medium must have the right to do so. This right can either be configured in the SafeGuard Policy Editor within a policy of type **Authentication (User may decrypt volume set to Yes)** or can be obtained for one-time use via a Challenge/Response procedure.
- The computer must support booting from different media than the fixed hard drive.

To regain access to encrypted data on the computer, do the following:

1. Obtain the Sophos SafeGuard Windows PE disk from technical support.

The help desk may download the Windows PE recovery disk with the latest Sophos SafeGuard filter drivers from the Sophos support site. For further information see the knowledgebase: <http://www.sophos.com/support/knowledgebase/article/108805.html>.

2. Log on at the Power-on Authentication with your credentials.
3. Insert the Windows PE recovery disk into the computer.
4. In the POA logon dialog under **Continue booting from:** select **external medium**. The computer is started.

Access to the data stored on this partition is recovered.

## 14.3 Recover a computer with a corrupt Master Boot Record

After a Sophos SafeGuard installation on the endpoint computer, a copy of the original Master Boot Record (MBR) is saved and stored in the computer's system kernel. If the MBR is corrupted, this might lead to an unbootable system. For recovering systems with a corrupt MBR Sophos SafeGuard offers the convenient recovery tool `BE_Restore.exe`. The following possibilities exist:

- Restore the MBR from a backup
- Repair the MBR

For a detailed description on this type of recovery see the Sophos SafeGuard Tools guide, chapter *Restoring a corrupted MBR*.

## 15 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 or User help for all further information.

Task	Manual/Chapter
Log on to the SafeGuard Policy Editor.	Administrator help, Logon to the SafeGuard Policy Editor
Log on to the Sophos SafeGuard protected computer	User help, Power-on Authentication
Ensure correct functioning of the Power-on Authentication	Administrator help/User Help, Supported Hotkeys in the Power-on Authentication
Displaying 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 company and Master Security Officer certificate.
Create administrative access to endpoint computers.	Administrator help, Administrative access to endpoint computers
Recover a password via Local Self Help	Administrator help/User help, Recovery via Local Self Help
Recover a password via Challenge/Response	Administrator help/User Help, Recovery via Challenge/Response
Recover data on endpoint computers.	Administrator help, Challenge/Response using Virtual Clients
Recover a corrupt Master Boot Record	Tools guide, Restoring a corrupted MBR
Upgrade SDE 4.60 or SGE 4.3x -4.5x to Sophos SafeGuard	Administrator help, Upgrading SafeGuard Easy 4.x/ SophosDisk Encryption 4.x to Sophos SafeGuard 5.5x

## 16 Technical support

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

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

## **17 Copyright**

Copyright © 1996 - 2010 Sophos Group and Utimaco Safeware AG. All rights reserved.

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

Sophos is a registered trademark of Sophos Plc and the Sophos Group. SafeGuard is a registered trademark of Utimaco Safeware AG - a member of the Sophos Group. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

All SafeGuard Products are copyright of Utimaco Safeware AG - a member of the Sophos Group, or, as applicable, its licensors. All other Sophos Products are copyright of Sophos plc., or, as applicable, its licensors.

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