

SOPHOS

Sophos SafeGuard Disk Encryption 5.50 Sophos SafeGuard Easy 5.50 Administrator help

Document date: November 2010



Content

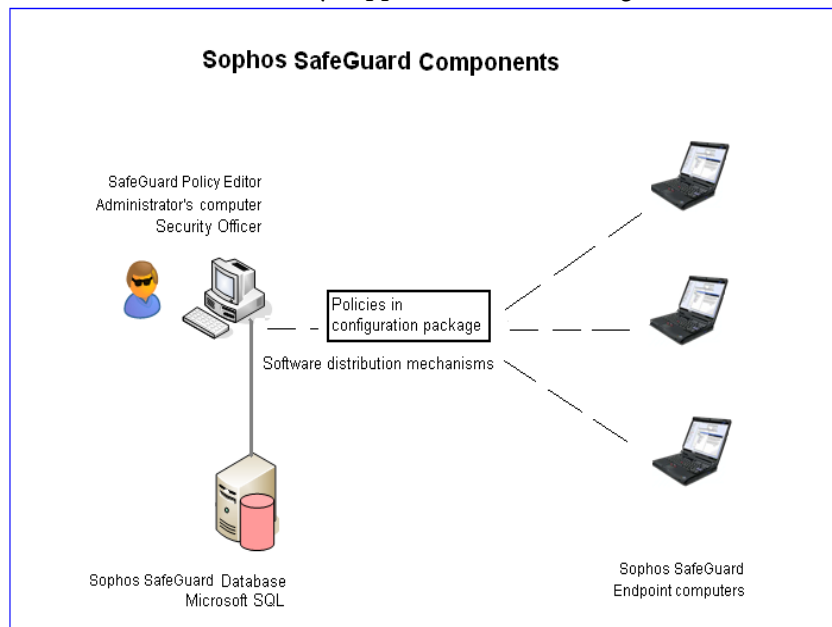
1	About Sophos SafeGuard	3
2	SafeGuard Policy Editor	5
3	Sophos SafeGuard on endpoint computers.....	7
4	Data encryption.....	8
5	Getting started	11
6	Installation	17
7	Installing the Sophos SafeGuard encryption software on computers with multiple operating systems	35
8	Logon to the SafeGuard Policy Editor.....	38
9	Working with policies	39
10	Working with configuration packages.....	43
11	Exporting company and Master Security Officer certificate.....	45
12	Restoring a corrupt SafeGuard Policy Editor installation	47
13	Restoring a corrupt database configuration	48
14	Administrative access to endpoint computers.....	49
15	Default Policies.....	61
16	Policy Settings.....	68
17	SafeGuard Data Exchange.....	100
18	Power-on Authentication (POA).....	102

19	Recovery options.....	112
20	Recovery via Local Self Help.....	113
21	Recovery via Challenge/Response.....	119
22	System Recovery.....	135
23	Preventing uninstallation from the endpoint computers.....	138
24	Updating Sophos SafeGuard	139
25	Upgrading Sophos SafeGuard 5.5x to SafeGuard Enterprise	143
26	Upgrading SafeGuard Easy 4.x/ Sophos SafeGuard Disk Encryption 4.x to Sophos SafeGuard 5.5x.....	145
27	Technical support.....	153
28	Copyright	154

1 About Sophos SafeGuard

Sophos SafeGuard is a state-of-the-art data security solution that uses a policy-based encryption strategy to provide powerful protection of information on endpoint computers.

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



1.1 Product bundles

Sophos SafeGuard is available with different product bundles: SGE (SafeGuard Easy) and ESDP (Endpoint Security and Data Protection). From version 5.50 SGE is the new product name for SafeGuard Enterprise Standalone. For each bundle, different modules and functions are available. The modules and functions not available for ESDP are marked by notes in this manual.

1.2 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>A set of default policies as well as a default configuration package for the endpoint computers may be created during initial configuration.</p> <p>The SafeGuard Policy Editor also provides recovery functions to regain access to endpoint computers, if users have for example, forgotten their password.</p>
Sophos SafeGuard Database	<p>Sophos SafeGuard Database holds all the relevant data concerning the policy settings for the endpoint computers.</p>
Sophos SafeGuard software on endpoint computers	<p>Encryption software on endpoint computers.</p>

2 SafeGuard Policy Editor

The SafeGuard Policy Editor is the management tool for Sophos SafeGuard protected computers that are managed locally.

The SafeGuard Policy Editor is installed on the computer that you want to use to carry out administrative tasks. As a security officer, you use the SafeGuard Policy Editor to manage Sophos SafeGuard policies and to create configuration settings for endpoint computers. The policies and settings are exported to configuration packages and deployed to the endpoint computers. Several configuration packages can be created, and distributed via third party mechanisms. The packages can be distributed when installing the Sophos SafeGuard encryption software. For changing settings on the endpoint computers afterwards, further configuration packages can be deployed.

The SafeGuard Policy Editor also provides recovery functions to regain access to endpoint computers, if users have, for example forgotten their password.

2.1 Features

For your convenience and to ease administration SafeGuard Policy Editor offers the following:

- **Default configuration:** A configuration package with pre-configured recommended policies for the endpoint computers can be created by default during initial configuration of the SafeGuard Policy Editor. Should the default policies not cover all your specific requirements, you can define your own policies in the SafeGuard Policy Editor.
- **Administrative access options:** To cater for special access requirements for post-installation and administrative tasks on endpoint computers Sophos SafeGuard offers the administrative access options service accounts and POA access accounts.
- **Encryption keys:** An automatically generated machine key will be used for SafeGuard Device Encryption (volume based encryption). For SafeGuard Data Exchange (file based encryption), keys generated locally on the endpoint compute will be used. SafeGuard Data Exchange is not available with ESDP (Endpoint Security and Data Protection).
- **Local Self Help:** For recovery of forgotten passwords Sophos SafeGuard offers the convenient recovery option Local Self Help. Local Self Help enables users to recover their password even without the assistance of a help desk.
- **Challenge/Response with help desk assistance:**

Challenge/Response with help desk assistance can be requested by a user in case a password has been forgotten or typed in incorrectly too often. It can also be applied to recover data in the scenario where the POA has become corrupted. Challenge/Response is based on specific key recovery files that are automatically generated when the Sophos SafeGuard endpoint computer is deployed.

2.2 Database

The Sophos SafeGuard policies are stored in an SQL database on the administrator's computer. You are prompted to install Microsoft SQL Server 2005 Express during the SafeGuard Policy Editor installation if an existing SQL server instance is unavailable. For this purpose, Microsoft SQL 2005 Express is included in your product delivery.

2.3 Upgrade

You can easily upgrade to the SafeGuard Enterprise suite with central management to make use of the full functionality of SafeGuard Enterprise.

2.4 Logging

Events for Sophos SafeGuard protected computers are logged in the Windows Event Viewer.

2.5 Differences to the SafeGuard Management Center

Due to a central management server the SafeGuard Management Center offers enhanced management functionalities, such as:

- Active Directory import with user and domain management.
- Central logging.
- Definable administrative roles.

The SafeGuard Management Center is available with SafeGuard Enterprise.

Note: You can also define settings and create configurations packages for Sophos SafeGuard computers that do not have any connection to a SafeGuard Enterprise Server in the SafeGuard Management Center.

3 Sophos SafeGuard on endpoint computers

Data encryption and protection against unauthorized access are the main security functions of Sophos SafeGuard. Sophos SafeGuard can be seamlessly integrated into the user's normal environment and is easy and intuitive to use. The Sophos SafeGuard authentication system, Power-on Authentication (POA), provides the necessary access protection and offers user-friendly support when recovering credentials.

3.1 Supported modules

The following modules are provided for the endpoint computers:

■ SafeGuard Device Encryption

- **Volume based encryption:** Ensures that all data on the specified volumes (such as boot volume, hard disk, partitions) is transparently encrypted (incl. boot files, swapfiles, idle files/hibernation files, temporary files, directory information etc.) without the user having to change normal operating procedures or consider security.
- **Power-on Authentication:** User logon is performed immediately after switching on the computer. After successful Power-on Authentication the user will be automatically logged on to the operating system.

■ SafeGuard Data Exchange

Easy data exchange with removable media on all platforms without re-encryption.

- **File based encryption:** All mobile writable media including external hard disks and USB sticks are encrypted transparently.

Note: This module is not supported with ESDP (Endpoint Security and Data Protection).

4 Data encryption

The core of Sophos SafeGuard is the encryption of data on different data storage devices. Encryption can be volume or file-based with different keys and algorithms.

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

Files are encrypted transparently. When users open, edit and save files, they are not prompted for encryption or decryption.

During first-time configuration in the SafeGuard Policy Editor, a default policy with pre-defined encryption settings is automatically created, see [Default Policies](#), page 61.

You can specify settings for encryption in a security policy of the type **Device Protection**. For further information, see [Working with policies](#), page 39 and see [Device Protection](#), page 86.

4.1 Volume-based encryption

With volume-based encryption, all data on a volume (including boot files, pagefiles, hibernation files, temporary files, directory information etc.) are encrypted. Users do not have to change normal operating procedures or consider security.

Note: If an encryption policy exists for a volume or a volume type and encryption of the volume fails, the user is not allowed to access it.

4.1.1 Fast initial encryption

Fast initial encryption is a special mode for volume-based encryption. It reduces the time needed for initial encryption (or final decryption) of volumes on endpoint computers by accessing only disk space that is actually in use.

For fast initial encryption, the following prerequisites apply:

- Fast initial encryption only works on NTFS-formatted volumes.
- NTFS-formatted volumes with a cluster size of 64 KB cannot be encrypted with the fast initial encryption mode.

Note: This mode leads to a less secure state if a disk has been employed before its current usage. Unused sectors may still contain data. Therefore, the fast initial encryption mode is disabled by default.

To enable fast initial encryption, select the volume-based setting **Fast initial encryption** in a policy of the type **Device Protection**.

Note: For volume decryption, the fast initial encryption mode will always be used, regardless of the specified policy setting. For decryption, the prerequisites listed also apply.

4.1.2 Volume-based encryption and Windows 7 system partition

For Windows 7 Professional, Enterprise and Ultimate, a system partition is created on endpoint computers without a drive letter assigned. This system partition cannot be encrypted by Sophos SafeGuard.

4.1.3 Volume-based encryption and Unidentified File System Objects

Unidentified File System Objects are volumes that cannot be clearly identified as plain or device-encrypted by SafeGuard Enterprise. If an encryption policy exists for an Unidentified File System Object, access to this volume will be denied. If no encryption policy exists, the user can access the volume.

Note: If an encryption policy with **Key to be used for encryption** set to an option that enables key selection (for example, **Any key in user key ring**) exists for an Unidentified File System Object volume, there is a period of time between the key selection dialog being displayed and access being denied. During this time period the volume can be accessed. As long as the key selection dialog is not confirmed, the volume is accessible. To avoid this, specify a preselected key for encryption. For further information on the relevant policy settings, see [Device Protection](#), page 86. This period of time also occurs for Unidentified File System Object volumes connected to an endpoint computer, if the user has already opened files on the volume when an encryption policy takes effect. In this case, it cannot be guaranteed that access to the volume will be denied as this could lead to data loss.

4.1.4 Encryption of volumes with enabled Autorun functionality

If you apply an encryption policy to volumes for which Autorun is enabled, the following can occur:

- The volume is not encrypted.
- If the volume is an Unidentified File System Object (see [Volume-based encryption and Unidentified File System Objects](#), page 9), access is not denied.

4.2 File-based encryption

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

File-based encryption ensures that all data is encrypted, apart from Boot Medium and directory information. With file-based encryption, even optical media such as CD/DVD can be encrypted. Also, data can be exchanged with external computers on which SafeGuard Enterprise is not installed, if policies permit.

Note: Data encrypted using “file-based encryption” cannot be compressed. Nor can compressed data be file-based encrypted.

Note: Boot volumes are never file-based encrypted. They are automatically exempted from file-based encryption, even if a corresponding rule is defined.

To apply file-based encryption to endpoint computers, create a policy of the type **Device Protection** and set the **Media encryption mode** to **File-based**. For further information, see [Device Protection](#), page 86.

4.2.1 Excluding applications from encryption

You can define applications to be ignored by the Sophos SafeGuard filter driver and thereby excluded from transparent encryption/decryption.

One example is a backup program. To ensure that data is not decrypted when creating a backup, this application can be exempted from encryption/decryption. The data is backed up in encrypted form.

A typical use case is for example to define backup programs as exempted so they will always be able to read and back up encrypted data.

Applications which might trigger malfunctions when used alongside Sophos SafeGuard, but do not require encryption, can generally be exempted from encryption.

You can define applications to be excluded from encryption/decryption in a policy of the type **Device Protection** with the target **Local Storage Devices**. The full name of the executable file (optionally including path information) is used to specify **Unhandled Applications**.

For further information, see [Device Protection](#), page 86.

5 Getting started

This chapter explains how to prepare for your Sophos SafeGuard installation successfully.

5.1 Deployment strategy

Before deploying Sophos SafeGuard on endpoint computers, it is recommended to define a deployment strategy taking specific requirements and available options into account.

The following options should be considered when defining a Sophos SafeGuard deployment strategy:

5.1.1 Policies

For policies, Sophos SafeGuard offers the following options:

- **Default policies**

Sophos SafeGuard offers predefined default policies for quick and easy policy deployment. During initial configuration in the SafeGuard Policy Editor a policy group with pre-defined encryption and authentication settings is created by default. For configuring endpoint computers, a configuration package containing these default policies is automatically created. For details on default policies and the settings defined in them, see [Default Policies](#), page 61.

- **Defining your own policies**

Should the default policies not cover all your specific requirements, you can define your own policies in the SafeGuard Policy Editor.

For details on creating policies, see [Working with policies](#), page 39. For details on deploying policies on endpoint computers, see [Working with configuration packages](#), page 43.

For a detailed description of all available policies and settings, see [Policy Settings](#), page 68.

5.1.2 Administrative access options

To cater for access requirements for administrative tasks after the installation of Sophos SafeGuard on endpoint computers, Sophos SafeGuard offers administrative access options for two different scenarios:

■ 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 POA users to the computers.

Service account lists are assigned to endpoint computers via policies. They should be assigned in the first Sophos SafeGuard configuration package you create for the configuration of the endpoint computers. Service Account lists can be updated by creating a new configuration package and deploying it to the endpoint computers.

For further details on service account lists, see [Service account lists for Windows logon](#), page 49.

■ POA access accounts for POA logon

POA access accounts are predefined local accounts that enable users (for example members of the IT team) to log on to endpoint computers to perform administrative tasks after the POA has been activated. POA access accounts enable POA logon, there is no automatic logon to Windows.

You can create POA access accounts in the SafeGuard Policy Editor, group them in POA access account groups, and assign groups to endpoint computers via Sophos SafeGuard configuration packages.

For further details on POA access accounts, see [POA access accounts for POA logon](#), page 54.

5.1.3 Recovery options

For situations requiring recovery (for example, forgotten passwords), Sophos SafeGuard offers two recovery options:

■ 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 helpdesk. To regain access to their computer, they simply answer a predefined number of questions in the Power-on Authentication.

In the default policies, Local Self Help is enabled and configured by default. If you do not use the default configuration, you have to enable Local Self Help via policy and define the questions to be answered by the end user.

For further details, see [Recovery via Local Self Help](#), page 113.

■ **Recovery via Challenge/Response**

The Challenge/Response recovery mechanism is a secure and efficient logon recovery system that helps users who cannot log on to their computers or access encrypted data. For Challenge/Response the assistance of a helpdesk is required.

In the default policies, Challenge/Response is enabled by default. If you do not use the default configuration, you have to enable Challenge/Response via policy. For data recovery via Challenge/Response you need to create specific files called Virtual Clients in the SafeGuard Policy Editor beforehand.

For further details, see [Recovery via Challenge/Response](#), page 119 and see [Creating a Virtual Client](#), page 126.

5.2 System requirements

Refer to the Startup guide for details on the system requirements for hardware and software, service packs and the disk space required during the installation and for effective operation.

5.2.1 Specific system requirements for endpoint computers

- 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.

5.3 Preparing for installation

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

5.3.1 General preparations

- To install the software and to operate the SafeGuard Policy Editor you need Windows administrator rights.
- Close all open applications.
- Ensure that there is enough free hard disk space. Information about this may be found in the Startup Guide.
- Read the release notes carefully.

5.3.2 Preparations for encryption

- A user account must be set up and active on the endpoint computers.
- Create a full backup of the data on the endpoint 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://ftp.ou.utimaco.de/>

For further information, see [Supported Hotkeys in the Power-on Authentication](#), page 109 in the Administrator help 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. You will find more information on this subject in the knowledgebase: <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. You will find more information on this subject in the knowledgebase: <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 that the MBR be "rewritten". To install Sophos SafeGuard you need a "spotless" master boot record. The use of imaging/cloning programs may have affected the state of this record.

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 knowledgebase: <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 yet been restarted, 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 should reboot the computer once before Sophos SafeGuard is installed.

5.4 Language settings

The language settings for the setup wizards, the SafeGuard Policy Editor and Sophos SafeGuard on the endpoint computers are as follows:

5.4.1 Setup wizard language

The installation and configuration wizards use the language setting of the operating system. English, German, French and Japanese are supported. If the operating system language is not available for the setup wizards, they will default to English.

5.4.2 SafeGuard Policy Editor language

You can set the language of the SafeGuard Policy Editor inside the SafeGuard Policy Editor:

- Open menu Tools > Options > General. Activate **Use user defined language** and select an available language. English, German, French and Japanese are supported.
- Restart the SafeGuard Policy Editor and it will be displayed in the selected language.

5.4.3 Sophos SafeGuard language on endpoint computers

You set the language of Sophos SafeGuard on the endpoint computer via a policy of type General in the SafeGuard Policy Editor, setting Customization > Client language:

- If the language of the operating system is selected, Sophos SafeGuard uses the language setting of the operating system. If the operating system language is not available in Sophos SafeGuard, the Sophos SafeGuard language will default to English.
- If one of the available languages is selected, Sophos SafeGuard product parts will be displayed in the selected language on the endpoint computer.

5.5 Interaction with other SafeGuard products

Please note the following interactions:

5.5.1 Interaction with SafeGuard LAN Crypt

Note the following:

- SafeGuard LAN Crypt 3.7x and Sophos SafeGuard 5.50 can coexist on the same computer and are fully compatible.
- SafeGuard LAN Crypt with versions below 3.7x and Sophos SafeGuard 5.5x cannot coexist on one computer.

If you are trying to install Sophos SafeGuard 5.50 on a computer with an already installed SafeGuard LAN Crypt of version 3.6x or below, the setup will be cancelled and a respective error message will be displayed.

5.5.2 Interaction with SafeGuard PrivateCrypto and SafeGuard PrivateDisk

Sophos SafeGuard 5.5x and the standalone products SafeGuard PrivateCrypto from version 2.30 as well as SafeGuard PrivateDisk from version 2.30 can coexist on the same computer.

5.5.3 Interaction with SafeGuard Removable Media

The SafeGuard Data Exchange module and SafeGuard Removable Media cannot coexist on the same computer. Before you install the SafeGuard Data Exchange module on an endpoint computer, check if SafeGuard Removable Media is already installed. In this case you have to uninstall SafeGuard Removable Media prior to installing SafeGuard Data Exchange on the endpoint computer.

Note: SafeGuard DataExchange is not available with ESDP.

6 Installation

Setting up Sophos SafeGuard involves the following:

	Task	Installation package/tool	
		ESDP	SGE
1	Set up the computer that is used for Sophos SafeGuard administration.		
	Install SafeGuard Policy Editor.	SDEPolicyEditor.msi	SGNPolicyEditor.msi
	Carry out initial configure in the SafeGuard Policy Editor creating a default configuration for the encryption software.	SafeGuard Policy Editor Configuration Wizard	
2	Tailor the Sophos SafeGuard encryption software (optional)		
	Create further configuration settings via user-defined policies, e.g. service account lists.	SafeGuard Policy Editor Policies area	
	Generate further configuration package(s) (MSI) including user-defined policies.	SafeGuard Policy Editor Configuration Package Tool	
3	Setup Sophos SafeGuard encryption software on the endpoint computers.		
	Provide endpoint computers with necessary requirements for successful installation of the Sophos SafeGuard encryption software.	SGxClientPreinstall.msi	SGxClientPreinstall.msi
	To apply Sophos SafeGuard Device Encryption (volume based encryption), install:	SDEClient.msi or	SGNClient.msi Note: In addition, Sophos SafeGuard Data Exchange (file based encryption) can be manually enabled in this package.
	To apply Sophos SafeGuard Data Exchange (file based encryption) only, install:	not available with ESDP	SGNClient_withoutDE.msi
	Deploy configuration package(s) to the endpoint computers.	Generated <Configpackage>.msi	

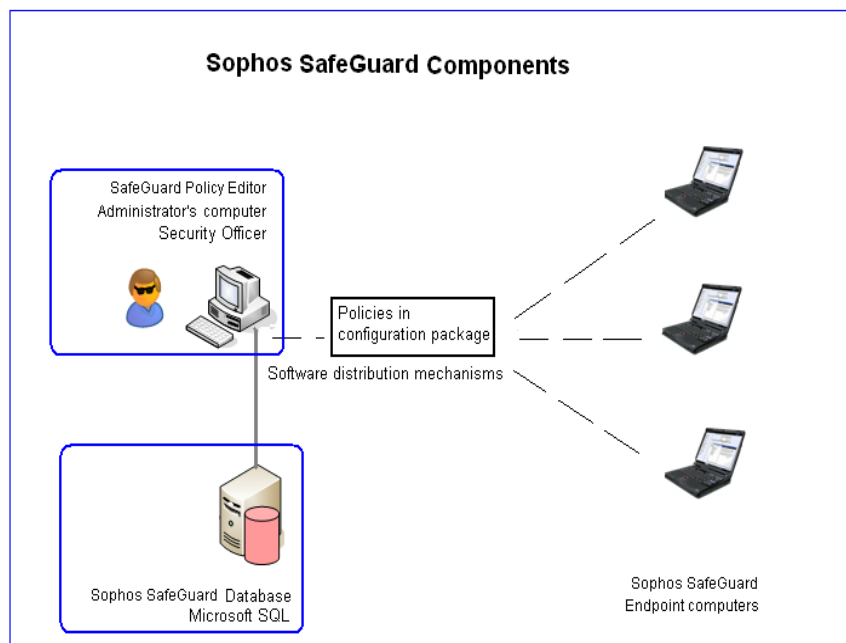
Note: When the operating system of the endpoint computer is Windows 7 64 bit or Windows Vista 64 bit, you may install the 64 bit variant of the “Client” package where available (<package name>_x64.msi).

6.1 Installing SafeGuard Policy Editor

Prerequisites:

The following prerequisites must be met:

- You need Windows administrator rights.
- If you want to use an already installed Microsoft SQL database server, you need the necessary SQL access rights and account data.
- .NET Framework 3.0 Service Pack 1 must be installed on the administrator's computer. You may download it for free from <http://www.microsoft.com/downloads>.



To deploy the encryption software to endpoint computers, first install the SafeGuard Policy Editor on an administrator's computer. You can also do the first time installation of 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.

1. Customers of ESDP double-click the SDEPolicyEditor.msi. Customers of SGE double-click the SGNPolicyEditor.msi. A wizard will guide you through the necessary steps.
2. Click **Next** in the welcome window.
3. Accept the license agreement.

4. Confirm the default installation path.

An SQL database instance is used to store Sophos SafeGuard policy settings. You may be prompted to install Microsoft SQ 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 SQL user account.

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

The SafeGuard Policy Editor is installed on the administrator's computer. Next you carry out the initial configuration in the SafeGuard Policy Editor.

6.2 Carry out initial configuration in the SafeGuard Policy Editor Configuration Wizard

You need to have Windows administrator rights.

1. After installation, 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**.

6.2.1 Configuring the database

A database is used to store all Sophos SafeGuard encryption policies and settings. The workflow depends on whether you create a new database with a first time installation or use an existing database. Using an existing database can be useful when you want to install additional instances of the SafeGuard Policy Editor, for example to enable help desk staff to carry out Challenge/Response.

1. On the **Database** page, do either of the following:
 - For a first time installation, activate **Create a new database**.
 - For an additional installation or to reuse a previously created database, activate **Use an existing database**. Under **Database name**, select the name of the database from the list.

2. Under **Database settings** do either of the following:
 - If only the pre-installed Microsoft SQL Express is available, the instance will already be displayed in **SQL Server Instance**. Your Windows credentials will be used as the SQL access account. Click **Next**.
 - If you use an existing database or if you have more than one SQL Server instance installed, click **Change** to select the one you want to use. A dialog is displayed where you have to configure the connection to the selected server. When finished, the selected settings will be displayed here. Click **Next**.

The connection to the database server has been established.

6.2.1.1 Carry out additional configuration of the database connection

Do the following:

1. In **Database Connection** under **Database Server**, select the required SQL database server from the list. All database servers available on your computer or network will be displayed. (The list is updated every 12 minutes). Activate **Use SSL** to secure the connection to this database server with SSL.
2. Under **Authentication**, select the type of authentication to be used to access the database:
 - Activate **Use Windows NT Authentication** to use your Windows credentials.

Note: Use this type when your computer is part of a domain. However, additional configuration might be required as the user needs to be authorized to connect to the database.

- Activate **Use SQL Server Authentication** to access the database with your SQL credentials. You will be prompted to enter and confirm them. Where necessary, you may obtain this information from your SQL administrator.

Note: Use this type when your computer is not part of a domain. Ensure to activate **Use SSL** to secure the connection to and from the database server. However, SSL encryption requires a working SSL environment on the computer on which the selected SQL database resides which you have to set up in advance. For further information see: <http://www.sophos.de/support/knowledgebase/article/108339.html>. With SQL authentication an upgrade to the SafeGuard Management Center can be easily achieved at a later point in time.

3. Click **Check connection**. If the connection to the SQL database has been established, a corresponding success message will be displayed.
4. Confirm with **OK** twice.

6.2.2 Creating the security officer certificate (new database)

For a first time installation and when creating a new database a security officer certificate will be created for authentication purposes. Only one account is created per installation. As security officer you access the SafeGuard Policy Editor to create Sophos SafeGuard policies and configure the encryption software for the end users. For recovering a broken database configuration, see [Restoring a corrupt database configuration](#), page 48.

1. On the **Security Officer** page, the security officer name is already displayed.
For installations with ESDP the security officer name is always Administrator. For all other installations the current user name is displayed.
2. Enter and confirm a password that you will need to access the SafeGuard Policy Editor.
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 to carry out recovery tasks.
3. Confirm the defaults with **Next**.

The newly created security officer certificate is stored in the certificate store. Next the company certificate will be created.

6.2.3 Importing the security officer certificate (when using an existing database)

When using an existing database the security officer certificate needs to be imported. Only certificates generated by the SafeGuard Policy Editor may be imported. Certificates created by a PKI (e.g. Verisign) are not allowed.

1. On the **Security Officer** page, click **Import** to import the security officer certificate.
2. Browse for the required certificate and confirm with **Open**.
3. Enter the password for the selected key file that you have used to authenticate at the SafeGuard Policy Editor.
4. Confirm the certificate with **Yes**.
5. Enter and confirm a password for authenticating at the SafeGuard Policy Editor.
6. Click **Next** and then **Finish** to complete the initial configuration.

Initial configuration in the SafeGuard Policy Editor is completed.

6.2.4 Creating the company certificate

The company certificate is used to secure policy settings in the database and on the Sophos SafeGuard protected computers. For recovering a broken database configuration, see [Restoring a corrupt database configuration](#), page 48.

1. On the **Company** page, enter a **Company name**. Ensure that **Automatically create certificate** is activated.

For a first time installation and when you have created a new database **Automatically create certificate** is already activated. The name is limited to 64 characters.

2. Click **Next**.

The newly created company certificate is stored in the database.

6.2.5 Backing up certificates

For recovery purposes the created security officer and company certificates need to be backed up to a safe location.

1. On the **Certificate Backup** page, specify a storage location for the certificate backups.
2. Confirm the storage location with **Next**.

The certificates will be backed up to the specified location.

Note: 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. You will need them to restore a broken installation or a corrupt database, see [Exporting company and Master Security Officer certificate](#), page 45.

6.2.6 Creating default policies

To minimize administration effort default policies are provided which cover a set of recommended configuration settings. A configuration package (MSI) containing these default policies will be created as part of the initial configuration. For detailed information on the default policies, see [Default Policies](#), page 61.

Note: 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.

1. On the **Default Policy** page, ensure that **Create default policy** is activated.
2. Enter or confirm the storage location for the configuration package (MSI) that will be created containing the default policies.
3. Confirm with **Next**.

The policy group will be displayed in the **Policies** navigation area of the SafeGuard Policy Editor. The configuration package containing these policies will be displayed in the SafeGuard Policy Editor **Configuration Package Tool**. Deploy the configuration package to the endpoint computers when installing the encryption software. If the default configuration does not meet your needs, you may create additional policies, publish them in a configuration package and deploy them to the endpoint computers.

6.2.7 Creating a recovery key store

To cater for Challenge/Response for Sophos SafeGuard protected computers, e.g. when a user has forgotten their password, specific key recovery files are needed. On each endpoint computer such a key recovery file is generated during Sophos SafeGuard deployment.

To complete the Challenge/Response it is essential to store these files on a network share to make them available to the help desk and to provide the help desk with the necessary access rights to this share. This key recovery file is encrypted by the company certificate. It can therefore safely be saved to the network or an external medium.

1. On the **Recovery Keys** page, accept the default **Network share settings**.

This will create a network share SafeGuardRecoveryKeys\$ and a directory on the local computer where the recovery keys will be saved automatically. The share is configured to only allow new files to be written to the share location. You may change the local path if required. The network share must be located on a drive that has been formatted with NTFS. NTFS allows for setting the access permissions as required. If **Network share settings** 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.

2. On the **Recovery Keys** page, grant the help desk sufficient access rights to the recovery key share: Confirm with **Next** to accept the default permissions. Access to the recovery keys share is managed via a new Windows group called "SafeGuardRecoveryKeyAccess". By default all members of the local administrators group are added to this group.

Note: In a domain environment this will also include the domain administrators group which is a member of the local administrators group. You may display or change the group members by clicking **Permissions**.

Note:

Within SafeGuard Policy Editor it is possible to create multiple policy configuration packages, for example one package for computers within a domain environment and an additional package for standalone computers.

3. Click **Next**.

Permissions to the network share will be set. For details on the permissions, see [Setting permissions for the network share](#), page 24.

6.2.8 Setting permissions for the network share

1. In **Network Share Permissions**, do either of the following:

- Click **Add local members** to add local members with administrative rights for recovery actions.
- Click **Add global members** to add global members with administrative rights for recovery actions.

2. Click **OK**.

A group "SafeGuardRecoveryKeyAccess" will be created on the computer which contains all the members displayed in **Network Share Permissions**.

The following NTFS permissions are automatically set on the specified local directory:

- **Everyone:** Create files - The Sophos SafeGuard computer running in the context of the logged in users will be allowed to add files, but cannot browse the directory, delete or read files. **The "Create Files" permission is available in the Advanced Security Settings of a directory.**
- **SafeGuardRecoveryKeyAccess:** Modify - All users displayed in the **Permissions** dialog are allowed to read, delete and add files.
- **Administrators:** Full Control

Sophos SafeGuard also removes permission inheritance on the directory to ensure that the above permissions will not be accidentally overwritten.

The network share SafeGuardRecoveryKeys\$ will be created with this permission:

- **Everyone:** Full Control

Note: The resulting permissions are the intersection between NTFS permissions and share permissions. As the NTFS permissions are more restrictive, they will apply

If you want to set up a network share manually, we suggest that you use the same permission settings as described above. In this case, ensure to disable permission inheritance on the directory manually.

6.2.9 Completing initial configuration

1. Click **Finish** to complete the initial configuration. SafeGuard Policy Editor will launch once the configuration wizard has closed.

Initial configuration in the SafeGuard Policy Editor is completed. Two files called Networkshare.xml and ConfigurationOutput.xml will be saved to the Temp path. The file Networkshare.xml contains the configuration settings from the wizard pages. The file ConfigurationOutput.xml logs all events that occurred during processing of the configuration settings. The events are shown in the final page of the SafeGuard Policy Editor Configuration Wizard.

6.3 Configure additional instances of the SafeGuard Policy Editor

You can configure additional instances of the SafeGuard Policy Editor to provide access to the Sophos SafeGuard help desk team for carrying out recovery tasks.

1. Start the SafeGuard Policy Editor on the respective computer. 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, enable **Use an existing database**. Under **Database settings**, select the relevant Database name from the list. Click **Change** to select the SQL Server instance you want to use. A dialog is displayed where you have to configure the connection to the selected instance.
4. On the **Database Connection** dialog, under **Database Server**, select the required SQL database instance from the list. All database servers available on your computer or network will be displayed. (The list is updated every 12 minutes). Activate **Use SSL** to secure the connection to this database server with SSL. This can be useful when the machine certificates are implemented on the database server before installing Sophos SafeGuard.

5. Under **Authentication** select the type of authentication to be used to access the database:

- Activate **Use Windows NT Authentication** to use your Windows credentials.

Note: Use this type when your computer is part of a domain. However, additional configuration might be required as the user needs to be authorized to connect to the database.

- Activate **Use SQL Server Authentication** to access the database with your SQL credentials. You will be prompted to enter and confirm them. Where necessary, you may obtain this information from your SQL administrator.

Note: Use this type when your computer is not part of a domain. Ensure to activate **Use SSL** to secure the connection to and from the database server. However, SSL encryption requires a working SSL environment on the computer on which the selected SQL database resides which you have to set up in advance. For further information see: <http://www.sophos.de/support/knowledgebase/article/108339.html>.

6. Click **Check connection**. If the connection to the SQL database has been established, a corresponding success message will be displayed.

7. Confirm with **OK** twice to return to the **Database** page. Then click **Next**.

8. In the **Security Officer** page, select **Import** to import the security officer certificate associated with the selected database. Browse for the required certificate and confirm with **Open**.

Only certificates generated by the SafeGuard Policy Editor may be imported. Certificates created by a PKI (e.g. Verisign) are not allowed.

9. Enter the password for the certificate store.

10. Click **Next** and then **Finish** to complete the SafeGuard Policy Editor configuration wizard.

6.4 Setting up Sophos SafeGuard on endpoint computers

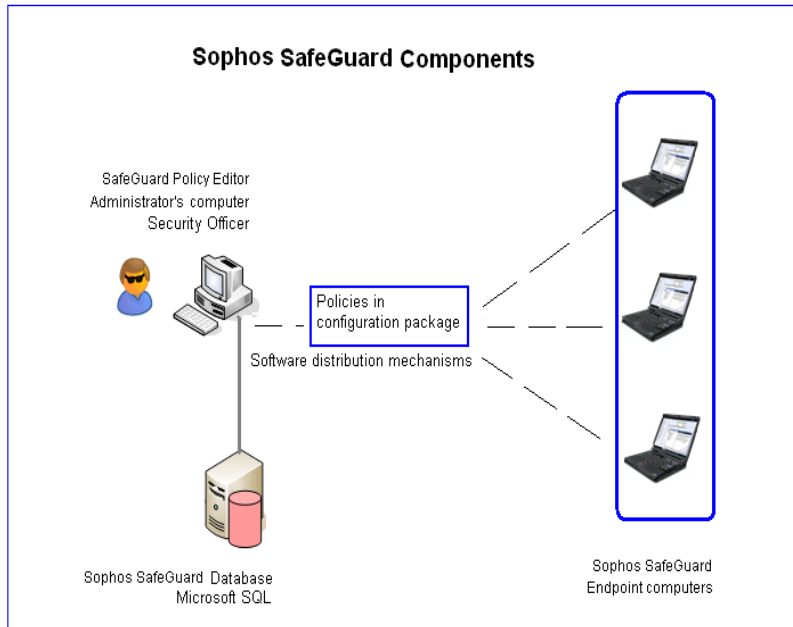
The endpoint computers can be equipped with different Sophos SafeGuard modules depending on your installation, see [Sophos SafeGuard on endpoint computers](#), page 7.

Sophos SafeGuard can be deployed in different ways to the endpoint computers:

Security officers may carry out the setup locally on the endpoints or carry out the installation and initial configuration of endpoints as part of a centralized software distribution. This ensures a standardized installation on multiple computers.

The different deployment options are also described in the following knowledgebase article: <http://www.sophos.de/support/knowledgebase/article/108426.html>

See the Startup guide (chapter *First logon after Sophos SafeGuard installation*) and 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.



6.4.1 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.

6.4.2 Setting up endpoint computers locally

If you want to carry out a trial installation on an endpoint computer, it might be useful to install Sophos SafeGuard locally first of all.

Before you install the encryption software, prepare for installation on the endpoint computer, see [Preparing for installation](#), page 14.

1. Log on to the computer as an administrator.
2. Install the preparatory installation package SGxClientPreinstall.msi that provides the endpoint computer with the necessary requirements for a successful installation of the encryption software, for example the relevant DLLs.

Note: Alternatively, you may install vcredist_x86.exe that you can download from here: <http://www.microsoft.com/downloads/details.aspx?FamilyID=766a6af7-ec73-40ff-b072-9112bab119c2> or check that MSVCR80.dll, version 8.0.50727.4053 is present in the Windows\WinSxS folder on the computer.

3. Double-click the relevant “Client” installation package (MSI) to start the encryption software installation wizard. It guides you through the necessary steps. Install either of the following:

Sophos SafeGuard Disk Encryption	Sophos SafeGuard Easy
SDEClient.msi for the 32 bit variant. SDEClient_x64.msi for the 64 bit variant.	SGNClient.msi for the 32 bit variant. SGNClient_x64.msi for the 64 bit variant. SGNClient_withoutDE.msi for SafeGuard Data Exchange only, 32 bit variant. SGNClient_withoutDE_x64.msi for SafeGuard Data Exchange only, 64 bit variant.

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 and Data Exchange.
 - Select **Typical** to install Device Protection only.
 - Select **Custom** and activate the features to your needs.

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

6. Accept the defaults on all further dialogs.

Sophos SafeGuard is installed on the endpoint computer.

7. In the SafeGuard Policy Editor, configure the encryption software to your needs:
 - Use the predefined default policies for quick and easy policy deployment created during initial configuration in the SafeGuard Policy Editor.
 - Should the default policies not cover all your specific requirements, create your own policies in the SafeGuard Policy Editor(see [Working with policies](#), page 39). For details on deploying policies on endpoint computers, see [Working with configuration packages](#), page 43.

For instance, your deployment strategy might require setting up administrative access to the computer for service staff. In this case you need to define a specific policy and create a configuration package containing these policies.
8. Install the relevant configuration package (MSI) on the computer.

Sophos SafeGuard has been set up on the endpoint computer. 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.

6.4.3 Setting up endpoint computers centrally

Setting up endpoint computer centrally ensures a standardized installation on multiple computers. Before you deploy the encryption software, prepare for installation on the endpoint computers, see [Preparing for installation](#), page 14.

1. Use your own tools to create the package to be installed on the endpoint computers. The package must include the following:
 - **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 installer that you downloaded from the Sophos website or on the product CD.

For the available packages, see [Installation](#), page 17.

- **Configuration package(s)**

Configure the encryption software to your needs:

Use the configuration package with predefined default policies created during initial configuration in the SafeGuard Policy Editor.

Should the default policies not cover all your specific requirements, create your own policies and publish them in a configuration package in the SafeGuard Policy Editor (see [Working with policies](#), page 39. For details on deploying policies on endpoint computers, see [Working with configuration packages](#), page 43.

For instance, your deployment strategy may require setting up administrative access to the computer for service staff. In this case you need to define a specific policy and deploy it to the computer within a configuration package.

- **Script with the commands for the pre-configured installation**

We recommend using the Windows Installer command-line tool msixec to create the script. For more information on msixec see see [Command for central install](#), page 31 or [http://msdn.microsoft.com/en-us/library/aa367988\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/aa367988(VS.85).aspx).

2. Create a folder Software to use as a central store for all applications.
3. Create the script: Enter the Windows Installer command msixec with the relevant parameters at the command prompt.
4. Distribute this package via company software distribution mechanisms to the endpoint computers.

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 msixec. For further information, see see [Supported Hotkeys in the Power-on Authentication](#), page 109 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>

6.4.3.1 Command for central install

When centrally installing Sophos SafeGuard on the endpoint computers, use the Windows Installer component "msiexec". "Msiexec" is already part of Windows XP, Vista and Windows 7, and it automatically carries out a pre-configured Sophos SafeGuard installation. As the source and the destination for the install can also be specified, there is the option of a standard install to multiple endpoint computers.

For more information on msiexec see: [http://msdn.microsoft.com/en-us/library/aa367988\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/aa367988(VS.85).aspx).

Command line syntax

```
msiexec /i <path+msi package name> /qn ADDLOCAL=ALL | <Features>
<parameter>
```

The command line syntax consists of:

- Windows Installer parameters, which, e.g. log warnings and error messages to a file during the install.
- Sophos SafeGuard features, which are to be installed, e.g. volume based encryption.
- Sophos SafeGuard parameters, e.g. to specify the install directory.

Command options

You can select all the available options using msiexec.exe in the prompt. The main options are described below.

Option	Description
/i	Specifies the fact that this is an installation.
/qn	Installs with no user interaction and does not display a user interface.
ADDLOCAL=	Lists the features that are to be installed. If the option is not specified, all features intended for a standard installation are installed. When listing the features under ADDLOCAL note the following:- only separate the features by a comma, not by a space. - respect upper and lower case. - If you select a feature, you also need to add all the feature parents to the command line!
ADDLOCAL=ALL	Installs all the available features
REBOOT=Force ReallySuppress	Forces or suppresses a reboot after installation. If nothing is specified, the reboot is forced after installation.
/L* <path + filename>	Logs all warnings and error messages in the specified log file. The parameter /Le <path + filename> only logs error messages

Option	Description
Installdir= <directory>	Specifies the directory in which the Sophos SafeGuard Client is to be installed. If no value is specified, the default installation directory will be <SYSTEM>:\PROGRAM FILES\SOPHOS.

6.4.3.2 Sophos SafeGuard features (ADDLOCAL)

For a central install, you must define in advance which Sophos SafeGuard features are to be installed on the endpoint computers. The features are listed after stating the option ADDLOCAL in the command.

The following tables lists the Sophos SafeGuard features that can be installed on the endpoint computers.

Features for SafeGuard Device Encryption

SGNClient.msi, SDEClient.msi or respective 64 bit variants.

Note: The features **Client** and **Authentication** must be installed by default. If you select a feature, you also need to add the feature parents to the command line!

Feature Parents	Feature
Client	Authentication The feature Authentication and its parent feature Client must be installed by default.
Client, Authentication	CredentialProvider For computers with Windows Vista you must select this feature. It enables logon via the Credential Provider.
Client, BaseEncryption	SectorBasedEncryption Installs Sophos SafeGuard volume based encryption with the following features: Any volumes, including removable media, can be encrypted with Sophos SafeGuard volume based encryption. Sophos SafeGuard Power-on Authentication (POA) Sophos SafeGuard Recovery with Challenge/Response

Feature Parents	Feature
Client	<p>SecureDataExchange</p> <p>Note: This feature is not supported with ESDP.</p> <p>SafeGuard Data Exchange with file based encryption is always installed at local level and for removable media. SafeGuard Data Exchange provides secure encryption for removable media. Data can securely and easily be shared with other users. All encryption and decryption processes run transparently and with minimal user interaction. If you have installed SafeGuard Data Exchange on your computer, SafeGuard Portable is installed as well. SafeGuard Portable enables data to be securely shared with computers that do not have SafeGuard Data Exchange installed.</p>

Features for SafeGuard Data Exchange

SGNClient_withoutDE.msi or SGNClient_withoutDE_x64.msi.

Note: These installation packages are not supported with ESDP.

Note: The features **Client** and **Authentication** must be installed by default. If you select a feature, you also need to add the feature parents to the command line!

Feature Parents	Feature
Client	<p>Authentication</p> <p>The feature Authentication and its parent feature Client must be installed by default.</p>
Client	<p>SecureDataExchange</p> <p>Note: This feature is not supported with ESDP.</p> <p>SafeGuard Data Exchange with file based encryption is always installed at local level and for removable media. SafeGuard Data Exchange provides secure encryption for removable media. Data can securely and easily be shared with other users. All encryption and decryption processes run transparently and with minimal user interaction. If you have installed SafeGuard Data Exchange on your computer, SafeGuard Portable is installed as well. SafeGuard Portable enables data to be securely shared with clients that do not have SafeGuard Data Exchange installed.</p>

Sample command for volume based encryption

The command given below takes the following effect:

- The endpoint computers are provided with the necessary requirements for successful installation of the encryption software.
- Sophos SafeGuard Power-on Authentication for authentication at Sophos SafeGuard endpoint computers is installed.
- Sophos SafeGuard volume based encryption is installed.
- A log file is created.
- The default configuration package is run.

Example:

```
msiexec /i F:\Software\SGxClientPreinstall.msi /qn /log
I:\Temp\SGxClientPreinstall.log

msiexec /i F:\Software\SGNClient.msi /qn /log I:\Temp\SGNClient.log
ADDLOCAL=Client,Authentication,BaseEncryption,SectorBasedEncryption
InstallDir=C:\Program Files\Sophos\Sophos SafeGuard

msiexec /i F:\Software\StandardConfig.msi /qn /log
I:\Temp\StandardConfig.log
```

6.4.4 FIPS-compliant installation

The FIPS certification describes security requirements for encryption modules. For example government bodies in the USA and in Canada require FIPS 140-2-certified software for particularly security-critical information.

Sophos SafeGuard uses FIPS-certified AES algorithms. By default, a new, faster implementation of the AES algorithms is installed that is not yet FIPS certified.

To use the FIPS certified variant of the AES algorithm, set the FIPS_AES property to 1 when installing the Sophos SafeGuard encryption software.

This can be done in two ways:

- Add the property to the command line script:

```
msiexec /i F:\Software\SGNClient.msi FIPS_AES=1
```
- Use a transform.

7 Installing the Sophos SafeGuard encryption software on computers with multiple operating systems

Note: This feature is not supported with ESDP (Endpoint Security and Data Protection).

The Sophos SafeGuard encryption software can be installed on a computer to protect its data even if several operating systems are installed on separate volumes of the hard disk. Sophos SafeGuard provides a so-called runtime system. Sophos SafeGuard Runtime enables the following when it is installed on volumes with an additional Windows installation:

- The Windows installation residing on these volumes may successfully be booted by a boot manager.
- Partitions on these volumes that have been encrypted by a full Sophos SafeGuard installation with the defined machine key can successfully be accessed.

7.1 Requirements and restrictions

Note the following:

- Sophos SafeGuard Runtime does not provide any Sophos SafeGuard features or functionality.
- Sophos SafeGuard Runtime only supports those operating systems that are also supported for the Sophos SafeGuard Client encryption software.
- Successful operation of USB keyboards may be restricted.
- Only boot managers that become active after Power-on Authentication are supported.
- Support for third party boot managers is not guaranteed. We recommend to use Microsoft boot managers.
- Sophos SafeGuard Runtime cannot be updated to a full Sophos SafeGuard installation.
- The Runtime installation package must be installed before the full version of the Sophos SafeGuard Client installation package is installed.
- Only volumes encrypted with the defined machine key in Sophos SafeGuard may be accessed.

7.2 Preparations

To set up Sophos SafeGuard Runtime, carry out the following preparations in the order mentioned:

1. Ensure that those volumes on which Sophos SafeGuard Runtime is to run are visible at the time of installation and may be addressed by their Windows name (e.g. C:).
2. Decide on which volume(s) of the hard disk Sophos SafeGuard Runtime is to be installed. In terms of Sophos SafeGuard, these volumes are defined as "secondary" Windows installations. There can be several secondary Windows installations. Use the following package: SGNClientRuntime.msi (or respective 64 bit variant when the computer's operating system is Windows 7 64 bit or Windows Vista 64 bit).
3. Decide on which volume of the hard disk the full version of the Sophos SafeGuard Client is to be installed. In terms of Sophos SafeGuard, this volume is defined as the "primary" Windows installation. There can only be one primary Windows installation. Use the following package: SGNClient.msi (or respective 64 bit variant when the computer's operating system is Windows 7 64 bit or Windows Vista 64 bit).

7.3 Setting up Sophos SafeGuard Runtime

Do the following:

1. Select the required secondary volume(s) of the hard disk, you want to install Sophos SafeGuard Runtime on.
2. Boot the secondary Windows installation on the selected volume.
3. Install the Client Runtime package on the selected volume.
4. Confirm the defaults in the next dialog of the installer. No special feature selection is necessary.
5. Select an installation folder for the runtime installation.
6. Confirm to finish the runtime installation.
7. Select the primary volume of the hard disk, you want to install Sophos SafeGuard Client on.
8. Boot the primary Windows installation on the selected volume.
9. Start the preparatory installation package SGxClientPreinstall.msi to provide endpoint computers with the necessary requirements for successful installation of the encryption software, for example the relevant DLLs.

10. Install the respective Sophos SafeGuard Client installation package on the selected volume.
11. Create the configuration package and deploy it on the endpoint computer.
12. Encrypt both volumes with the defined machine key.

7.4 Booting from a secondary volume via a boot manager

Do the following:

1. Start the computer.
2. Log on at the Power-on Authentication with your credentials.
3. Start the boot manager and select the required secondary volume as boot volume.
4. Reboot the computer from this volume.

Each volume encrypted with the defined machine key can be accessed.

8 Logon to the SafeGuard Policy Editor

To log on to the SafeGuard Policy Editor do the following:

1. Start the SafeGuard Policy Editor. A logon dialog is displayed.
2. Enter the security officer password specified during initial configuration, and confirm with **OK**.

The SafeGuard Policy Editor is opened.

9 Working with policies

The following sections explain the administrative tasks concerning policies, for example creating, grouping and backing up policies.

A set of recommended default policies is already created during initial configuration via the SafeGuard Policy Editor, see [Carry out initial configuration in the SafeGuard Policy Editor Configuration Wizard](#), page 19. For a detailed description of the default policy, see [Default Policies](#), page 61.

Furthermore, for a description of all policy settings available with Sophos SafeGuard, see [Policy Settings](#), page 68.

9.1 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.)

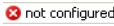
For each target, a separate policy has to be created. Later on you can combine the individual policies in a policy group named *Encryption*, for example.

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.






9.2 Editing policy settings

When selecting a policy in the navigation window, you can edit the policy settings in the action area.

	<p>A red icon in front of a „not configured“ setting indicates that for this policy setting a value has to be defined. To be able to save the policy, you first have to select a setting other than „not configured“.</p>
---	---

9.2.1 Setting policy settings to default values

In the toolbar the following icons are available for setting policy settings:

	<p>Displays default values for not configured policy settings.</p>
	<p>Sets marked policy setting to “not configured”.</p>
	<p>Sets all policy settings in an area to “not configured”.</p>
	<p>Sets the default value for the marked policy</p>
	<p>Sets all policy settings in an area to the default value.</p>

9.2.2 Differentiating between machine- and user-specific policies

<p>Policy color blue</p>	<p>Policy is applied to machines only, not users.</p>
<p>Policy color black</p>	<p>Policy is applied to machines and users</p>

9.3 Policy groups

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

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 point at different targets, the settings will be added.

9.3.1 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.

9.3.2 Policy grouping results

The result of policy grouping is displayed separately.

To display the result, click tab **Resulting**.

- For each policy type a separate tab is shown.

The settings resulting from combining the individual policies into a group are displayed.

- For policies for device protection, a tab for each policy target (e.g. boot volumes, drive X etc.) is shown.

9.4 Backing up policies and policy groups

You can create backups of policies and policy groups as XML files. If necessary, the relevant policies/policy groups can then be restored from these XML files.

To create a backup of a policy/policy group:

1. Select the policy/policy group in the navigation window under **Policy Items** or **Policy Groups**.
2. Right-click to display the context menu and select **Backup Policy**.
The **Backup Policy** command is also available in the **Actions** menu.
3. In the **Save As** dialog enter a file name for the XML file and select a storage location for the file. Click **Save**.

The backup of the policy/policy group is stored as an XML file in the specified directory.

9.5 Restoring policies and policy groups

To restore a policy/policy group from an XML file, do the following:

1. Select **Policy Items/Policy Groups** in the navigation window.
2. Right-click to display the context menu and select **Restore Policy**.
The **Restore Policy** command is also available in the **Actions** menu.
3. Select the XML file from which the policy/policy group is to be restored and click **Open**.

The policy/policy group is restored.

10 Working with configuration packages

Sophos SafeGuard protected computers receive their encryption policies via configuration packages created in the SafeGuard Policy Editor. For successful operation of Sophos SafeGuard on the endpoint computers, you need to create a configuration package containing the relevant policy groups and distribute it to the endpoint computers.

During initial configuration in the SafeGuard Policy Editor configuration wizard a default configuration package with default policies can already be created.

Whenever you change any policy settings, you have to create new configuration packages and distribute them to the endpoint computers.

The following sections explain how to create configuration packages and distribute them to the endpoint computers.

Note: Check your network and computers in regular intervals for outdated or unused configuration packages and, for security reasons, make sure to delete them.

10.1 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.

10.2 Distributing configuration packages

Configuration packages have to be installed on the endpoint computers after installation of the Sophos SafeGuard encryption software or after any change in the configuration settings.

Distribute the configuration package via your company software distribution mechanisms or install it manually on the endpoint computers.

Note: To change the policy settings for a Sophos SafeGuard protected computer create a new configuration package including the changed policies and distribute it to the computer.

Note: If you try to install an older configuration package over a newer one, the installation is aborted and an error message is displayed.

11 Exporting company and Master Security Officer certificate

In a Sophos SafeGuard installation, the following two items are critical and require thorough backup in a safe location:

- the company certificate stored in the SafeGuard Database.
- the Master Security Officer (MSO) certificate residing in the certificate store of the computer on which the SafeGuard Policy Editor is installed.

Note: In the SafeGuard Policy Editor the MSO is the officer defined during initial configuration. With ESDP this officer is always called “Administrator”.

Both certificates can be exported in form of .p12 files for backup purposes. Corrupted installations of the SafeGuard Policy Editor or a corrupted database can then be restored by importing the relevant certificate (.p12 file).

Note: We advise carrying out this task right after initial configuration in the SafeGuard Policy Editor.

11.1 Exporting the company certificates

1. In the SafeGuard Policy Editor menu bar, select **Tools > Options**.
2. Select the **Certificates** tab and click the **Export** button in the **Company Certificate** section.
3. You are prompted to enter a password for securing the exported file. Enter a password, confirm it and click **OK**.
4. Enter a file name and storage location for the file and click **OK**.

The company certificate is exported as a .p12 file to the defined location and can be used for recovery purposes.

11.2 Exporting the Master Security Officer certificate

To back up the Master Security Officer (MSO) certificate of the MSO logged on to the SafeGuard Policy Editor, do the following:

1. In the SafeGuard Policy Editor menu bar, select **Tools > Options**.
2. Select the **Certificates** tab and click the **Export** button in the **<Administrator> Certificate** section.
3. You are prompted to enter a password for securing the exported file. Enter a password, confirm it and click **OK**.
4. Enter a file name and storage location for the file to be exported and confirm with **OK**.

The Master Security Officer certificate of the currently logged on MSO is exported as a .p12 file to the defined location and can be used for recovery purposes.

12 Restoring a corrupt SafeGuard Policy Editor installation

If the installation of the SafeGuard Policy Editor is corrupted, but the database is still intact, the installation can be easily restored by installing the SafeGuard Policy Editor afresh and using the existing database as well as the backed up Security Officer certificate.

Do the following:

1. Install the Policy Editor installation package afresh. Open the SafeGuard Policy Editor. The Configuration Wizard is started automatically.
2. In **Database**, activate **Use an existing database**. Under **Database name**, select the name of the database from the list. Under **Database settings**, configure the connection to the database if required. Click **Next**.
3. In **Security Officer**, do either of the following:
 - If the backed up certificate file can be found on the computer, it will be displayed. Enter the password you use for authenticating at the SafeGuard Policy Editor.
 - If the backed up certificate file cannot be found on the computer, click **Import**. Browse for the backed up certificate file and confirm with **Open**. Enter the password for the selected certificate file. Confirm with **Yes**. Enter and confirm a password for authenticating at the SafeGuard Policy Editor.
4. Click **Next** and then **Finish** to complete the SafeGuard Policy Editor configuration.

The corrupt SafeGuard Policy Editor installation is restored.

13 Restoring a corrupt database configuration

A corrupt database configuration can be restored by installing the SafeGuard Policy Editor afresh to create a new instance of the database based upon the backed up certificate files. This will ensure that all existing Sophos SafeGuard endpoint computers still accept policies from the new installation and avoids having to set up and restore the whole database afresh.

- The company and Master Security Officer certificates of the relevant database configuration must have been exported to .p12 files and must be available and valid.
- The passwords for the two .p12 files as well as for the certificate store must be known to you.

Do the following:

1. Install the Policy Editor installation package afresh. Open the SafeGuard Policy Editor. The Configuration Wizard is started automatically.
2. In **Database**, select **Create a new database**. Under **Database settings**, configure the connection to the database. Click **Next**.
3. In **Security Officer**, select the relevant security officer. Uncheck **Automatically create certificate**. Click **Import** to browse for the backed up certificate file. Enter and confirm the respective security officer password for the certificate store. The certificate is imported. Click **Next**.
4. In **Company Information**, uncheck **Automatically create certificate**. Click **Import** to browse for the backed up certificate file that contains the valid company certificate. You are prompted to enter the password specified for the certificate store. Enter the password and confirm with **OK**. Confirm the message with **Yes**. The company certificate is imported.
5. In **Certificate Backup**, specify a storage location for the certificate backups. Confirm the storage location with **Next**.
6. In **Default Policy**, uncheck **Create default policy** and confirm with **Next**.
7. In **Recovery Keys**, uncheck **Network share** settings and click **Next**, then **Finish**.

The database configuration is restored.

14 Administrative access to endpoint computers

To cater for access requirements for administrative tasks after the installation of Sophos SafeGuard on endpoint computers, Sophos SafeGuard offers 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. Service account lists are defined in the **Policies** area of the SafeGuard Policy Editor and assigned via policies included in Sophos SafeGuard configuration packages to the endpoint computers. Users included on a service account list are treated as guest users when logging on at the endpoint computer.

Note: Service account lists are assigned to endpoint computers via policies. They should be assigned in the first Sophos SafeGuard configuration package you create for the configuration of the endpoint computers. Service Account lists can be updated by creating a new configuration package and deploying it to the endpoint computers.

■ POA access accounts for POA logon

POA access accounts are predefined local accounts that enable users (for example members, of the IT team) to log on to endpoint computers to perform administrative tasks after the POA has been activated. POA access accounts enable POA logon, there is no automatic logon to Windows. These access accounts are defined in the **Users** area of the SafeGuard Policy Editor (user ID and password) and assigned to the endpoint computers via POA access groups included in Sophos SafeGuard configuration packages.

14.1 Service account lists for Windows logon

A typical scenario for most implementations is that a rollout team installs new computers in an environment including the installation of Sophos SafeGuard. For installation or verification reasons, rollout operators may log on to the respective computer before the end user receives the new machine and is able to activate the Power-on Authentication.

Thus, the scenario may be as follows:

1. Sophos SafeGuard is installed on an endpoint computer.
2. After rebooting the computer, the rollout operator logs on.
3. The rollout operator is added to the POA and the POA becomes active.

Upon receiving the computer the end user will not be able to log on to the POA and needs to perform a Challenge/Response procedure.

To ensure that administrative operations on a Sophos SafeGuard protected computer do not lead to an activation of the Power-on Authentication and the addition of rollout operators as users to the computer, Sophos SafeGuard offers the possibility of creating service account lists for endpoint computers. The users included in these lists are thereby treated as Sophos SafeGuard guest users.

With service accounts the scenario is as follows:

1. Sophos SafeGuard is installed on an endpoint computer.
2. After rebooting the computer, a rollout operator included on a service account list logs on (Windows logon).
3. According to the service account list applied to the computer the user is identified as a service account and will be treated as a guest user.

The rollout operator will not be added to the POA and the POA will not become active. The end user can log on and activate the POA.

Note: Service Account Lists should be assigned in the first Sophos SafeGuard configuration package you create for the configuration of the endpoint computers. Service account lists can be updated by creating a new configuration package with changed settings and deploy them to the endpoint computers.

14.1.1 Creating service account lists and adding users

To create service account lists and add users, do as follows:

1. Click **Policies** in the navigation area.
2. Select **Service account lists** in the policy navigation window.
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 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 and can be selected for assignment when creating a policy.

14.1.1.1 Additional information for entering user and domain names

There are different methods for specifying users in service account lists using the two fields **User Name** and **Domain Name** (see [Covering different combinations for logging on](#), page 51). Furthermore, certain restrictions apply for valid input in these fields (see [Restrictions](#), page 52).

Covering different combinations for logging on

The two separate fields **User Name** and **Domain Name** per list entry offer the flexibility to cover all available combinations for logging on, for example "user@domain" or "domain\user".

To handle several user name/domain name combinations, you can use asterisks (*) as wild cards. An asterisk is allowed as the first sign, the last sign and the only sign.

For example:

- **User Name:** Administrator
- **Domain Name:** *

This combination specifies all users with the user name "Administrator" who log on to any network or local machine.

The predefined domain name [LOCALHOST] available in the drop-down list of the **Domain Name** field stands for the logon on any local workstation.

For example:

- **User Name:** "*admin"
- **Domain Name:** [LOCALHOST]

This combination specifies all users whose user names end on "admin" and who log on to any local machine.

Furthermore, users may log on in different ways, e.g.:

- user: test, domain: mycompany or
- user: test, domain: mycompany.com.

As domain specifications in the service account lists are not automatically resolved, there are three possible methods for specifying the domain correctly:

- You know exactly how the user is going to log on and enter the domain accordingly.
- You create several service account list entries.
- You use wild cards to cover all different cases (user: test, domain: mycompany*).

Note: To avoid any problems caused by the fact that Windows may not use the same character sequence, but truncate names, it is recommended to enter the FullQualifiedName and the NetBIOS name or use wildcards.

Restrictions

Asterisks are only allowed as the first sign, the last sign and the only sign. Following are examples for valid and invalid strings using asterisks:

- Valid strings are for example admin*, *, *strator, *minis*.
- Invalid strings are for example **, Admin*trator, Ad*minst*.

Furthermore the following restrictions apply:

- The character ? is not allowed in user logon names.
- The characters / \ [] : ; | = , + * ? < > " are not allowed in domain names.

14.1.2 Editing and deleting service account lists

As a security officer with the right **Modify service account lists** you can edit or delete service account lists at any time:

- To edit a service account list, double-click it in the policy navigation window. The service account list is opened and you can add, delete or modify user names on the list.
- To delete a service account list, select it in the policy navigation window, open the context menu and select **Delete**.

14.1.3 Assigning a service account list via policy

To select and assign a service account list, do as follows:

1. Create a new policy of the type **Authentication** or select an existing one.
2. Under **Logon Options**, select the required service account list from the drop-down list of the **Service Account List** field.

Note: The default setting of this field is [**No list**], i.e. no service account list applies. Rollout operators logging on to the computer after installation of Sophos SafeGuard will therefore not be treated as guest users and may activate Power-on Authentication and be added to the computer. To undo the assignment of a service account list, select the [**No list**] option.

3. Save your changes by clicking the **Save** icon in the toolbar.

You can now transfer the policy to the respective computers to make the service accounts available on the computer.

Note: If you select different service account lists in different policies which are all relevant according to the RSOP (Resulting Set of Policies, the settings valid for a specific computer/group), the service account list assigned in the last policy applied will overrule all previously assigned service account lists. Service account lists will not be merged.

14.1.4 Transferring the policy to the endpoint computer

Sophos SafeGuard protected computers receive policies via configuration packages created via **Tools > Configuration Package Tool** in the SafeGuard Policy Editor.

The configuration file may be distributed via company software distribution mechanisms or the configuration package is installed manually on the endpoint computers.

Note: As the service account list functionality is especially helpful and important during initial installation in the rollout phase of an implementation, it is recommended to include an **Authentication** policy with the required service account list settings in the policy group transferred with the initial Sophos SafeGuard configuration package created in the SafeGuard Policy Editor for configuring the endpoint computer after installation.

Note: To change the policy settings for a Sophos SafeGuard protected computer, create a new configuration package including the changed policies and distribute it to the computer.

14.1.5 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.

14.1.5.1 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).

14.1.6 Log events

Actions performed regarding service account lists are reported by the following log events:

SafeGuard Policy Editor

- Service account list <name> created
- Service account list <name> modified
- Service account list <name> deleted

Sophos SafeGuard endpoint computer

- Windows user <domain/user name> logged on at <timestamp> to machine <domain/workstation name> as SGN service account.
- New service account list <name> imported.
- Service account list <name> deleted.

14.2 POA access accounts for POA logon

After Sophos SafeGuard has been installed and the Power-on Authentication (POA) has been activated, access to endpoint computers to perform administrative tasks may be required. With POA access accounts, users (for example members of the IT team) can log on at the Power-on Authentication on endpoint computers for administrative tasks without having to initiate a Challenge/Response procedure. There is no automatic logon to Windows; users have to log on to Windows with their existing Windows accounts.

You can create POA access accounts in the SafeGuard Policy Editor, group them into POA access account groups, and assign groups to endpoint computers via Sophos SafeGuard configuration packages. The users, i.e. POA access accounts, included in the POA access accounts group assigned, will be added to the POA and can log on using their predefined user name and password.

14.2.1 Creating POA access accounts

To create POA access accounts, do as follows:

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.
5. Optionally, enter a description for the new POA user.
6. Enter a password for the new POA access account and confirm it.

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.

7. 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.

14.2.2 Changing the password for a POA access account

To change the password for a POA access account, do as follows:

1. Click **Users** in the navigation area of the SafeGuard Policy Editor.
2. In the **Users** navigation window under **POA**, **POA Users**, select the relevant POA user.
3. In the context menu of the POA user, select **Properties**.

The properties dialog for the POA user is displayed.

4. In tab **General** under **User Password**, enter the new password and confirm it.
5. Click **OK**.

The new password applies for the relevant POA access account.

14.2.3 Deleting POA access accounts

To delete POA access accounts, do as follows:

1. Click **Users** in the navigation area of the SafeGuard Policy Editor.
2. In the **Users** navigation window under **POA, POA Users**, select the relevant POA access account.
3. Right-click on the POA access account and select **Delete** from the context menu.

The POA access account, i.e. the POA user, is deleted and is no longer displayed in the **Users** navigation window.

Note: If the user is part of one or several POA groups, the POA access account will also be removed from all groups. However, the POA access account will still be available on the endpoint computer until a new configuration package has been created and assigned. For further details on POA groups, see [Creating POA access account groups](#), page 56. For further details on changing the POA access account assignment, see [Changing POA access accounts assignments on endpoint computers](#), page 59

14.2.4 Creating POA access account groups

To be able to assign POA access accounts to endpoint computers via configuration packages, the accounts must be arranged in groups. When creating configuration packages, you can select a POA access account group for assignment.

To create POA access account groups, do as follows:

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

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

4. In the **Full name** field, enter a name for the new POA group.

5. Optionally, enter a description for the new POA group.
6. Click **OK**.

The new POA access account group is created and is displayed under **POA Groups** in the **Users** navigation area. You can now add users, i.e. POA access accounts, to the POA access account group.

14.2.5 Adding accounts to POA access account groups

To add users, i.e. POA access accounts, to POA access account groups, do as follows:

1. Click **Users** in the navigation area of the SafeGuard Policy Editor.
2. In the **Users** navigation window under **POA, POA Group**, select the relevant POA group.

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

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

The **Select member object** dialog is displayed.

4. Select the user, i.e. POA access account, you want to add to the group.
5. Click **OK**.

The POA access account is added to the group and displayed in the **Members** tab.

Note: You can also add accounts to groups by selecting the POA user, i.e. POA access account, in the navigation window and following the steps described above. The only difference in this approach is that the action area displays the **Member of** tab after selecting the user. This tab shows the groups the user has been assigned to. The basic workflow is identical.

14.2.5.1 Removing members from POA access account groups

To remove members, i.e. POA access accounts, from POA access account groups, do as follows:

1. Click **Users** in the navigation area of the SafeGuard Policy Editor.
2. In the **Users** navigation window under **POA, POA Group**, select the relevant POA group.

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

3. Select the user you want to delete from the group.
4. In the SafeGuard Policy Editor toolbar, click the **Remove (Delete)** icon (red cross sign).

The user is removed from the group.

Note: You can also remove members from groups by selecting the POA user, i.e. POA access account, in the navigation window and following the steps described above. The only difference in this approach is that the action area displays the **Member of** tab after selecting the user. This tab shows the groups the user has been assigned to. The basic workflow is identical

14.2.6 Assigning POA access accounts to endpoint computers

To assign POA access groups to endpoint computers via configuration packages, do as follows:

1. In the SafeGuard Policy Editor, select **Configuration Package Tool** from the **Tools** menu.
2. Select an existing configuration package or create a new one.
For details on creating a new configuration package, see [Creating a Sophos SafeGuard configuration package](#), page 43.
3. Specify a **POA Group** created beforehand in the **Users** area of the SafeGuard Policy Editor, to be applied to the computers.
The default setting for the POA group is **No Group**.
Furthermore, an empty group is available for selection by default. This group can be used to delete a POA access account group assignment on endpoint computers. For further details see [Deleting POA access accounts from endpoint computers](#), page 59.
4. Specify an output path for the configuration package (MSI).
5. Click **Create Configuration Package**.
6. Deploy the configuration package (MSI) to the endpoint computers.

By installing the configuration package, the users, i.e. POA access accounts, included in the group are added to the POA on the endpoint computers. The POA access accounts are available for POA logon.

14.2.7 Changing POA access accounts assignments on endpoint computers

To change the POA access accounts assignment for endpoint computers, do as follows:

1. Create a new POA access account group or modify an existing one.
2. Create a new configuration package and select the new or modified POA access account group.

The new POA access account group is available on the endpoint computer, all users included are added to the POA. The new group overwrites the old one. POA access account groups are not merged.

14.2.8 Deleting POA access accounts from endpoint computers

POA access accounts can be deleted from endpoint computers by assigning an empty POA access account group. Do as follows:

1. In the SafeGuard Policy Editor, select the **Configuration Package Tool** from the **Tools** menu.
2. Select an existing configuration package or create a new one.
For details on creating a new configuration package, see [Creating a Sophos SafeGuard configuration package](#), page 43.
3. Specify an empty **POA Group** created beforehand in the **Users** area of the SafeGuard Policy Editor, or select the empty POA group that is available by default in the **Configuration Package Tool**.
4. Specify an output path for the configuration package (MSI).
5. Click **Create Configuration Package**.
6. Deploy the configuration package to the endpoint computers.

By installing the configuration package, all POA access accounts are removed from the endpoint computers, i.e. all relevant users are removed from the POA.

14.2.9 Logging on to an endpoint computer using a POA access account

To log on using a POA access account, do as follows:

1. Switch on the computer.

The Power-on Authentication logon dialog is displayed.

2. Enter the **User name** and the **Password** of the predefined POA access account.

You are not automatically logged on to Windows. Therefore, the Windows logon dialog is displayed.

3. In the **Domain field**, select the domain <POA>.
4. Log on to Windows using your existing Windows user account.

15 Default Policies

During initial configuration via the SafeGuard Policy Editor a policy group with pre-defined encryption and authentication settings is created by default. A configuration package (MSI) containing these default policies is automatically created.

After installation, the policy items and the group will be displayed in the **Policies** navigation area of the SafeGuard Policy Editor. The automatically created default configuration package will be shown for selection in the **Configuration Package Tool** of the SafeGuard Policy Editor.

Note: The default policies can only be created during the initial configuration in the SafeGuard Policy Editor Configuration Wizard.

The following two sections list the default policies available with SGE (SafeGuard Easy) and ESDP (Endpoint Security and Data Protection).

For a detailed description of the policy settings, see [Policy Settings](#), page 68.

15.1 Default Policies available with SGE

For options listed in the following table with the setting not configured, default values automatically apply. The relevant default values are indicated in brackets.

Note: For a detailed description of the policy settings, see [Policy Settings](#), page 68.

Policy	Settings
<p>Default General Settings Policy Policy type: General Settings</p>	<p>Customization:</p> <ul style="list-style-type: none"> ■ Language used on client: Use OS language settings <p>Logon Recovery:</p> <ul style="list-style-type: none"> ■ Activate Logon recovery after Windows Local Cache corruption: No <p>Local Self Help:</p> <ul style="list-style-type: none"> ■ Enable Local Self Help: Yes ■ Minimal length of answers: 3 ■ Users can define their own questions: Yes <p>Challenge/Response (C/R):</p> <ul style="list-style-type: none"> ■ Enable logon recovery via C/R: Yes ■ Allow automatic logon to Windows: Yes

Policy	Settings
<p>Default Authentication Policy Policy type: Authentication</p>	<p>Access:</p> <ul style="list-style-type: none"> ■ User may only boot from hard disk: Yes <p>Logon Options:</p> <ul style="list-style-type: none"> ■ Logon Mode: User ID/Password ■ Display unsuccessful logons for this user: No ■ Display last user logon: No ■ Disable 'forced logoff' in workstation lock: No ■ Active user/domain preselection: Yes ■ Pass through to Windows: Let user choose freely <p>Failed Logons:</p> <ul style="list-style-type: none"> ■ Maximum no. of failed logons: 16 ■ Logon failed messages in POA: Standard <p>Reaction to failed logons:</p> <ul style="list-style-type: none"> ■ Lock machine: Yes
<p>Default Password Policy Policy type: Password</p>	<p>Password:</p> <ul style="list-style-type: none"> ■ Min. password length: 4 ■ Max. password length: 128 ■ Min. number of letters: 0 ■ Min. number of digits: 0 ■ Min. number of special characters: 0 ■ Case sensitive: No ■ Keyboard row forbidden: No ■ Keyboard column forbidden: No ■ 3 or more consecutive characters forbidden: No ■ User name as password forbidden: No ■ Use forbidden password list: No <p>Changes:</p> <ul style="list-style-type: none"> ■ Password change allowed after min. (days): not configured (default value 0 applies) ■ Password expires after (days): not configured (default value 999 applies) ■ Notify of forced change before (days): not configured (default value 10 applies) <p>General:</p> <ul style="list-style-type: none"> ■ Password history length: 0

Policy	Settings
<p>Default Device Encryption Policy Policy type: Device Protection</p>	<p>Encrypt all internal disks.</p> <ul style="list-style-type: none"> ■ Media encryption mode: Volume based <p>General Settings:</p> <ul style="list-style-type: none"> ■ Algorithm to be used for encryption: AES256 ■ Key to be used for encryption: Defined machine key ■ User is allowed to create local key: not configured (default value Yes applies) <p>Volume Based Settings:</p> <ul style="list-style-type: none"> ■ User may add or remove keys to or from encryption: not configured (default value No applies) ■ Reaction to unencrypted volumes: Accept all media and encrypt ■ User may decrypt volume: No ■ Proceed on bad sectors: Yes
<p>Default Data Exchange Policy Policy type: Device Protection</p>	<p>Encrypt removable media</p> <ul style="list-style-type: none"> ■ Media encryption mode: File based <p>General Settings:</p> <ul style="list-style-type: none"> ■ Algorithm to be used for encryption: AES256 ■ Key to be used for encryption: Any key in user key ring <p>File Based Settings:</p> <ul style="list-style-type: none"> ■ Copy SG Portable to Removable Media: Yes ■ User may define a Media Passphrase for devices: Yes

Policy	Settings
<p>Default Machine Settings Policy Policy type: Specific Machine Settings</p>	<p>Power-on Authentication (POA):</p> <ul style="list-style-type: none"> ■ Enable Power-on Authentication: Yes <p>Secure Wake on LAN (WOL):</p> <ul style="list-style-type: none"> ■ Number of autologons: 0 ■ Windows logon allowed during WOL: No <p>Display Options:</p> <ul style="list-style-type: none"> ■ Display machine identification: Workstation name ■ Display legal notice: No ■ Display additional information: Never ■ Enable and show system tray icon: Yes ■ Show overlay icons in Explorer: Yes ■ Virtual Keyboard in POA: Yes <p>Installation Options:</p> <ul style="list-style-type: none"> ■ Uninstallation allowed: Yes ■ Enable Sophos tamper protection: Yes <p>Note: This setting only applies to endpoint computers where Sophos Endpoint Security and Control version 9.5 or higher is installed.</p>
<p>Default Logging Policy Policy type: Logging</p>	<p>Only log errors in the event log, discard others.</p>

15.2 Default Policies available with ESDP

For options listed in the following table with the setting not configured, default values automatically apply. The relevant default values are indicated in brackets.

Note: For a detailed description of the policy settings, see [Policy Settings](#), page 68.

Policy	Settings
<p>Default General Settings Policy Policy type: General Settings</p>	<p>Customization:</p> <ul style="list-style-type: none"> ■ Language used on client: Use OS language settings <p>Logon Recovery:</p> <ul style="list-style-type: none"> ■ Activate Logon recovery after Windows Local Cache corruption: No <p>Local Self Help:</p> <ul style="list-style-type: none"> ■ Enable Local Self Help: Yes ■ Minimal length of answers: 3 ■ Users can define their own questions: Yes <p>Challenge/Response (C/R):</p> <ul style="list-style-type: none"> ■ Enable logon recovery via C/R: Yes ■ Allow automatic logon to Windows: Yes
<p>Default Authentication Policy Policy type: Authentication</p>	<p>Access:</p> <ul style="list-style-type: none"> ■ User may only boot from hard disk: Yes <p>Logon Options:</p> <ul style="list-style-type: none"> ■ Logon Mode: User ID/Password ■ Display unsuccessful logons for this user: No ■ Display last user logon: No ■ Disable 'forced logoff' in workstation lock: No ■ Active user/domain preselection: Yes ■ Pass through to Windows: Let user choose freely <p>Failed Logons:</p> <ul style="list-style-type: none"> ■ Maximum no. of failed logons: 16 ■ Logon failed messages in POA: Standard <p>Reaction to failed logons:</p> <ul style="list-style-type: none"> ■ Lock machine: Yes

Policy	Settings
<p>Default Password Policy Policy type: Password</p>	<p>Password:</p> <ul style="list-style-type: none"> ■ Min. password length: 4 ■ Max. password length: 128 ■ Min. number of letters: 0 ■ Min. number of digits: 0 ■ Min. number of special characters: 0 ■ Case sensitive: No ■ Keyboard row forbidden: No ■ Keyboard column forbidden: No ■ 3 or more consecutive characters forbidden: No ■ User name as password forbidden: No ■ Use forbidden password list: No <p>Changes:</p> <ul style="list-style-type: none"> ■ Password change allowed after min. (days): not configured (default value 0 applies) ■ Password expires after (days): not configured (default value 999 applies) ■ Notify of forced change before (days): not configured (default value 10 applies) <p>General:</p> <ul style="list-style-type: none"> ■ Password history length: 0
<p>Default Device Encryption Policy Policy type: Device Protection</p>	<p>Encrypt all internal disks.</p> <ul style="list-style-type: none"> ■ Media encryption mode: Volume based <p>General Settings:</p> <ul style="list-style-type: none"> ■ Algorithm to be used for encryption: AES256 ■ Key to be used for encryption: Defined machine key <p>Volume Based Settings:</p> <ul style="list-style-type: none"> ■ Reaction to unencrypted volumes: Accept all media and encrypt ■ User may decrypt volume: No ■ Proceed on bad sectors: Yes

Policy	Settings
<p>Default Machine Settings Policy Policy type: Specific Machine Settings</p>	<p>Power-on Authentication (POA):</p> <ul style="list-style-type: none"> ■ Enable Power-on Authentication: Yes <p>Secure Wake on LAN (WOL):</p> <ul style="list-style-type: none"> ■ Number of autologons: 0 ■ Windows logon allowed during WOL: No <p>Display Options:</p> <ul style="list-style-type: none"> ■ Display machine identification: Workstation name ■ Display legal notice: No ■ Display additional information: Never ■ Enable and show system tray icon: Yes ■ Show overlay icons in Explorer: Yes ■ Virtual Keyboard in POA: Yes <p>Installation Options:</p> <ul style="list-style-type: none"> ■ Uninstallation allowed: Yes ■ Enable Sophos tamper protection: Yes <p>Note: This setting only applies to endpoint computers where Sophos Endpoint Security and Control version 9.5 or higher is installed.</p>
<p>Default Logging Policy Policy type: Logging</p>	<p>Only log errors in the event log, discard others.</p>

16 Policy Settings

The Sophos SafeGuard policies include all settings which need to be active to implement a companywide security policy on the endpoint computers.

The Sophos SafeGuard policies can incorporate settings for the following areas (policy types):

- **General Settings**

Contains for example settings for transfer rate, background images, etc.

- **Authentication**

Contains settings for logon mode, device lock, etc.

- **Passwords**

Defines the requirements for user passwords.

- **Passphrases for SafeGuard Data Exchange**

Note: These settings are not supported with ESDP (Endpoint Security and Data Protection).

Defines the requirements for passphrases. Passphrases are used for secure data exchange with SafeGuard Data Exchange during key generation.

- **Device protection**

Contains the settings for volume- or file based encryption (including settings for SafeGuard Data Exchange and SafeGuard Portable): algorithms, keys, the drives on which data is to be encrypted, etc.

- **Specific machine settings**

Contains settings for the Power-on Authentication (activate/deactivate), for secure Wake On LAN, display options, etc.

- **Logging**

Defines the events to be logged.

The following sections provide a detailed description of all policy settings available in SafeGuard Policy Editor.





Different settings are available with SGE (SafeGuard Easy) and ESDP (Endpoint Security and Data Protection). For ESDP, file based policy settings and settings relating to SafeGuard Data Exchange are not available. In the following sections the settings available for SGE and ESDP are marked by a tick in the relevant columns.



16.1 General settings

Policy setting	SGE	ESDP	Explanation
CUSTOMIZATION			
Language used on client	✔	✔	Determines the language in which settings for Sophos SafeGuard are displayed on the endpoint computer. Besides the supported languages, users may select the endpoint computer's operating system language setting.
LOGON RECOVERY			
Activate logon recovery after Windows Local Cache corruption	✔	✔	The Windows Local Cache stores all keys, policies, user certificates and audit files. All data stored in the local cache are signed and cannot be changed manually. By default, logon recovery is deactivated when the Windows Local Cache is corrupted, i.e. it will be restored automatically from its backup. In this case, no Challenge/Response procedure is required for repairing the Windows Local Cache. If the Windows Local Cache is to be repaired explicitly via a Challenge/Response procedure, set this field to "YES".
Enable Local Self Help			
Enable Local Self Help	✔	✔	Determines whether a Sophos SafeGuard user is permitted to log on to their computer via Local Self Help if they have forgotten their password. Using Local Self Help they can log on by answering a specified number of previously defined questions in the Power-on Authentication.

Policy setting	SGE	ESDP	Explanation
			Thus, the user can regain access to their computer even if neither telephone nor internet connection are available. A Challenge/Response procedure is not necessary in this case. Local Self Help helps reducing help desk efforts and cost. For the user to be able to use Local Self Help, automatic logon to Windows has to be enabled. Otherwise, Local Self Help will not work.
Minimal length of answers	✔	✔	In this field, define the minimum length (in characters) for the answers to be saved for Local Self Help on the endpoint computer.
Welcome text under Windows	✔	✔	In this field you can specify the individual information text to be displayed in the first dialog when launching the Local Self Help Wizard on the endpoint computer. Prior to specifying the text here, it has to be created and registered.
Users can define their own questions	✔	✔	As a security officer you can define the set of questions to be answered centrally and distribute it to the endpoint computer via the policy. However, you can also grant the users the right to define their own questions. To entitle users to define their own questions, select option Yes in this field.
Challenge / Response (CR)			
Enable Logon Recovery via C/R	✔	✔	Determines whether for logon recovery, a user is permitted to generate a challenge in the Power-on Authentication (POA) to regain access to their computer via a Challenge/Response procedure.

Policy setting	SGE	ESDP	Explanation
			<ul style="list-style-type: none"> ■ YES: User is permitted to generate a challenge and the Challenge button in the POA is active. In this case, the user can regain access to their computer via a C/R procedure. ■ NO: User is not permitted to issue a challenge and the Challenge button in the POA is inactive. In this case, the user cannot initiate a C/R procedure to regain access to their computer. <p>Sophos SafeGuard also offers the logon recovery method Local Self Help. It can be activated via the policy setting Enable Local Self Help.</p>
Information text	✔	✔	<p>Displays an information text when a Challenge/Response procedure is initiated in POA. Information texts can include, e.g. "Please contact Support Desk on telephone number 01234-56789." Prior to specifying a text here, you must create it as a text file in the Policies navigation area under Information text.</p>

Policy setting	SGE	ESDP	Explanation
Allow automatic logon to Windows			<p>Allows the user to log on to Windows automatically after authentication via Challenge/Response.</p> <ul style="list-style-type: none"> ■ YES: User is automatically logged on to Windows. ■ NO: Windows logon screen appears. <p>Application case: A user has forgotten their password. After the Challenge/Response procedure, Sophos SafeGuard logs the user on at the computer without an Sophos SafeGuard password. In this case automatic Windows logon is switched off and the Windows logon screen is displayed. The user cannot log on because they do not know the Sophos SafeGuard password (= Windows password). YES allows automatic logon and the user is able to move on from the Windows logon screen.</p>
IMAGES			<p>Prerequisite: New images must be registered in the policy navigation area of the SafeGuard Policy Editor under Images. The images will only be available after registration. Supported formats: .BMP, PNG, JPEG.</p>
<p>Background image in POA</p> <p>Background image in POA (low resolution)</p>			<p>Swaps the blue background bitmap with the SafeGuard design for the background of your choice. Customers might for example use the company logo in POA and at Windows logon. Maximum file size for all background bitmaps: 500 KB</p> <p>Normal:</p> <ul style="list-style-type: none"> ■ Resolution: 1024x768 (VESA mode) ■ Colors: unlimited <p>Low:</p> <ul style="list-style-type: none"> ■ Resolution: 640x480 (VGA mode) ■ Colors: 16 colors





Policy setting	SGE	ESDP	Explanation
<p>Logon image in POA</p> <p>Logon image in POA (low resolution)</p>			<p>Swaps the Sophos SafeGuard bitmap displayed in the POA logon dialog. For example, the company logo can be displayed in this dialog.</p> <p>Normal:</p> <ul style="list-style-type: none"> ■ Resolution: 413 x 140 pixels ■ Colors: unlimited <p>Low:</p> <ul style="list-style-type: none"> ■ Resolution: 413 x 140 pixels ■ Colors: 16 colors

16.2 Authentication

The way users log on to their computer is determined in policy of the type **Authentication**.

Policy Setting	SGE	ESDP	Explanation
ACCESS			
Users may only boot from hard disk	✔	✔	Determines whether users may start the PC from the hard drive and/or another medium. YES: Users can only boot from the hard disk. The POA does not offer the option to start the PC with a floppy disk or other external medium. NO: Users may start the PC from hard disk, floppy disk or external medium (USB, CD etc.)
LOGON OPTIONS			
Logon mode	✔	✔ Available option for this setting: User ID/Password Note: Fingerprint logon is not available with ESDP.	Determines how a user needs to authenticate themselves at the POA. <ul style="list-style-type: none"> ■ User ID/Password: Logon must be via user name and password in the POA. ■ Fingerprint: Select this setting to enable logon with Lenovo Fingerprint Reader. Users to whom this policy applies can then log on with a fingerprint or a user name and password. This procedure provides the maximum level of security. When logging on, the user swipes his or her finger over the fingerprint reader. Upon successful recognition of the fingerprint, the Power-on Authentication process reads the user's credentials and logs the user on to Power-on Authentication. The system then transfers the credentials to Windows, and the user is logged on to the computer. <p>Note: After selecting this logon procedure, the user can log on only with a pre-enrolled fingerprint or a user name and password.</p>

Policy Setting	SGE	ESDP	Explanation
Display unsuccessful logons for this user	✔	✔	Displays (setting: YES) after logon at the POA and Windows a dialog showing information on the last failed logon (user name/date/time).
Display last user logon	✔	✔	Displays (setting: YES) after logon at the POA and Windows a dialog showing information on the <ul style="list-style-type: none"> ■ last successful logon (user name/ date/time) ■ last user credentials of the logged on user
Disable “forced logoff” in workstation lock	✔	✔	If users wish to exit the endpoint computer for a short time only, they can click Block workstation to block the computer for other users and unlock it with the user password. If this option is set to NO , the user who has locked the computer as well as an administrator can unlock the it. If an administrator unlocks the computer, the currently logged on user is logged off automatically. Setting this field to YES changes this behavior. In this case, only the user can unlock the computer. The administrator cannot unlock it and the user will not be logged off automatically. Note: This setting only takes effect under Windows XP.
Activate user/domain preselection	✔	✔	Yes: The POA saves the user name and domain of the last logged on user. Users therefore do not need to enter their user names every time they log on. No: The POA <u>does not</u> save the user name and the domain of the last logged on user.

Policy Setting	SGE	ESDP	Explanation
Pass through to Windows			<p>Note: For the user to be able to grant other users access to their computer, the user has to be permitted to deactivate logon passthrough to Windows.</p> <ul style="list-style-type: none"> ■ Let user choose freely The user can decide by enabling/disabling this option in the POA logon dialog whether automatic logon at Windows is to be performed. ■ Enforce pass-through to Windows The user will always be automatically logged on to Windows. ■ Disable pass-through to Windows After the POA logon, the Windows logon dialog will be displayed. The user has to log on to Windows manually.
Service Account List			<p>To prevent that administrative operations on a Sophos SafeGuard protected computer lead to an activation of the Power-on Authentication and the addition of rollout operators as users to the computer, Sophos SafeGuard offers the possibility of creating service account lists for Sophos SafeGuard endpoint computers. The users included in these lists are thereby treated as Sophos SafeGuard guest users.</p> <p>Prior to selecting a list here you first have to create the lists in the Policies navigation under Service Account Lists.</p>

Policy Setting	SGE	ESDP	Explanation
FAILED LOGONS			
Maximum no. of failed logons	✔	✔	Determines how many times a user can attempt to log on using an invalid user name or password. After incorrectly entering a user name or password three times in a row for instance, a fourth attempt will trigger the “Response to a failed logon” setting.
Reaction to failed logons			
Lock machine	✔	✔	Determines whether the PC is locked after failed attempts to log on. The computer lock can be lifted by an administrator who must reboot the PC and log on. In this context, also take Windows user lock into consideration.
LOCK OPTIONS			
Lock screen after X minutes inactivity	✔	✔	Determines the time after which an unused desktop is automatically locked. The default value is 0 minutes in which case the desktop will not be locked.
Lock screen after resume	✔	✔	Determines whether the screen is locked if the computer is reactivated from standby mode.

16.3 Creating forbidden password list for use in policies

For policies of the type **Password** a list of forbidden passwords can be created to define character sequences which must not be used in passwords.

Note: In the lists, forbidden passwords are separated by line breaks.

The text files containing the required information have to be created prior to registering them in the SafeGuard Policy Editor. The maximum files size for text files is **50 KB**. Sophos SafeGuard only uses Unicode UTF-16 coded texts. If you do not create the text files in this format, they will be automatically converted upon registration.

In case of a conversion process, a message will be displayed indicating that the file is being converted.

To register text files, do the following:

1. In the policy navigation area, right-click **Information text** and select **New > Text**.
2. Enter a name for the text to be displayed in the **Text item name field**.
3. Click [...] to select the previously created text file. If the file needs to be converted, a message will be displayed.
4. Click **OK**.

The new text item is displayed as a subnode below **Information text** in the policy navigation area. If you select a text item, its contents will be displayed in the window on the right-hand side. The text item can now be selected when creating policies.

Proceed as described to register further text items. All registered text items will be shown as subnodes.

Note: Using the **Modify Text** button, you can add new text to existing text. When clicking this button a dialog is displayed for selecting another text file. The text contained in this file will be appended at the end of the existing text.

16.4 Syntax rules for passwords

Passwords can contain, numbers, letters and special characters (e.g.+ - ; etc.). However, when issuing a new password, do not use any character with the combination ALT + < character > as this input mode is not available at Power-on Authentication. Rules for passwords used to log on to the system are defined in policies of the type **Password**.

Note: If password rules have been defined in the SafeGuard Policy Editor, no rules should be defined in Active Directory.

Policy Setting	SGE	ESDP	Explanation
RULES			
Min. password length	✔	✔	Displays how many characters a password must comprise when changed by the user. The required value can be entered directly or increased/reduced using the arrow keys.
Max. password length	✔	✔	Displays the maximum number of characters a password must comprise when changed by the user. The required value can be entered directly or increased/reduced using the arrow keys.
Min. number of letters Min. number of digits Min. number of special characters	✔	✔	This setting specifies that a password may not consist exclusively of letters, numbers or special characters, but must consist of a combination of at least two (e.g. 15flower etc). This setting is only practical, if a minimum password length of greater than 2 has been defined.

Policy Setting	SGE	ESDP	Explanation
Case sensitive	✔	✔	<p>This setting is only effective with Use forbidden password list and User name as password forbidden.</p> <p>Case 1: You have entered “board” in the list of forbidden passwords. If option Case sensitive is set to YES, additional password variants such as BOARD, BoARd will not be accepted and logon will be denied.</p> <p>Case 2: “EMaier” is entered as a user name. If option Case sensitive is set to YES and option User name as password forbidden is set to NO, user EMAier cannot use any variant of this user name (e.g. “emaier“ or “eMaiER“) as a password.</p>
Keyboard row forbidden	✔	✔	<p>Consecutive key sequences include e.g. “123” or “qwe” A maximum of two adjacent characters on the keyboard is allowed. Consecutive key sequences relate only to the alphanumeric keyboard area.</p>
Keyboard column forbidden	✔	✔	<p>Refers to keys arranged consecutively in columns on the keyboard such as “yaq1”, “xsw2” or “3edc” (but not “yse4”, “xdr5” or “cft6”!). A maximum of two adjacent symbols in a single keyboard column is permitted. If you disallow keyboard columns, combinations like these are rejected as passwords. Consecutive key sequences relate only to the alphanumeric keyboard area.</p>
3 or more consecutive characters forbidden	✔	✔	<p>Activation of this option disallows key sequences.</p> <ul style="list-style-type: none"> ■ which are consecutive series of ASCII code symbols in both ascending and descending order (“abc”; “cba”; “;<” etc.). ■ which consist of three or more identical symbols (“aaa” or “111”).

Policy Setting	SGE	ESDP	Explanation
User name as password forbidden	✔	✔	<p>Determines whether user name and password may be identical.</p> <p>Yes: Users may use their Windows user names as passwords.</p> <p>No: Windows user name and password must be different.</p>
Use forbidden password list	✔	✔	<p>Determines whether certain character sequences must not be used for passwords. The character sequences are stored in the list of forbidden passwords (e.g. .txt file).</p>
List of forbidden passwords	✔	✔	<p>Defines character sequences which must not be used for passwords. If a user uses a forbidden password, an error message will be displayed.</p> <p>Important prerequisite:</p> <p>A list (file) of forbidden passwords must be registered in the SafeGuard Policy Editor in the policies navigation area under Information text. The list is only available after registration.</p> <p>Maximum file size: 50 KB Supported format: Unicode</p> <p>Defining forbidden passwords</p> <p>In the list, forbidden passwords are separated by a line break. Wildcard: The wildcard character “*” can represent any character and any number of characters in a password. Therefore *123* means that any series of characters containing 123 will be disallowed as a password.</p> <ul style="list-style-type: none"> ■ If the list contains only a wildcard, the user will no longer be able to log on to the system after a forced password change. ■ Users must not be permitted to access the file. ■ Option Use forbidden password list must be activated.

Policy Setting	SGE	ESDP	Explanation
CHANGES			
Password change allowed after min. (days)	✔	✔	Determines the period during which a password may not be changed. This setting prevents the user from changing a password too many times within a specific period. Example: User Miller defines a new password (e.g. "13jk56"). The minimum change interval for this user (or group to which this user is assigned) is set to five days. After two days the user wants to change the password to "74jk56". The password change is rejected because Mrs Miller may only define a new password after five days have passed.
Password expires after (days)	✔	✔	If the maximum period of validity is activated, the user has to define a new password after the set period has expired.
Notify of forced change before (days)	✔	✔	A warning message is displayed "n" days before password expiry reminding the user to change their password in "n" days. Alternatively, the user may change the password immediately.
GENERAL			
Password history length	✔	✔	Determines when previously used passwords can be reused. It makes sense to define the history length in conjunction with the "Password expires after (days)" setting.




Policy Setting	SGE	ESDP	Explanation
			<p>Example: The password history length for user Miller is set to 4, and the number of days after which the user must change their password is 30. Mr Miller is currently logging on using the password “Informatics”.</p> <p>After the 30 day period expires, he is asked to change his password. Mr Miller types in “Informatics” as the new password and receives an error message that this password has already been used and he needs to select a new password. Mr Miller cannot use password “Informatics” until after the fourth request to change the password (in other words password history length = 4).</p>

16.5 Passphrase rules for SafeGuard Data Exchange

Note: These settings are not supported with ESDP (Endpoint Security and Data Protection). For a description of SafeGuard Data Exchange, see [SafeGuard Data Exchange](#), page 100.

The user must enter a passphrase for secure data exchange via SafeGuard Data Exchange which is used to generate local keys. The requirements are defined in policies of the type **Passphrase**. For further details on SafeGuard Data Exchange and SafeGuard Portable refer to the Sophos SafeGuard User help, chapter *SafeGuard Data Exchange*.

Policy Setting	SGE	ESDP	Explanation
Min. Passphrase length	✔		Defines the minimum number of characters for the passphrase from which the key is generated. The required value can be entered directly or increased/reduced using the arrow keys.
Max. Passphrase length	✔		Defines the maximum number of characters for the passphrase. The required value can be entered directly or increased/reduced using the arrow keys.
Min. number of letters Min. number of digits Min. number of special characters	✔		This setting specifies that a passphrase may not consist exclusively of letters, numbers or symbols, but must consist of a combination of at least two (e.g. 15 flower etc). This setting is only practical if a minimum passphrase length of greater than 2 has been defined.
Case sensitive	✔		This setting is effective when User name as Passphrase forbidden is active. Example: “EMaier” is entered as a user name. If the option Case sensitive is set to YES and User name Passphrase forbidden is set to NO , user EMaier cannot use any variant of this user name (e.g. emaier or eMaiER) as a passphrase.
Keyboard row forbidden	✔		Consecutive key sequences include e.g. “123” or “qwe” A maximum of two adjacent characters on the keyboard is allowed. Consecutive key sequences relate only to the alphanumeric keyboard area.

Policy Setting	SGE	ESDP	Explanation
Keyboard column forbidden			Refers to keys arranged consecutively in columns on the keyboard such as “yaq1”, “xsw2” or “3edc” (but not “yse4”, “xdr5” or “cft6”!). A maximum of two adjacent characters in a single keyboard column is permitted. If you disallow keyboard columns, these combinations are rejected for passphrases. Consecutive key sequences relate only to the alphanumeric keyboard area.
3 or more consecutive characters forbidden			Activation of this option disallows key sequences <ul style="list-style-type: none"> ■ which are consecutive series of ASCII code symbols in both ascending and descending order (“abc”; “cba”; “;<” etc.). ■ which consist of three or more identical symbols (“aaa” or “111”).
User name as Passphrase forbidden			Determines whether the user name and passphrase may be identical. YES: Users may use their Windows user names as passphrases. NO: Windows user name and passphrase must be different.

16.6 Device Protection

The core of Sophos SafeGuard is the encryption of data on different data storage devices. Encryption can be volume or file based with different keys and algorithms. Policies of the type Device Protection also include settings for SafeGuard Data Exchange and SafeGuard Portable.

Note: For further details on SafeGuard Data Exchange and SafeGuard Portable refer to the Sophos SafeGuard User help, chapter *SafeGuard Data Exchange*.

Note: SafeGuard Data Exchange, SafeGuard Portable and file based encryption are not supported with ESDP.

When creating a policy for device protection, you first have to specify the target for device protection. Possible targets are:

- Mass storage (boot volumes/other volumes)
- Removable media (Not supported for installations with ESDP.)
- Optical drives (Not supported for installations with ESDP.)

For each target, a separate policy has to be created.

Policy Setting	SGE	ESDP	Description
Media encryption mode	✔	✔ Available options for this setting: <ul style="list-style-type: none"> ■ No Encryption ■ Volume based Note: File based settings are not available with ESDP.	Used to protect devices (PCs, Notebooks) and all types of removable media. The primary objective is to encrypt all data stored on local or external storage devices. The transparent operating method enables users to continue to use their usual applications e.g. Microsoft Office as usual. Transparent encryption means that all encrypted data (whether in encrypted directories or volumes) is automatically decrypted in the main memory as soon as it is opened in a program. A file is automatically re-encrypted when it is saved.



Policy Setting	SGE	ESDP	Description
			<p>The following options are available:</p> <ul style="list-style-type: none"> ■ No Encryption ■ Volume based (= transparent, sector based encryption) Ensures that all data is encrypted (incl. boot files, swapfiles, idle files/ hibernation files, temporary files, directory information etc.) without the user having to change normal operating procedures or consider security. <p>Note: If an encryption policy exists for a volume or a volume type and encryption of the volume fails, the user is not allowed to access it.</p> <p>Windows 7 System Partition: Note that for Windows 7 Professional, Enterprise and Ultimate, a system partition is created on endpoint computers without a drive letter assigned. This system partition cannot be encrypted by Sophos SafeGuard.</p> <p>Access to Unidentified File System Objects: Unidentified File System Objects are volumes that cannot be clearly identified as plain or device-encrypted by Sophos SafeGuard. If an encryption policy exists for an Unidentified File System Object, access to this volume will be denied. If no encryption policy exists, the user can access the volume If an encryption policy with Key to be used for encryption set to an option that enables key selection (e.g., Any key in user key ring) exists for an Unidentified File System Object volume, there is a period of time between the key selection dialog being displayed and access being denied.</p>

Policy Setting	SGE	ESDP	Description
			<p>During this time period the volume can be accessed. As long as the key selection dialog is not confirmed, the volume is accessible. To avoid this, specify a preselected key for encryption (see description of policy setting Key to be used for encryption).</p> <p>Furthermore, this period of time also occurs for Unidentified File System Object volumes connected to an endpoint computer, if the user has already opened files on the volume when an encryption policy takes effect, or if Autorun is enabled. In this case, it cannot be guaranteed that access to the volume will be denied as this could lead to data loss.</p> <p>Volumes with enabled Autorun functionality:</p> <p>If Autorun is enabled for a volume for which an encryption policy exists, the following problems can occur:</p> <ul style="list-style-type: none"> ■ The volume is not encrypted ■ If the volume is a UFO, access is not denied. ■ File based (= transparent, file based encryption (Smart Media Encryption)) <p>Ensures that all data is encrypted (apart from Boot Medium and directory information) with the benefit that even optical media such as CD/DVD can be encrypted or data can be swapped with external computers on which SafeGuard is not installed (provided policies permit).</p>

Policy Setting	SGE	ESDP	Description
			Note: Data encrypted using “File based encryption” cannot be compressed. Nor can compressed data be file based encrypted. Boot volumes will never be file-based encrypted. They will be automatically exempt from file-based encryption, even if a corresponding rule is defined.
GENERAL SETTINGS			
Algorithms to be used for encryption	✔	✔	Sets the encryption algorithm. List of all usable algorithms with respective standards: AES256: 32 bytes (256 bits) AES128: 16 bytes (128 bits)
Key to be used for encryption	✔	✔	Defines which key is used for encryption. For Sophos SafeGuard encryption, only an automatically generated machine key is used for volume based encryption. For file based encryption only local keys created by the user can be used. The following option is available: Defined machine key: The machine key is used - the user CANNOT select a key.
User is allowed to create a local key	✔		This setting determines whether the user can generate a local key on their computer or not. Local keys are generated on the endpoint computer based on a passphrase entered by the user. The passphrase requirements can be set in policies of the type Passphrase . Note: As only local keys are used for file based encryption, the user has to be able to create local keys, if policies for file based encryption are to become effective. The default setting of this field (not configured) allows the user to create local keys.

Policy Setting	SGE	ESDP	Description
VOLUME BASED SETTINGS			
Users may add or remove keys to or from encrypted volume	✔		<p>YES: Sophos SafeGuard users may add/remove keys to/from a key ring. The dialog is displayed via the context menu command Encryption/Encryption tab.</p> <p>NO: Sophos SafeGuard users may not add additional keys.</p>
Reaction to unencrypted volumes	✔	✔	<p>Defines how Sophos SafeGuard handles unencrypted media.</p> <p>The following options are available:</p> <ul style="list-style-type: none"> ■ Reject (= text medium is not encrypted) ■ Accept only blank media and encrypt ■ Accept all media and encrypt
User may decrypt volumes	✔	✔	Allows the Sophos SafeGuard user to decrypt the volume via a context menu command in Windows Explorer.
Fast initial encryption	✔	✔	<p>Select this setting to enable the fast initial encryption mode for volume-based encryption. This mode reduces the time needed for initial encryption on endpoint computers.</p> <p>Note: This mode may lead to a less secure state.</p> <p>For further information, see Fast initial encryption, page 8.</p>
Proceed on bad sectors	✔	✔	Specifies whether encryption should proceed or be stopped in case bad sectors are detected. The default setting is YES .
FILE BASED SETTINGS			
Initial encryption of all files	✔		Automatically starts initial encryption for a volume after user logon. The user may need to select a key from the key ring beforehand.
User may cancel initial encryption	✔		Enables a user to cancel initial encryption.
User is allowed to access unencrypted files	✔		Defines whether a user may access unencrypted data on a volume.

Policy Setting	SGE	ESDP	Description
User may decrypt files	✔		Enables a user to decrypt individual files or whole directories (via the Windows Explorer extension <right-click>).
User may define a Media Passphrase for devices	✔		Enables a user to define a media passphrase on their computer. The media passphrase allows to easily access all used local keys on computers without SafeGuard Data Exchange via SafeGuard Portable.
Unhandled Applications	✔		<p>Allows other applications to be defined which are to be ignored by the Sophos SafeGuard filter driver and thereby excluded from transparent encryption/decryption. The delimiter to be used for these applications is ‘;’.</p> <p>One example of an unhandled application is a backup program. To ensure that data is not decrypted when creating a backup, this application can be exempted from encryption/decryption. The data is backed up in encrypted form.</p> <p>Note: Since these are machine-specific settings, they are not applied until the endpoint computer is rebooted.</p> <p>Defining unhandled applications</p> <p>Typical use:</p> <p>Backup programs can be defined as exempted so they will always be able to read and back up encrypted data.</p> <p>Applications which might trigger malfunctions when used alongside Sophos SafeGuard, but do not require encryption, can generally be exempted from encryption.</p>

Policy Setting	SGE	ESDP	Description
			<p>The full name of the executable file (optionally including path information) is used to specify an exempted application.</p> <p>Note: Unhandled applications can only be defined for local storage devices. For a global policy of the type Device Protection, target Local Storage Devices must be selected. For all other targets, option Unhandled Applications is not available.</p>
<p>Removable Media only Copy SG Portable to Removable Media</p>			<p>If this option is switched on, SafeGuard Portable is copied to any removable media connected to the endpoint computer.</p> <p>SafeGuard Portable enables the exchange of encrypted data with removable media without the recipient having Sophos SafeGuard installed.</p> <p>The recipient can decrypt and re-encrypt the encrypted files using SafeGuard Portable and the corresponding passphrase. The recipient can re-encrypt files with SafeGuard Portable or use the original key for encryption.</p> <p>SafeGuard Portable does not have to be installed or copied to the recipient's computer but can be used directly from the removable media.</p>
<p>Plaintext folder</p>			<p>The folder specified here will be created on every removable media. Files that are copied to this folder will always stay plain.</p>

16.7 Specific machine settings - basic settings









Policy Setting	SGE	ESDP	Explanation
POWER-ON AUTHENTICATION (POA)			
Enable Power-on Authentication	✔	✔	<p>Defines whether POA is permanently switched on or off.</p> <p>Note: For security reasons we strongly recommend to keep the POA switched on. Deactivating the POA reduces the system security to Windows logon security and increases the risk of unauthorized access to encrypted data.</p>
Forbid guest user	✔	✔	<p>Defines whether a user is entitled to log on to Windows.</p>
Secure Wake On LAN (WOL)	✔	✔	<p>The “Secure Wake On LAN” policy enables the endpoint computer to prepare for software rollouts in which the necessary parameters such as temporary deactivation of POA and a time interval for Wake On LAN can be imported directly into and analyzed by the endpoint computer. The rollout team can design a scheduling script using the commands provided to guarantee maximum Sophos SafeGuard protection despite deactivated POA.</p> <p>Please be advised that deactivating the POA - even for a limited number of boot processes - reduces the level of security for your system!</p>



Policy Setting	SGE	ESDP	Explanation
			<p>EXAMPLE: The SW rollout team notifies the Sophos SafeGuard security officer (SO) about a planned software rollout for the 25th September 2010 between 03:00 and 06:00 am. 2 reboots are required. The local software rollout agent must be able to log on to Windows. The SO creates the following policy and assigns it to the corresponding endpoint computers:</p> <p>Number of auto logons (0 = no WOL): 5</p> <p>Windows logon permitted during WOL: Yes</p> <p>Start of time slot for external WOL Start: 24th Sept. 2010, 12:00</p> <p>End of time slot for external WOL Start: 25th Sept. 2010, 06:00</p> <p>The SO provides a buffer of 3 for automatic logons.</p> <p>The security officer sets the time interval to 12 o'clock midday on the day before the software rollout to allow the scheduling script SGMCMDDIntn.exe to be started promptly and WOL starts no later than the 25th September at 3:00 am.</p> <p>The software rollout team produces two commands for the scheduling script:</p> <ul style="list-style-type: none"> ■ Starting 24th Sept.2010, 12:15 am, SGMCMDDIntn.exe /WOLstart ■ Starting 26th Sept.2010, 09.00 am SGMCMDDIntn.exe /WOLstop

Policy Setting	SGE	ESDP	Explanation
			<p>The software rollout script is dated 25.09.2010, 03:00. WOL can be explicitly deactivated again at the end of the script using SGMCMDDIntn.exe / WOLstop.</p> <p>All endpoint computers logging on before the 24th of September 2010 and which connect to the rollout servers, will receive the new policy and the scheduling commands.</p> <p>Any endpoint computer on which the schedule triggers the command SGMCMDDIntn/WOLstart between 24th Sept. 2010,12:00 midday and 25th Sept. 2010, 06:00 am falls within the WOL time interval and therefore Wake On LAN will be activated.</p>
Number of auto logons	✔	✔	<p>Defines the number of reboots while Power-on Authentication is switched off for Wake On LAN.</p> <p>This setting temporarily overwrites the Enable Power On Authentication setting until the automatic logons reach the preset number. Power-on Authentication is then reactivated.</p> <p>Example: the number of automatic logons is set to 2, "Enable Power-on Authentication" is switched on. The PC boots twice without authentication. via POA.</p> <p>For Wake On LAN, we always recommend allowing three more reboots than necessary to overcome any unforeseen problems.</p>
Windows logon allowed during WOL	✔	✔	<p>Determines whether Windows logon is permitted during Wake On LAN, e.g. for a software update. This setting is analyzed by the POA.</p>

Policy Setting	SGE	ESDP	Explanation
Start of time slot for external WOL start End of time slot for external WOL start	✔	✔	<p>Date and time can be either selected or input for the start and end of the Wake On LAN (WOL).</p> <p>Date format: <i>MM/DD/YYYY</i> Time format: <i>HH:MM</i></p> <p>The following input combinations are possible:</p> <ul style="list-style-type: none"> ■ Defined start and end of WOL. ■ End of WOL is defined, start is open ■ No entries: no time interval has been set for the endpoint computer <p>In the event of a planned software rollout, the SO should set the time frame for the WOL such that the scheduling script can be started early enough to allow all endpoint computers sufficient time for booting.</p> <p>WOLstart: The starting point for the WOL in the scheduling script must be within the time interval set in the policy. If no interval is defined, WOL is not locally activated on the Sophos SafeGuard endpoint computer.</p> <p>WOLstop: This command is carried out irrespective of the final point set for the WOL.</p>
DISPLAY OPTIONS			
Display machine identification	✔	✔	<p>Displays either the computer name or a defined text in the POA title bar.</p> <p>If the Windows network settings include the machine name this is automatically incorporated into the basic settings.</p>
Machine identification text	✔	✔	<p>The text to be displayed in the POA title bar.</p> <p>If you have selected Defined name in the Display machine identification field, you can enter the text in this input field.</p>

Policy Setting	SGE	ESDP	Explanation
Display legal notice	✔	✔	Displays a text box with a configurable content which is displayed prior to authentication in the POA. In some countries a text box with certain content must be displayed by law. The box needs to be confirmed by the user before the system continues. Prior to specifying a text, the text has to be registered as a text item in the policy navigation area under Information text .
Legal notice text	✔	✔	The text to be displayed as a legal notice. In this field, you can select a text item registered under Information text in the policy navigation area .
Display additional information	✔	✔	Displays a text box with a configurable content which appears after the legal notice (if activated). You can define whether the additional information is to be displayed <ul style="list-style-type: none"> ■ Never ■ Every system start ■ Every logon
Additional information text	✔	✔	The text to be displayed as additional information. In this field, you can select a text item registered under Information text in the policy navigation area .
Show for (sec.)	✔	✔	In this field you can define how long (in seconds) additional information is to be displayed. You can specify the number of seconds after which the text box for additional information will be closed automatically. The user can close the text box any time by clicking OK .

Policy Setting	SGE	ESDP	Explanation
Enable and show the system tray icon			<p>Via the Sophos SafeGuard System Tray Icon the user can access all user functions quickly and easily on their computer. In addition, information about the Sophos SafeGuard status (new policies received,...) can be displayed in balloon tool tips.</p> <p>Yes: The system tray icon is displayed in the information area of the taskbar and the user is continually informed via the Tool Tips balloon about the status of Sophos SafeGuard.</p> <p>No:The system tray icon is not displayed. No status information for the user via the balloon tool tips.</p> <p>Silent: The system tray icon is displayed in the information area of the taskbar but there is no status information for the user via the balloon tool tips.</p>
Show overlay icons in Explorer			Defines whether Windows key symbols will be shown to indicate the encryption status of volumes, devices, folders and files.
Virtual Keyboard in POA			Defines whether a virtual keyboard can be shown on request in the POA dialog for entering the password.
INSTALLATION OPTIONS			
Uninstallation allowed			Determines whether uninstallation of Sophos SafeGuard is allowed on the endpoint computers. When Uninstallation allowed is set to No , Sophos SafeGuard cannot be uninstalled, even by somebody having administrator rights, while this setting is active within a policy.

Policy Setting	SGE	ESDP	Explanation
<p>Enable Sophos tamper protection</p>			<p>Activates/deactivates Sophos Tamper Protection. If you have allowed uninstallation of Sophos SafeGuard via the policy setting Uninstallation allowed, you can set this policy setting to Yes, to ensure that uninstallation attempts are checked by Sophos Tamper Protection to prevent casual removal of the software.</p> <p>If Sophos Tamper Protection does not allow uninstallation, any uninstallation attempts will be canceled.</p> <p>If Enable Sophos Tamper Protection is set to No, uninstallation of Sophos SafeGuard will not be checked or prevented by Sophos Tamper Protection.</p> <p>Note: This setting only applies to endpoint computers using Sophos Endpoint Security and Control version 9.5 or higher.</p>

16.8 Logging

Events for Sophos SafeGuard are logged in the Windows Event Viewer. To specify the events to be logged in the Windows Event Viewer, create a policy of the type **Logging** and select the required events by clicking on them.

Many different events from different categories (for example Authentication, Encryption, etc.) are available for selection. It is recommended to define a strategy for logging, and determine the events necessary according to reporting and auditing requirements.

17 SafeGuard Data Exchange

Note: SafeGuard Data Exchange and SafeGuard Portable are not supported with ESDP (Endpoint Security and Data Protection).

SafeGuard Data Exchange is used to encrypt data stored on removable media connected to a Sophos SafeGuard endpoint computer and to exchange these data with other users. All encryption and decryption processes run transparently and involve minimum user interaction.

Only users who have the appropriate keys can read the contents of the encrypted data. All subsequent encryption processes run transparently.

As a security officer you define the specific settings in a policy of the type **Device Protection** with **Device protection target: Removable Media**.

17.1 Local Keys

SafeGuard Data Exchange supports encryption using local keys. Local keys are created on the endpoint computers and can be used to encrypt data on removable media. They are created by entering a passphrase.

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

If local keys are used to encrypt files on removable media, these files can be decrypted using SafeGuard Portable on a computer without SafeGuard Data Exchange. When the files are opened with SafeGuard Portable the user is prompted to enter the passphrase that was specified when the key was created. If the user knows the passphrase they can open the file.

Using SafeGuard Portable every user who knows the passphrase can get access to an encrypted file on removable media. This way it is also possible to share encrypted data with partners, who do not have Sophos SafeGuard. They only need to be provided with SafeGuard Portable and the passphrase for the files they should have access to.

If different local keys are used to encrypt files on removable media, you can even restrict access to files. For example: You encrypt the files on a USB stick using a key with passphrase `my_localkey` and encrypt a single file named `ForMyPartner.doc` using the passphrase `partner_localkey`. If you give the USB stick to a partner and provide them with the passphrase `partner_localkey`, they will only have access to `ForMyPartner.doc`.

Note: By default SafeGuard Portable is automatically copied to all removable media connected to the system. If you do not want SafeGuard Portable to be automatically copied to removable media, deactivate the **Copy SG Portable to Removable Media** option in a policy of the type **Device Encryption**.

17.2 Media passphrase

Additionally SafeGuard Data Exchange allows to specify that one single media passphrase for all removable media - except optical media - has to be created on the endpoint computers. The media passphrase provides access to all used local keys in SafeGuard Portable. The user only has to enter one single passphrase and gets access to all encrypted files in SafeGuard Portable, regardless of the local key used for encryption.

On every computer a unique Media Encryption Key for data encryption is automatically created for each device. This key is protected with the media passphrase. On a computer with SafeGuard Data Exchange it is therefore not necessary to enter the media passphrase to access encrypted files on the removable media. Access is granted automatically if the appropriate key is part of the user's key ring.

Media passphrase functionality is available when the **User may define a Media Passphrase for devices** option is activated in a policy of the type **Device Protection**.

When this setting becomes active on the computer, the user is automatically prompted to enter a media passphrase, when he connects removable media for the first time. The user may also change the media passphrase and it will be synchronized automatically when the passphrase known on the computer and the media passphrase of the removable media are out of sync.

In case the user forgets the media passphrase, it can be recovered by the user without any need of a help desk.

Note: To enable the media passphrase activate the **User may define a Media Passphrase for devices** option in a policy of the type **Device Encryption**.

On a Sophos SafeGuard protected computer without an activated media passphrase feature no keys are available after installation has been completed since Sophos SafeGuard endpoint computers only use local keys. Before encryption can be used, the user has to create a key.

In case the media passphrase feature is activated in a removable media policy for Sophos SafeGuard protected computers, the media encryption key is created automatically on the endpoint computer and can be used for encryption immediately after installation has been completed. It is available as „predefined“ key“ in the users key ring and is displayed as <user name> in dialogs for key selection.

If available, the media encryption keys will also be used for all initial encryption tasks.

18 Power-on Authentication (POA)

Sophos SafeGuard identifies the user even before the operating system starts up. To do this, Sophos SafeGuard's own system core starts before this. It is protected against modifications and is saved, hidden, on the hard disk. Only when the user has been properly authenticated in the POA, the actual operating system (Windows) is started from the encrypted partition and the user is logged on automatically to Windows later. The procedure is the same when the endpoint computer is switched back on from hibernation (Suspend to Disk).



The Sophos SafeGuard Power-on Authentication has benefits such as:

- a graphical user interface with mouse support and draggable windows, so it is easy to read and use.
- a graphical layout which, following guidelines, can be adapted by corporate computers (background image, logon image, welcome message, etc.).
- support for Windows user accounts and passwords even pre-boot, no more separate credentials which the user has to remember
- support for Unicode and therefore also foreign language passwords and user interfaces

18.1 Logon delay

On a Sophos SafeGuard protected computer, a logon delay applies if a user provides incorrect credentials during authentication at Windows or at the Power-on Authentication. With every failed logon attempt the delay is increased. After a failed logon a dialog is shown to display the remaining delay time.

You can specify the number of logon attempts allowed in a policy of the type **Authentication** using option **Maximum no. of failed logons**.

18.2 Machine lock

In a policy of the type **Authentication** you can also specify that the computer is to be locked after the set number of failed logon attempts by setting option **Lock Machine** to **Yes**. For unlocking their computer, users have to initiate a Challenge/Response procedure.

18.3 Configuring the Power-on Authentication

The POA dialog consists of these components:

- Logon image
- Dialog text
- Language of the keyboard layout



You can alter the look of the POA dialog to suit your preferences using, e.g., policy settings in the SafeGuard Policy Editor.

18.3.1 Background and logon image

By default the background and logon images that appear in the POA are in SafeGuard design. However, different images can be shown, e.g. the company's logo.

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

For usage in Sophos SafeGuard, background and logon images must fulfill certain requirements:

Background image

Maximum file size for all background images: **500 KB**

Sophos SafeGuard supports two variants for background images:

- **1024x768** (VESA mode)

Colors: no restrictions

Option in policy type **General Settings: Background image in POA**

- **640x480** (VGA mode)

Colors: 16

Option in policy type **General Settings: Background image in POA (low resolution)**

Logon image

Maximum file size for all logon images: **100 KB**

Sophos SafeGuard supports two variants for logon images:

- **413x140**

Colors: no restrictions

Option in policy type **General Settings: Logon image in POA**

- **413x140**

Colors: 16

Option in policy type **General Settings: Logon image in POA (low resolution)**

Images, information texts and lists have to be created as files (BMP, PNG, JPG or text files) first and can then be registered in the navigation window.

18.3.1.1 Registering images

To register images do the following:

1. In the **Policies** navigation area right-click **Images** and select **New > Image**.
2. Enter a name for the image in the **Image Name** field.
3. Click [...] to select the previously created image.
4. Click **OK**.

The new image will be shown as a subnode of **Images** in the policy navigation area. If you select the image, it will be displayed in action area. The image can now be selected when creating policies.

Proceed as described to register further images. All registered images will be shown as subnodes.

Note: Using the **Modify Image** button you can exchange the picture assigned. Upon clicking this button a dialog is displayed for selecting a different image.

18.3.2 User defined information text in the POA

You can customize the POA to display the following **user-defined information texts**:

- Information text to be displayed upon initiating a Challenge/Response procedure for logon recovery (e.g.: "Please contact Support Desk on telephone number 01234-56789.")

Option in policy type **General Settings: Information text**

- Legal notices to be displayed after logging on to the POA

Option in policy type **Specific Machine Settings: Legal notice text**

- Text for additional information to be displayed after logging on to the POA

Option in policy type **Specific Machine Settings: Additional information text**

18.3.2.1 Registering information texts

The text files containing the required information have to be created prior to registering them in the SafeGuard Policy Editor. The maximum files size for information texts is **50 KB**. Sophos SafeGuard only uses Unicode UTF-16 coded texts. If you do not create the text files in this format, they will be automatically converted upon registration.

In case of a conversion process, a message will be displayed indicating that the file is being converted.

To register information texts:

1. In the **Policies** navigation area right-click **Information text** and select **New > Text**.
2. Enter a name for the text to be displayed in the **Text item name** field.
3. Click [...] to select the previously created text file. If the file needs to be converted, a message will be displayed.
4. Click **OK**.

The new text item is displayed as a subnode below **Information text** in the policy navigation area. If you select a text item, its contents will be displayed in the window on the right-hand side. The text item can now be selected when creating policies.

Proceed as described to register further text items. All registered text items will be shown as subnodes.

Note: Using the **Modify Text** button, you can add new text to existing text. When clicking this button a dialog is displayed for selecting another text file. The text contained in this file will be appended at the end of the existing text.

18.3.3 Language for 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.

After installation, the language in which the POA dialog text is displayed can only be changed via a policy defined in the SafeGuard Policy Editor. Changing the default language under Windows does not affect the language of the POA dialog text.

The language for the POA dialog text is defined via a policy of the type **General Settings** (option **Language used on Client**).

18.3.4 Keyboard Layout

Almost every country has its own keyboard layout, i.e. the keys are assigned differently. The keyboard layout in the POA is significant when entering user names, passwords and response code.

As the default, Sophos SafeGuard adopts the keyboard layout in the POA which is set in Windows' Regional and Language Options for the Windows default user at the time Sophos SafeGuard is installed. If "German" is the keyboard layout set under Windows, the German keyboard layout will be used in the POA.

The language of the keyboard layout being used is displayed in the POA, e.g. "EN" for English. Apart from the default keyboard layout, the US keyboard layout (English) can also be used.

There are certain exceptions:

- The keyboard layout is, indeed, supported, but the absence of a font (e.g. for Bulgarian) means that only special characters are displayed in the **User Name** field.
- No specific keyboard layout is available (e.g. Dominican Republic). In these cases, the POA falls back on the original keyboard layout. For the Dominican Republic, this is "Spanish".

Note: All the unsupported keyboard layouts use the US keyboard layout as the default. This also means that the only characters that are recognized and can be keyed in are those which are supported in the US keyboard layout. So users can only log on to the POA if their user name and password is composed of characters that are supported by the US keyboard layout or the respective fallback keyboard of their language.

18.3.4.1 Virtual keyboard

Sophos SafeGuard provides a virtual keyboard which users can show/hide at the POA and click the on-screen keys to enter credentials etc.

As a security officer you can activate/deactivate the display of the virtual keyboard in a policy of the type **Specific Machine Settings** using the **Virtual Keyboard** option.

Virtual keyboard support must be activated/deactivated via a policy setting.

The virtual keyboard will support different layouts and it will be possible to change the layout using the same options as for changing the POA keyboard layout.

18.3.4.2 Changing the keyboard layout

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

To change the language of the keyboard layout, do as follows:

1. Select **Start > Control Panel > Regional and Language Options > Advanced**.
2. In the **Regional Options** tab, select the required language.
3. In the **Advanced** tab, activate option **Apply all settings to the current user account and to the default user profile** under **Default user account settings**.
4. Confirm your settings with **OK**.

The POA remembers the keyboard layout used for the last successful logon and automatically enables it for the next logon. This requires two reboots of the endpoint computer. If the remembered keyboard layout is deactivated via **Regional and Language Options**, it is still maintained up to the point where the user selects a different one.

Note: Additionally, it is required to change the language of the keyboard layout for non-Unicode programs.

If the language you want is not available on the system, Windows may prompt you to install it. After you have done so you need to reboot the computer twice so that, first, the new keyboard layout can be read in by the Power-on Authentication and, secondly, the POA can set the new layout.

You can change the required keyboard layout for the Power-on Authentication using the mouse or keyboard (**Alt+Shift**).

You can see which languages are installed and available on the system via **Start > Run > regedit > HKEY_USERS\DEFAULT\Keyboard Layout\Preload**.

18.4 Supported Hotkeys in the Power-on Authentication

Certain hardware settings and functionalities can lead to problems when booting endpoint computers, causing the system to hang. The Power-on Authentication supports a number of hotkeys for modifying these hardware settings and deactivating functionalities. Furthermore, grey and black lists covering functions known to cause problems are integrated in the .msi file installed on the computer.

We recommend that you install an updated version of the POA 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>

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

Note: When defining a customized file, only this will be used instead of the one integrated in the .msi file. Only when no POA configuration file is defined or found, the default file will be applied.

To install the POA configuration file, enter the following command:

```
MSIEXEC /i <Client MSI package> POACFG=<path of the POA configuration file>
```

For further information see the knowledgebase: <http://www.sophos.com/support/knowledgebase/article/65700.html>.

The following hotkeys are supported in the POA:

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

USB Hotkeys dependency matrix

Shift F3	Shift F5	Shift F7	Legacy	USB 1.x	USB 2.0	Comment
off	off	off	on	on	on	3.
on	off	off	off	on	on	Default
off	on	off	on	off	off	1., 2.
on	on	off	on	off	off	1., 2.
off	off	on	on	on	off	3.
on	off	on	off	on	off	
off	on	on	on	off	off	
on	on	on	on	off	off	2.

1. Shift F5 disables both USB 1.x and USB 2.0.

Note: Pressing Shift F5 during boot time will considerably reduce the time the POA is launched. However, please be aware that if the computer uses a USB keyboard or USB mouse, they might be disabled when pressing **Shift F5**.

2. If no USB support is active, the POA tries to use BIOS SMM instead of backing up and restoring the USB controller. The Legacy mode may work in this scenario.
3. Legacy support is active, USB is active. The POA tries to backup and restore the USB controller. The system might hang depending on the BIOS version used.

You can specify changes that can be carried out using hotkeys when installing Sophos SafeGuard encryption software using a .mst file. This is done using the appropriate call in combination with msixexec.

NOVESA	Defines whether VESA or VGA mode is used.0 = VESA mode (standard)1 = VGA mode
NOLEGACY	Defines whether Legacy Support is activated after POA log on.0 = Legacy Support activated 1 = Legacy Support not activated (standard)
ALTERNATE:	Defines whether USB devices are supported by the POA. 0 = USB support is activated (standard)1 = no USB support
NOATA	Defines whether int13 device driver is used.0 = standard ATA device driver (default)1 = Int13 device driver
ACPIAPIC	Defines whether ACPI/APIC support is used.0 = no ACPI/APIC support (default)1 = ACPI/APIC support active

NOVESA	Defines whether VESA or VGA mode is used.0 = VESA mode (standard)1 = VGA mode
--------	---

18.5 Disabled POA and Lenovo Rescue and Recovery

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

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

19 Recovery options

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

For detailed information see [Recovery via Local Self Help](#), page 113.

■ 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.

For detailed information see [Recovery via Challenge/Response](#), page 119.

■ System recovery

Sophos SafeGuard offers different methods and tools for recovery regarding crucial system components and Sophos SafeGuard components, for example:

- Corrupted MBR
- Sophos SafeGuard kernel problems
- Volume access problems
- Windows boot problems

For detailed information see [System Recovery](#), page 135.

20 Recovery via Local Self Help

Sophos SafeGuard offers Local Self Help for Sophos SafeGuard protected computers to enable users who have forgotten their password to log on to their computers without the assistance of the help desk.

With Local Self Help, users can, for example, regain access to their laptops in situations where neither telephone nor network connections are available and where they cannot use a Challenge/Response procedure (for example aboard an aircraft). The user can log on to their computer by answering a predefined number of questions in the Power-on Authentication.

As a security officer you can define the set of questions to be answered centrally and distribute it to the computer via a policy. We provide you with a predefined question theme as a template. You can use this question theme as is or modify it. In the relevant policy, you can also grant the users the right to define their own questions.

For providing the initial answers and editing the questions, the Local Help Self Wizard is available on the endpoint computer after the function has been enabled by policy. For a detailed description of Local Self Help on the endpoint computer refer to the Sophos SafeGuard User help, chapter *Recovery via Local Self Help*.

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.

20.1 Defining Local Self Help settings via policy

You define the settings for Local Self Help in a policy of the type **General Settings** under **Logon Recovery - Enable Local Self Help**. This is where you enable the function to be used on the endpoint computers and define further rights and parameters.

20.1.1 Enabling Local Self Help

To activate Local Self Help for use on endpoint computers, select **Yes** in the **Enable Local Self Help** field.

After the policy has become effective on the computers, this setting entitles the users to use Local Self Help for logon recovery. To be able to use Local Self Help, the users now have to activate this recovery method by answering a specified number from the set of questions received or by creating and answering their own questions - depending on permission.

For this purpose, the Local Self Help Wizard will be available via the System Tray Icon in the Windows taskbar after receiving the policy and restarting the computer.

20.1.2 Defining further settings

Besides enabling Local Self Help you can define the following parameters for this function in a policy of the type **General Settings**:

- **Minimal length of answers**

In this field, define the minimum length of the answers in characters. The default is **1**.

- **Welcome text under Windows**

In this field, you can specify the individual information text to be displayed in the first dialog when launching the Local Self Help Wizard on the computer. Prior to specifying the text here, it has to be created and registered.

- **Users can define their own questions**

There are the following possible scenarios for the definition of questions for Local Self Help:

- As a security officer you define the questions and distribute them to the users. The users are not permitted to define their own questions.
- As a security officer you define the questions and distribute them to the users. In addition, the users are permitted to define their own questions. When answering the minimum number of questions required for activating Local Self Help, the users can choose between predefined questions and their own questions or use a combination of both.
- You entitle the users to define their own questions. The users activate Local Self Help on their computers by defining and answering their own questions.

To entitle users to define their own questions, select option **Yes** in the **Users can define their own questions** field.

20.2 Defining questions

To be able to use Local Self Help on the endpoint computer, the user has to answer and save at least ten questions. To log on at the Power-on Authentication via Local Self Help, the user has to answer five questions randomly selected from these ten questions.

If the user is not permitted to define their own questions, you therefore have to transfer at least ten predefined questions to the computer with the policy to enable the user to activate Local Self Help.

For registering and editing Local Self Help questions you as a security officer need the right to **Modify selfhelp questions**.

20.2.1 Using the template

For Local Self Help a predefined question theme is available. By default, this question theme is available in German and English in the policy navigation area under **Local Self Help questions**.

Optionally, the question theme is also available in French, Italian, Spanish, and Japanese. You can additionally import these language versions into the policy navigation area.

Note: When entering answers in Japanese to activate Local Self Help on endpoint computers, users have to use Romaji (Roman) characters. Otherwise the answers will not match when users enter them in the Power-on Authentication.

You can use the predefined question theme as is, edit it or delete it.

If you leave the two language versions of the predefined question theme as is and enable Local Self Help via a policy of the type **General Settings**, the two predefined question themes will be transferred automatically to the endpoint computers with the policy.

20.3 Importing question themes

Using the import procedure, you can import additional language versions of the predefined question theme or your own question lists created as .XML files.

To import a set of questions:

1. Create a new question theme.
2. In the **Policies** navigation area select the new question theme under **Local Self Help questions**.
3. Right-click in the action area to open the context menu for the question theme. In the context menu, select **Import**.
4. Select the required directory and question theme and click **Open**.

The imported questions are displayed in the action area. You can now save the question theme as is or edit it.

20.4 Creating a new question theme and adding questions

Besides using question themes in different languages, you can also create new question themes covering different topics, to provide users with several different question themes to suite their preferences.

To create a new question theme and add questions, do the following:

1. In the **Policies** navigation area, select **Local Self Help questions**.
2. Right-click **Local Self Help questions** and select **New > Question Theme**.
3. Enter a name for the question theme and click **OK**.
4. In the **Policies** navigation area select the new question theme under **Local Self Help questions**.
5. Right-click in action area to open the context menu for the question theme. In the context menu, select **Add**.
6. A new question line is added. Enter your question and press **Enter**. To add further questions repeat this step.
7. To save your changes click the **Save** icon in the toolbar.

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

20.5 Editing question themes

To edit existing question themes do the following:

1. In the **Policies** navigation area, select the required question theme under **Local Self Help questions**
2. You can now add, modify or delete questions.
 - To add questions, right-click in the action area, to display the context menu. In the context menu, click **Add**. A new line is added to the question list. Enter your question on the line.
 - To modify questions, click the required question text in the action area. The question is marked by a pencil icon. Enter your changes on the question line.
 - To delete questions, select the required question by clicking on the grey box at the beginning of the question line in the action area and click **Delete** in the context menu of the question.
3. To save your changes click the **Save** icon in the toolbar.

The modified question theme is registered and will be transferred with the policy of the type **General Settings** that will enable Local Self Help on the endpoint computers.

20.6 Deleting question themes

To delete an entire question them, right-click the required theme **Local Self Help questions** in the **Policies** navigation area, and select **Delete**.

Note: If you delete a question theme after users have answered some of these questions to activate Local Self Help on their computers, the users' answers become invalid, as the questions no longer exist.

20.7 Registering welcome texts

You can register a welcome text to be displayed in the first dialog of the Local Self Help Wizard in the Policies navigation area of the SafeGuard Policy Editor.

The text files containing the required information have to be created prior to registering them in the SafeGuard Policy Editor. The maximum files size for information texts is 50 KB. Sophos SafeGuard only uses Unicode UTF-16 coded texts. If you do not create the text files in this format, they will be automatically converted upon registration.

In case of a conversion process, a message will be displayed indicating that the file is being converted.

To register information texts:

1. In the **Policies** navigation area right-click **Information text** and select **New > Text**.
2. Enter a name for the text to be displayed in the **Text item name** field.
3. Click [...] to select the previously created text file. If the file needs to be converted, a message will be displayed.
4. Click **OK**.

The new text item is displayed as a subnode below **Information text** in the **Policies** navigation area. If you select a text item, its contents will be displayed in the window on the right-hand side. The text item can now be selected when creating policies.

Proceed as described to register further text items. All registered text items will be shown as subnodes.

21 Recovery via Challenge/Response

To smoothen the workflow and to reduce help desk costs, Sophos SafeGuard provides a Challenge/Response recovery solution. Sophos SafeGuard offers help to users failing to log on to their computers or failing to access encrypted data by providing a user-friendly Challenge/Response mechanism.

This functionality is integrated in the SafeGuard Policy Editor as a Recovery Wizard.

21.1 Benefits of Challenge/Response

The challenge/response mechanism is a secure and efficient recovery system to fall back on.

- No confidential data is exchanged in unencrypted form throughout the entire process.
- There is no point in third parties eavesdropping on this procedure because the data they spy out cannot be used at any later point in time or on any other devices.
- The user can start working again quickly. No encrypted data is lost only because the password has been forgotten.

21.2 Typical situations for requiring help desk assistance

- A user has forgotten the password at POA level and the computer has been locked.

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 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. For further information, see [Recovery via Local Self Help](#), page 113.

- The Power-on Authentication local cache is partly damaged.

Sophos SafeGuard offers different recovery workflows for these typical scenarios enabling the users to access their computers again.

21.3 Challenge/Response workflow

The Challenge/Response procedure is based on two components:

- The endpoint computer on which the Challenge code will be generated.
- The SafeGuard Policy Editor where, as a help desk officer with sufficient rights, you will create a response code that will authorize the user to perform the requested action on their computer.

1. On the endpoint computer, the user requests the challenge code. Depending on the recovery type, this is either requested in the Power-on Authentication or via the KeyRecovery Tool.

A challenge code in form of an ASCII character string will be generated and displayed.

2. The user contacts the help desk and provides the necessary identification as well as the challenge code to the help desk.
3. The help desk launches the Recovery Wizard in the SafeGuard Policy Editor.
4. The help desk selects the appropriate recovery type, confirms the identification information and the challenge code and selects the required recovery action.

A response code in form of an ASCII character string will be generated and displayed.

5. The help desk provides the user with the response code e.g. via phone or text message.
6. The user enters the response code. Depending on the recovery type, this is either done in the POA or via the KeyRecovery Tool.

The user is then permitted to perform the authorized action, for example resetting the password and may resume working.

21.4 Launching the Recovery Wizard

To be able to perform a recovery procedure, make sure you have the required rights and permissions.

1. Log on to the SafeGuard Policy Editor.
2. Click **Tools > Recovery** in the menu bar.

The SafeGuard Recovery Wizard is started. You can select which type of recovery is requested.

21.5 Recovery types

Select which type of recovery you want to use. The following recovery types are provided:

■ Challenge/Response for Sophos SafeGuard Client

Sophos SafeGuard provides Challenge/Response when the user has forgotten their password or entered the password incorrectly too often.

Note: Also see the logon recovery method Local Self Help that does not require any help desk assistance.

■ Challenge/Response using Virtual Clients

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.

21.6 Challenge/Response for Sophos SafeGuard client

Sophos SafeGuard provides Challenge/Response e.g. when the user has forgotten the password or entered the password incorrectly too often. Recovery information needed for a Challenge/Response is in this case based on the key recovery file. On each Sophos SafeGuard endpoint computer this key recovery file is generated during Sophos SafeGuard deployment.

If this key recovery file is accessible to the Sophos SafeGuard help desk, e.g. via a shared network path, Challenge/Response for a Sophos SafeGuard protected computer may be provided.

To facilitate searching and grouping of the key recovery files, the files will carry the name of the computer: `computername.GUID.xml` in their file name. This allows for wild card search with asterisks (*), for example: `*.GUID.xml`.

Note: When a computer is renamed, it will not be renamed accordingly in the computer's local cache. The local cache stores all keys, policies, user certificates and audit files. The new computer name therefore has to be removed from the local cache so that only the previous name will remain, even if a computer is renamed under Windows.

21.6.1 POA recovery actions

Challenge/Response for an endpoint computer must be initiated in the following situations:

- The user has entered the password incorrectly too often at POA level and the computer has been locked.
- The user has forgotten the password.
- A corrupted local cache needs to be repaired.

For a Sophos SafeGuard protected computer only the defined machine key, but no user key is available in the database. Therefore, the only recovery action possible in a Challenge/Response session is **Booting SGN client without user logon**.

The Challenge/Response procedure will enable the computer to boot through Power-on Authentication. The user will then be able to log on to Windows.

Potential recovery use cases:

The user has entered the password incorrectly too often at POA level and the computer has been locked.

The computer is locked, and the user is prompted to initiate a Challenge/Response procedure to unlock the computer. As in this case resetting the password is not needed as the user still remembers the current password, Challenge/Response procedure will enable the computer to boot through Power-on Authentication. The user can then enter the correct password at Windows level and use the computer again.

The user has forgotten the password.

Note: We recommend to primarily using 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. For further information, see [Recovery via Local Self Help](#), page 113.

When recovering a forgotten password via Challenge/Response a password reset is required.

1. The Challenge/Response procedure will enable the computer to boot through Power-on Authentication.
2. 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.

3. 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.
4. 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.
5. 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**.
6. 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.
7. 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.

Keys for SafeGuard Data Exchange

When the user has forgotten the Windows password and has to enter a new one, a new user certificate is created as well. Therefore, the user will not be able to use the keys already created for SafeGuard Data Exchange any longer. To be able to continue using the already generated user keys for SafeGuard Data Exchanges the user has to remember the SafeGuard Data Exchange passphrases to reactivate these keys.

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

The local cache needs to be repaired

The local cache stores all keys, policies, user certificates and audit files. By default, logon recovery is deactivated when the local cache is corrupted, i.e. it will be restored automatically from its backup. In this case, no Challenge/Response procedure is required for repairing the local cache. However, logon recovery can be activated by policy, if the local cache is to be repaired explicitly via a Challenge/Response procedure. In this case, the user is prompted automatically to initiate a Challenge/Response procedure, if the local cache is corrupted.

21.6.2 Generating a response using the key recovery file

The key recovery file generated during installation of the Sophos SafeGuard encryption software needs to be stored in a location a help desk officer is able to access and the name of the file must be known.

To generate a response, do the following:

1. In the SafeGuard Policy Editor, select **Tools > Recovery** from the menu bar to open the Recovery Wizard.
2. In **Recovery type**, select **Sophos SafeGuard Client**.
3. Locate the required key recovery file by clicking **Browse**. For better identification the recovery files carry the name of the computer: `computername.GUID.xml`.
4. Enter the challenge code the user has passed on to you and click **Next**. The challenge code is verified.

If the challenge code has been entered correctly, the recovery action requested by the Sophos SafeGuard computer as well as the possible recovery actions are displayed. If the code has been entered incorrectly, **Invalid** is displayed below the block containing the error.

5. Select the required action to be taken by the user and click **Next**.
6. A response code is generated. Communicate the response code to the user. A spelling aid is provided. You may also copy the response code to the clipboard.

The user can enter the response code, perform the requested action and resume working.

21.7 Challenge/Response using Virtual Clients

When using Virtual Clients Sophos SafeGuard offers recovery of encrypted volumes even in complex disaster situations. e.g. when the POA is corrupted. Challenge/Response using Virtual Clients is based on the following:

- **Key Recovery file**

It is created during Sophos SafeGuard encryption configuration and contains the encryption key for the endpoint computer. This key recovery file is generated for each Sophos SafeGuard protected computer and contains the defined machine key which is encrypted with the company certificate. It needs to be accessible to the help desk, e.g. on a memory stick or via a shared network path.

- **Virtual Client file**

Specific files called Virtual Clients that are created in the SafeGuard Policy Editor and are used as reference information in the database.

- **Sophos SafeGuard modified Windows PE recovery disk**

The recovery disk is used for booting the endpoint computer from BIOS.

- **KeyRecovery Tool**

The tool is used to start the Challenge/Response procedure. It is already available on the Sophos SafeGuard modified Windows PE recovery disk. Additionally you will find it in the Tools directory of your Sophos SafeGuard software delivery.

21.7.1 Virtual Clients

Virtual Clients are specific encrypted key files that are used for recovering an encrypted volume when no reference information on the computer is available in the database and usually Challenge/Response would not be supported. The Virtual Client is used as identification and reference information during the Challenge/Response and is stored in the database.

To enable a Challenge/Response procedure in complex disaster situations, the Virtual Clients need to be created and distributed beforehand to the user prior to the Challenge/Response procedure. Access to the computer can then be regained with the help of these Virtual Clients, a KeyRecovery Tool and a SafeGuard modified Windows PE recovery disk available with your product.

21.7.2 Recovery workflow using Virtual Clients

To access the encrypted computer, the following general workflow applies:

1. Obtain the Sophos SafeGuard recovery disk from technical support.
 2. 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>.
 3. Create the Virtual Client in the SafeGuard Policy Editor.
 4. Export the Virtual Client to a file.
 5. Boot the computer from the recovery disk.
 6. Import the Virtual Client file into the KeyRecovery Tool.
 7. Initiate the Challenge in the KeyRecovery Tool.
 8. Confirm the Virtual Client in the SafeGuard Policy Editor.
 9. Select the required recovery action.
 10. Enter the challenge code in the SafeGuard Policy Editor.
 11. Generate the response code in the SafeGuard Policy Editor.
 12. Enter the response code into the KeyRecovery tool.
- The computer can be accessed again.

21.7.3 Creating a Virtual Client

Virtual Clients are specific encrypted key files that can be used for recovery in a Challenge/Response procedure as reference information on the computer.

Virtual Client files can be used by different computers and for several Challenge/Response sessions.

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.

The new Virtual Client is displayed in the action area. Next you export it to a file.

21.7.4 Exporting a Virtual Client

Virtual Clients need to be exported to files in order to distribute them to the endpoint computers and use them for recovery. These files are always called recoverytoken.tok.

1. In the SafeGuard Policy Editor, select the **Virtual Clients** area.
2. In the left-hand navigation window, click **Virtual Clients**.
3. In the action area search for the respective Virtual Client by clicking the magnifier icon. The available Virtual Clients are displayed.
4. Select the respective entry in the action area and click **Export Virtual Client** in the toolbar.
5. Select a storage location for the Virtual Client file recoverytoken.tok and confirm with **OK**.
Choose a safe place to store the file.

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

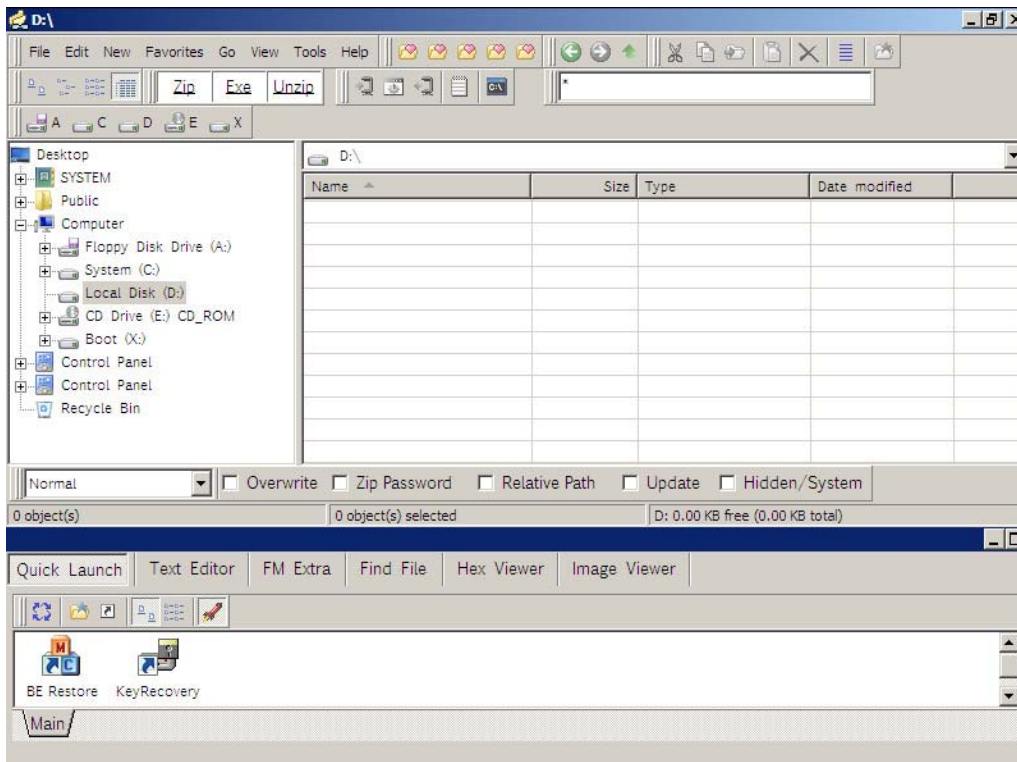
6. Copy the Virtual Client file recoverytoken.tok to a removable medium. We recommend using a memory stick.

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

21.7.5 Booting the computer from the recovery disk

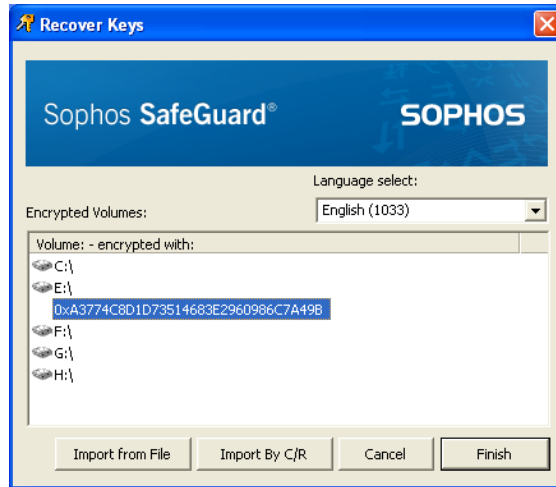
Make sure that the boot sequence in the BIOS settings allows booting from CD.

1. On the endpoint computer, insert the recovery disk and start the computer. The integrated file manager opens. At a glance, you can see the mounted volumes and drives.



The contents of the encrypted drive are not visible in the file manager. Neither the file system, nor the capacity and used/free space are indicated in the properties of the encrypted drive.

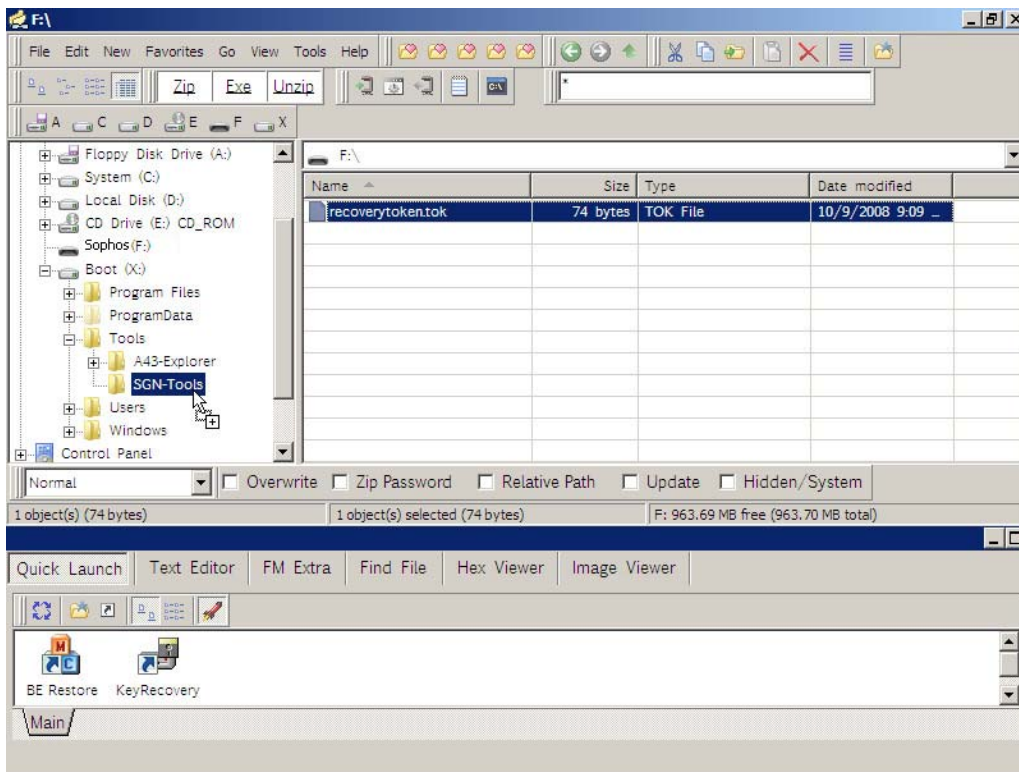
2. At the bottom of the file manager in section **Quick Launch**, click the KeyRecovery icon to open the KeyRecovery Tool. The Key Recovery Tool displays the key ID of the encrypted drives.



3. Find the key ID of the drives that you need to access. The key ID will be requested later on.
Next import the Virtual Client into the Key Recovery Tool.

21.7.6 Importing the Virtual Client into the KeyRecovery Tool

- The computer has been booted from the recovery disk.
 - Ensure that the USB drive with the Virtual Client file recoverytoken.tok stored on it has been mounted successfully.
1. In the Windows PE file manager select the drive on which the Virtual Client is stored. The file recoverytoken.tok will be displayed on the right.
 2. Select the file recoverytoken.tok and drag it to the drive in which the KeyRecovery Tool is located. There, drop it into the Tools\SGN-Tools directory.



21.7.7 Initiating the Challenge in the KeyRecovery Tool

1. At the bottom of the Windows PE file manager in section **Quick Launch**, click the KeyRecovery icon to open the KeyRecovery Tool. The Key Recovery Tool displays the key ID of the encrypted drives.

The tool is started displaying a list of all volumes and their corresponding encryption information (key ID).



2. Select the volume you want to decrypt and click Import by C/R to generate the Challenge Code.

As reference in the Sophos SafeGuard database the Virtual Client file is used and stated in the challenge. The Challenge code is generated and displayed.

3. Communicate the Virtual Client name and the challenge code to the help desk, e.g. via phone or text message. A spelling aid is provided.

21.7.8 Generating a Response using Virtual Clients

To access a Sophos SafeGuard protected computer and to generate a Response using Virtual Clients two actions are required:

1. Confirm the Virtual Client in the SafeGuard Policy Editor database.
2. Select the requested recovery action. As only the key recovery file is available for decryption, this file needs to be selected so that a Response code can be generated.

21.7.8.1 Confirming the Virtual Client

Prerequisite:

The Virtual Client must have been created in the SafeGuard Policy Editor in **Virtual Clients** and must be available in the database.

1. In the SafeGuard Policy Editor click **Tools > Recovery** to open the Recovery Wizard.
2. In **Recovery type** select **Virtual Client**.
3. Enter the name of the Virtual Client the user has given to you. There are different ways to do so:
 - Enter the unique name directly.
 - Select a name by clicking [...] in the **Virtual Client** section of the **Recovery type** dialog. Then click **Find now**. A list of Virtual Clients is displayed. Select the required Virtual Client and click **OK**. The Virtual Client name is then displayed in the **Recovery type** window below **Virtual Client**.
4. Click **Next** to confirm the name of the Virtual Client file.

Next select the requested recovery action.

21.7.8.2 Selecting the key recovery file

Prerequisite:

You must have selected the required Virtual Client in the SafeGuard Policy Editor Recovery Wizard.

The required key recovery file needed to regain access to the computer must be accessible to the help desk, e.g. on a network share.

1. In the Recovery wizard, in Virtual Client, select the requested recovery action **Key requested** and click **Next**.
2. Activate **Select key recovery file containing recovery key**.
3. Click [...] next to this option to browse for the respective file. For better identification the recovery files carry the name of the computer: computername.GUID.xml.
4. Confirm with **Next**. The window for entering the challenge code is displayed.

5. Enter the challenge code the user has passed on to you and click **Next**. The challenge code is verified.

If the challenge code has been entered correctly, the response code is generated. If the code has been entered incorrectly, **Invalid** is displayed below the block containing the error.

6. Pass the response code on to the user. A spelling aid is provided. You can also copy the response code to the clipboard.

21.7.9 Entering the Response code in the KeyRecovery Tool

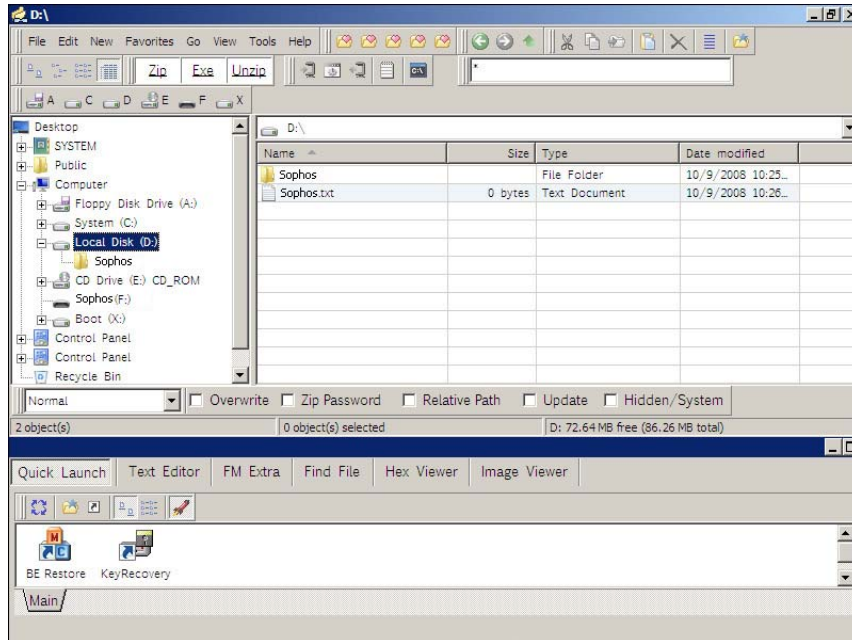
1. In the KeyRecovery Tool on the endpoint computer, enter the response code the help desk has given to you.

Within the response code the required recovery key is transported.

2. Click OK. The drive selected for Challenge/Response has been decrypted.



3. To ensure that description has been successful, select the decrypted drive in the Windows PE file manager:



The contents of the decrypted drive are now displayed in the file manager. The file system as well as the capacity and used/free space are now indicated in the properties of the decrypted drive.

Access to the data stored on this partition is recovered. As a result of the successful decryption you can read, write and copy data from and/or to the respective drive.

21.7.10 Deleting Virtual Clients

Virtual Clients that are no longer needed may be deleted from the Sophos SafeGuard Database.

1. In the SafeGuard Policy Editor, select the **Virtual Clients** area.
2. In the left-hand navigation window, click **Virtual Clients**.
3. In the action area on the right click the magnifier icon to search for the respective Virtual Client. The available Virtual Clients are displayed.
4. Select the required entry and click **Delete Virtual Client** in the toolbar.
5. Click the **Save** icon in the toolbar to save your changes to the database.

The Virtual Client is deleted from the database and can no longer be used in a Challenge/Response procedure.

22 System Recovery

Sophos SafeGuard encrypts files and drives transparently. Boot drives can also be encrypted, so decryption functionalities such as code, encryption algorithms and encryption key must be available very early in the boot phase. Therefore encrypted information cannot be accessed if the crucial Sophos SafeGuard modules are unavailable or do not work.

The following sections cover possible error sources and recovery methods.

22.1 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 a 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.

22.2 Corrupted MBR

For resolving problems with a corrupted MBR Sophos SafeGuard offers the tool BE_Restore.exe.

For a detailed description on how to restore a corrupted MBR with this tool refer to the SafeGuard Tools Guide.

22.3 Volumes

Sophos SafeGuard provides drive-based encryption. This includes saving encryption information consisting of the boot sector, primary and backup KSA and the original boot sector on each drive itself.

As soon as one of the below units is damaged, the volume cannot be accessed any longer:

- either of the two Key Storage Areas (KSA)
- Original MBR

22.3.1 Boot sector

During the encryption process a volume's boot sector is swapped for the Sophos SafeGuard boot sector.

The Sophos SafeGuard boot sector holds information about

- the location of the primary and backup KSA in clusters and sectors in relation to the start of the partition
- the size of the KSA

Even if the Sophos SafeGuard boot sector is damaged, encrypted volumes cannot be accessed.

The tool BE_Restore can restore the damaged boot sector. For a detailed description of this tool refer to the SafeGuard Tools Guide

22.3.2 Original boot sector

The original boot sector is the one that is run after the DEK (Data Encryption Key) has been decrypted and the algorithm and the key have been loaded to the BE filter driver.

If this boot sector is defective, Windows is unable to access the volume. Normally the common error message “Device is not formatted. Would you like to format it now? Yes/No” is displayed.

Nonetheless, Sophos SafeGuard will load the DEK for this volume. A tool that is used to repair the boot sector needs to be compatible with the Sophos SafeGuard Upper Volume Filter.

22.4 Setting up WinPE for Sophos SafeGuard

To get access to encrypted drives with a computer's BOOTKEY within a WinPE environment, Sophos SafeGuard offers WinPE with the required Sophos SafeGuard function modules and drivers. To start SetupWinPE for WinPE enter the following command:

```
SetupWinPE -pe2 <WinPE image file>
```

WinPE image file being the full path name of a WinPE image file

SetupWinPE makes all the changes needed.

Note: Note that, with this type of WinPE environment, only encrypted drives that are encrypted with the BOOTKEY can be accessed.

23 Preventing uninstallation from the endpoint computers

To provide extra protection for endpoint computers you can prevent local uninstallation of Sophos SafeGuard via a policy of type **Machine specific settings**. To prevent local uninstallation, set the **Uninstallation allowed** option in a **Machine specific settings** policy to **No** and deploy the policy to the endpoint computers. If this kind of policy applies to the endpoint computer, uninstallation attempts will be cancelled and the unauthorized attempt will be logged.

Note: If you use a demo version, you should not activate this policy setting or in any case deactivate it prior to expiry of the demo version to ensure easy uninstallation.

23.1 Sophos Tamper Protection

Sophos Tamper protection prevents casual removal of Sophos SafeGuard, if the option **Uninstallation allowed** in the **Machine specific settings** policy that applies to the endpoint computer is set to **Yes** or **not configured**.

Note: Sophos Tamper Protection only applies to endpoint computers using Sophos Endpoint Security and Control version 9.5 or higher.

You can activate Sophos Tamper protection in a policy of the type **Machine specific settings**. If the **Uninstallation allowed** option in this policy is set to **Yes** or not configured, the option **Enable Sophos Tamper Protection** becomes available for selection.

If you set **Enable Sophos Tamper Protection** to **Yes**, any uninstallation attempt will be explicitly checked by Sophos Tamper Protection. If Sophos Tamper Protection does not allow uninstallation, the process will be canceled.

If you set **Enable Sophos Tamper Protection** to **No**, uninstallation of Sophos SafeGuard will not be prevented.

If **Enable Sophos Tamper Protection** is set to **not configured**, the default value **Yes** applies.

24 Updating Sophos SafeGuard

An update of Sophos SafeGuard comprises the following components which must be carried out in the order mentioned:

1. Sophos SafeGuard Database
2. SafeGuard Policy Editor
3. Sophos SafeGuard protected computer

Sophos SafeGuard 5.50 will update directly from SafeGuard Enterprise standalone 5.35 or higher without changing any settings that were previously set up. If you want to update from older versions you first have to update to version 5.40.

24.1 Updating the database

Prerequisites

- There must be a Sophos SafeGuard Database version 5.35 or higher installed (former product name up to version 5.40: SafeGuard Enterprise standalone). Older versions must first be updated to version 5.40.
- The SQL scripts that are to be run must be present on the database computer.
- .NET Framework 3.0 Service Pack 1 must be installed for successfully updating to the latest version
- You need Windows administrator rights.
- Back up the database before starting the update.

In the Tools directory of your software delivery several SQL scripts are provided for updating the database

To update the database, do the following:

1. Close the SafeGuard Policy Editor.
2. Set the relevant database to SINGLE_USER mode for running the SQL scripts.

3. The database must be converted version by version to the current version. Depending on the version installed, start the following SQL scripts in sequence:
 - a) 5.35 > 5.40: Run MigrateSGN535_SGN540.sql
 - b) 5.4x > 5.50: Run MigrateSGN540_SGN550.sql
4. Set the relevant database to MULTI_ USER mode again.

After updating the database the cryptographic check sums of some tables might no longer be correct. When starting the SafeGuard Policy Editor warning messages will be displayed accordingly. You can repair the tables in the relevant dialog.

The latest version of the Sophos SafeGuard database is then ready for use.

24.2 Updating SafeGuard Policy Editor

Prerequisites

- There must be a SafeGuard Policy Editor version 5.35 or higher installed. Older versions must first be updated to version 5.40.
- The SafeGuard Policy Editor does not need to be uninstalled.
- The Sophos SafeGuard database has already been updated to the latest version.
- .NET Framework 3.0 Service Pack 1 must be installed for successfully updating to the latest version. You may download it for free from <http://www.microsoft.com/downloads>.
- ASP.NET must be converted to version 2.0.
- You need Windows administrator rights.

Do the following:

1. Install the latest version of the SafeGuard Policy Editor installation package. You do not need to run the Configuration Wizard again.

The SafeGuard Policy Editor has been updated to the latest version.

24.3 Updating Sophos SafeGuard protected computers

SafeGuard Policy Editor version 5.5x can manage Sophos SafeGuard protected computers version 5.35 or higher.

Prerequisites

- Version 5.35 or higher of the Sophos SafeGuard “Client” installation package must be installed. Older versions must first be updated to version 5.40.
- The Sophos SafeGuard database and the SafeGuard Policy Editor have already been updated to the latest version.
- You need Windows administrator rights.

Do the following:

1. Install the preparatory MSI package SGxClientPreinstall.msi that provides the endpoint computer with the necessary requirements for a successful installation of the current encryption software, for example the required DLLs.

Note: Alternatively, you may install vcredist_x86.exe that you can download from here: <http://www.microsoft.com/downloads/details.aspx?FamilyID=766a6af7-ec73-40ff-b072-9112bab119c2> or check that MSVCR80.dll, version 8.0.50727.4053 is present in the Windows\WinSxS folder on the computer.

2. Install the latest version of the respective Client installation package afresh.

Windows Installer recognizes the modules that are already installed and only installs these modules afresh. If Power-on Authentication is installed, an updated POA kernel will also be available after a successful update (policies, keys etc.). Sophos SafeGuard will be automatically restarted on the computer.

- If the Sophos SafeGuard configuration has not changed, you do not need to create and install a new Sophos SafeGuard configuration package. For security reasons however, we recommend that you delete all outdated or unused configuration packages.
- You only need to create and reinstall a new Sophos SafeGuard configuration package if there have been changes to the configuration, for example when the policy settings have changed. If you do create a new Sophos SafeGuard configuration package, ensure to delete the outdated one.

Note: If you try to install an older Sophos SafeGuard configuration package over a newer one, the installation is aborted and an error message is displayed.

24.4 Enhancing Sophos SafeGuard with volume based encryption

Note: This description is not applicable to Sophos SafeGuard with the ESDP (Endpoint Security and Data Protection).

If you want to enhance a Sophos SafeGuard protected computer on which only the SafeGuard Data Exchange module with file based encryption is installed to a Sophos SafeGuard Client with volume based encryption and SafeGuard Data Exchange with file based encryption you need to carry out the following steps. These steps are necessary to ensure a secure and correct authentication at the Power-on Authentication.

1. Uninstall the SafeGuard Data Exchange installation package (SGNClient_withoutDE.msi/SGNClient_withoutDE_x64.msi).
2. Uninstall the Sophos SafeGuard configuration package.
3. Install the Sophos SafeGuard Device Encryption package with volume based encryption selecting the features Device Encryption and Data Exchange (SGNClient.msi/SGNClient_x64.msi).
4. Generate and install a new Sophos SafeGuard configuration package on the computer.

The key recovery file as well as the local keys created during the installation of the Data Exchange package will not be deleted but will still be available.

25 Upgrading Sophos SafeGuard 5.5x to SafeGuard Enterprise

You can easily upgrade Sophos SafeGuard 5.5.x to the SafeGuard Enterprise suite with central management to make use of the full functionality of SafeGuard Enterprise.

For this purpose, the following steps must be taken:

- The SafeGuard Policy Editor must be upgraded to the SafeGuard Management Center.
- The Sophos SafeGuard encrypted endpoint computers must be upgraded to SafeGuard Enterprise protected computers.

25.1 Upgrading SafeGuard Policy Editor to SafeGuard Management Center

You can upgrade the SafeGuard Policy Editor to the SafeGuard Management Center to use comprehensive management features, e.g. user and computer management, as well as logging.

Prerequisites

- You do not have to uninstall SafeGuard Policy Editor.
- Set up the SafeGuard Enterprise Server prior to migration.

Upgrading SafeGuard Policy Editor

To upgrade, simply install the SGNManagementCenter.msi package on the computer, on which the SafeGuard Policy Editor has been set up.

1. Start SGNManagementCenter.msi from the installation folder of your product delivery.
2. Click **Next** in the welcome window.
3. Accept the license agreement.
4. Select an installation path.
5. Confirm that the installation has completed successfully.
6. If necessary, restart your computer.
7. Configure the SafeGuard Management Center.

The SafeGuard Policy Editor has been upgraded to the SafeGuard Management Center.

25.2 Upgrading Sophos SafeGuard configurations to SafeGuard Enterprise

You can upgrade a Sophos SafeGuard configuration of an endpoint computer to a SafeGuard Enterprise configuration. In this way, the computers are defined in the SafeGuard Management Center as objects which can be managed and which have a connection to the SafeGuard Enterprise Server.

Note: The reverse procedure, i.e. downgrading a SafeGuard Enterprise configuration to a Sophos SafeGuard configuration, is not advisable. To do this, you would have to completely reinstall Sophos SafeGuard encryption software on to the endpoint computer.

Prerequisites

- SafeGuard Policy Editor has been upgraded to the SafeGuard Management Center.
- Sophos SafeGuard encryption software on the endpoint computer does not have to be uninstalled.
- Ensure to backup the endpoint computer before starting the upgrade.
- You need Windows administrator rights.

Upgrading Sophos SafeGuard configurations to SafeGuard Enterprise.

To upgrade you only have to create a different configuration package in the SafeGuard Management Center and deploy it to the respective computers.

1. Create the configuration package for the managed SafeGuard Enterprise Client in the SafeGuard Management Center via **Tools > Configuration Package Tool > Create Configuration Package (managed)**.
2. Assign this package to the Sophos SafeGuard computers, via a group policy.
During upgrade all users and certificates will be deleted and the Power-on Authentication will be disabled as the user-computer assignment is not upgraded. After the upgrade, the endpoint computers are therefore unprotected!
3. Reboot twice after upgrading: The first logon is still done via Autologon. New keys and certificates are assigned to the user. Thus users can only log on at the Power-on Authentication when rebooting for the second time. Only after the second reboot the computers are protected again.

The Sophos SafeGuard configuration on the endpoint computer is now a SafeGuard Enterprise configuration.

26 Upgrading SafeGuard Easy 4.x/ Sophos SafeGuard Disk Encryption 4.x to Sophos SafeGuard 5.5x

SafeGuard Easy 4.5x as well as Sophos SafeGuard Disk Encryption 4.60 can be directly upgraded to Sophos SafeGuard 5.50 by simply installing the SafeGuard Device Encryption Client installation package on the computer.

Direct upgrade has been tested and is supported for SafeGuard Easy 4.5x. A direct upgrade should also work for versions between 4.3x and 4.4x. Direct upgrade for versions older than 4.3x is not supported, they must be updated to SafeGuard Easy 4.50 beforehand.

Hard drive encryption is being maintained, so there is no need to decrypt and re-encrypt them. It is not necessary either to uninstall SafeGuard Easy or Sophos SafeGuard Disk Encryption.

This chapter describes how to upgrade to Sophos SafeGuard and explains which features can be migrated and details the limitations.

26.1 Prerequisites

The following prerequisites must be met:

- Direct upgrade has been tested and is supported for SafeGuard Easy 4.5x. A direct upgrade should also work for versions between 4.3x and 4.4x. Direct upgrade for versions older than 4.3x is not supported, they must be updated to SafeGuard Easy 4.50 beforehand.
- Direct upgrade is supported for Sophos SafeGuard Disk Encryption version 4.6x.
- SafeGuard Easy /Sophos Safeguard Disk Encryption must be running on the following operating system:
 - Windows XP Professional Workstation Service Pack 2, 3
- Windows Installer Version 3.01 or higher has to be installed.
- The hardware must meet the system requirements for Sophos SafeGuard 5.50.
- When using special software (for example Lenovo middleware) it must meet the system requirements for Sophos SafeGuard 5.50.
- Upgrading may only take place if the hard disks are encrypted with the following algorithms: AES128, AES256, 3DES, IDEA.

26.1.1 Limitations

The upgrade is subject to the following limitations:

- Only the SafeGuard Device Encryption installation package with the standard features can be installed (SGNClient.msi/SDEClient.msi). If the module SafeGuard Data Exchange is to be installed in addition, this has to be done in a separate step. (Note that SafeGuard Data Exchange is not supported with ESDP).
- The installation package without volume based encryption (SGNClient_withoutDE.msi) is not supported for upgrading to Sophos SafeGuard.
- The following installations cannot be upgraded to Sophos SafeGuard and installing Sophos SafeGuard should not be attempted.

Note: If you start a upgrade in the cases mentioned below, an error message will be displayed. (error number 5006).

- Twin Boot installations
- Installations with active Compaq Switch
- Lenovo Computrace installations
- Hard disks that are partially encrypted, e.g. only have boot sector encryption
- Hard disks with hidden partitions
- Hard disks that have been encrypted with one of the following algorithms: XOR, STEALTH, DES, RIJNDAEL, Blowfish-8, Blowfish-16
- Multi-boot scenarios with a second Windows or Linux partition
- Removable media that have been encrypted with one of the following algorithms XOR, STEALTH, DES, RIJNDAEL, Blowfish-8, Blowfish-16 cannot be upgraded.

Note: There is a risk of data being lost if a removable device has been encrypted with one of the algorithms XOR, STEALTH, DES, RIJNDAEL, Blowfish-8, Blowfish-16. The data on the removable medium cannot be accessed with Sophos SafeGuard after upgrading!

- Removable media with Super Floppy volumes cannot be transformed after migration.
- Removable media can be converted to a Sophos SafeGuardcompatible format. After conversion, an encrypted data medium can only be read with Sophos SafeGuard and only at the one endpoint computer where it was converted.

Note: Removable media encryption and migration is not supported for ESDP.

26.2 Which functionality is upgraded

The table below shows which functionality is upgraded and how it is mapped in Sophos SafeGuard.

SafeGuard Easy/Sophos SafeGuard Disk Encryption	Upgrade	Sophos SafeGuard
Encrypted hard disks	Yes	The hard disk keys are protected by Sophos SafeGuard Power-on Authentication. So the hard disk key is at no time exposed. If "Boot Protection" mode has been selected in SafeGuard Easy, the current version has to be uninstalled. The hard disk's encryption algorithm is not changed by the upgrade. Therefore the actual algorithm for this type of upgraded hard disk may differ from the general Sophos SafeGuard policy.
Encrypted removable media (not applicable to Sophos SafeGuard Disk Encryption with ESDP)	Yes	Encrypted data media, e.g. USB memory sticks, can be converted to the Sophos SafeGuard format. Note: After conversion, an encrypted data medium can only be read with SafeGuard Enterprise and only at the one endpoint computer where it was converted. The conversion needs to be confirmed in each case.
Encryption algorithms	To some degree	The algorithms AES128, AES256, 3DES, IDEA can be migrated. AES-128 and 3-DES however, are not available for selection in the SafeGuard Policy Editor for media that is to be newly encrypted.
Challenge/Response	To some degree	The Challenge/Response procedure is maintained.
User names	No	As the Windows user names are used in Sophos SafeGuard, there is no need to reuse the SafeGuard Easy/Sophos SafeGuard Disk Encryption specific user names. So registering the upgraded computers is done in the same way as with a new Sophos SafeGuard installation: by centrally assigning or locally registering the computer's users. Note: After the upgrade the first user to log on to Windows will be set to be the primary user within the POA (unless they are specified on the Service Account list).

SafeGuard Easy/Sophos SafeGuard Disk Encryption	Upgrade	Sophos SafeGuard
User passwords	No	As the Windows passwords are used in Sophos SafeGuard, there is no need to reuse the SafeGuard Easy/Sophos SafeGuard Disk Encryption specific passwords. SafeGuard Easy/Sophos SafeGuard Disk Encryption passwords will therefore not be upgraded.
Policies, settings (e.g. minimum password length)	No	To ensure that all the settings are consistent, no automatic upgrade is executed. The policies have to be reset in the SafeGuard Policy Editor.
Pre-Boot Authentication	No	Pre-Boot Authentication (PBA) is replaced by the Sophos SafeGuard Power-on Authentication (POA).
Installations without GINA	Yes	Installations without GINA are upgraded to Sophos SafeGuard with SGNGINA installed.
Token/Smartcards	No	Tokens/smartcard authentication is not supported with Sophos SafeGuard. If you would like to use token/smartcards, we recommend migrating to SafeGuard Enterprise.
Logon with Lenovo Fingerprint Reader	To some degree Note: Fingerprint logon is not available with ESDP.	Fingerprint logon can continue to be used in Sophos SafeGuard. The fingerprint reader hardware and software has to be supported by Sophos SafeGuard and the fingerprint user data have to be rolled out again. For further information on fingerprint logon refer to the user help.

26.3 Preparing for upgrade

The following measures should be taken before starting the installation of Sophos SafeGuard:

- Before upgrading the endpoints, prepare a Sophos SafeGuard configuration package using SafeGuard Policy Editor. After the encryption software has been installed on the endpoints, deploy the configuration package to the endpoints. The policies transferred with the first configuration package should correspond to the previous configuration of the SafeGuard Easy/Sophos SafeGuard Disk Encryption computer.

If no configuration package is installed with the upgrade, all drives that were encrypted with SafeGuard Easy/Sophos SafeGuard Disk Encryption will stay encrypted.

- To reduce the risk of data loss, we recommend that you create a full backup of the computers that are to be upgraded.

Perform the steps that are recommended prior to a Sophos SafeGuard installation, e.g. use “chkdsk” and “defrag”. For further information see [Preparing for installation](#), page 14. For further information on “chkdsk” and “defrag” see our knowledgebase:

- chdsk: <http://www.sophos.com/support/knowledgebase/article/108088.html>
- defrag: <http://www.sophos.de/support/knowledgebase/article/109226.html>
- We recommend that you create a valid kernel backup and save this backup in a location that can always be accessed, e.g. a network path. For further information see your SafeGuard Easy 4.5x/Sophos SafeGuard Disk Encryption 4.60 manuals/help, chapter *Saving the system kernel and creating emergency media*.
- To reduce the risk of data loss, we recommend that you create a test environment for the first upgrade.
- When upgrading from older versions of SafeGuard Easy, first upgrade to version 4.50.
- Leave the computers switched on throughout the upgrade process.
- The security officer should keep the users' Windows credentials at hand in case users have forgotten their Windows passwords after migration. This can happen if users have previously logged on to the Pre-Boot Authentication and have later been logged on via Windows Secure Autologon (SAL). So users never used their Windows credentials.

Note: Users need to know their password for Windows logon before upgrading. This is essential as a Windows password cannot be subsequently set after upgrade and installation of Sophos SafeGuard. If users do not know their Windows password because they have used Secure Automatic Logon in SafeGuard Easy/Sophos Disk Encryption, they will not be able to log on to Sophos SafeGuard. In this case pass-through to Windows is rejected and users will not be able to log on to Sophos SafeGuard. Thus, there is the risk of data loss as users will not be able to access their computers anymore.

26.4 Starting the upgrade

Note: The installation can be carried out on a running SafeGuard Easy /Sophos SafeGuard Disk Encryption system. No decryption of encrypted hard drives or volumes is necessary.

Note: Use the SafeGuard Device Encryption Client package (SGNClient.msi/SDEClient.msi) from the installation folder with the standard feature set. The client package SGNClient_withoutDE.msi cannot be used for upgrading. For a successful upgrade the installation should best be performed centrally in unattended mode. Installation via the setup folder is not recommended!

Do the following:

1. Double-click WIZLDR.exe from the SafeGuard Easy/Sophos SafeGuard Disk Encryption program folder of the endpoint computer that is to be upgraded. This will start the Migration Wizard.
2. In the Migration Wizard, enter the SYSTEM password and confirm with **Next**. In **Destination folder**, confirm the default with **Next** and click **Finish** to complete the action. A migration configuration file SGEMIG.cfg will be created.

3. In the Windows Explorer, rename this file from SGEMIG.cfg to SGE2SGN.cfg.

Note: Owner/creator rights have to be set for this file and the file path where it is stored during the upgrade. Otherwise, the upgrade may fail and a message stating that SGE2SGN.cfg cannot be found will be displayed.

4. Enter the “msiexec” command at the command prompt to install the Sophos SafeGuard preinstallation package as well as the “Client” installation package on the SafeGuard Easy/Sophos SafeGuard Disk Encryption endpoint. Add the parameter MIGFILE stating the file path of the migration configuration file SGE2SGN.cfg:

Example:

```
msiexec /i \\Distributionserver\Software\Sophos\SafeGuard\SGxClientPreinstall.msi
```

```
msiexec /i \\Distributionserver\Software\Sophos\SafeGuard\SDEClient.msi
```

```
/L*VX“\\Distributionserver\Software\Sophos\SafeGuard\%Computername%.log“
```

```
MIGFILE=\\Distributionserver\Software\Sophos\SafeGuard\SGE2SGN.cfg
```

- If the upgrade is successful, Sophos SafeGuard can be used on the computer.
- If the upgrade fails, SafeGuard Easy/Sophos SafeGuard Disk Encryption can still be used on the computer. In such cases, Sophos SafeGuard is automatically removed.

26.5 Configuring the upgraded endpoint computers

The endpoint computers are initially configured by configuration packages which, among other aspects, activate the Power-on Authentication.

Therefore, during the upgrade, first the preinstallation package and Sophos SafeGuard installation package containing the encryption software should be installed. Only after the POA has been activated and the user has logged on successfully to Windows, endpoint configuration should take place.

1. Create the initial configuration package in the SafeGuard Policy Editor via **Tools > Configuration Package Tool** with the required policy settings.
2. Install the configuration package on the endpoint computers.

Note: The policies transferred with the first Sophos SafeGuard configuration package have to correspond to the previous configuration of the SafeGuard Easy/Sophos SafeGuard Disk Encryption computer.

26.6 After the upgrade

After successful upgrade the following is available in Sophos SafeGuard after logging on to the Power-on Authentication:

- the keys and algorithms of encrypted volumes.
- the keys and algorithms for encrypted removable media (applicable only when upgrading from SafeGuard Easy).

Encrypted volumes remain encrypted and the encryption keys are automatically converted to a Sophos SafeGuard compatible format.

Note: To be able to decrypt the hard disk or add and remove keys for hard disk encryption the user first needs to restart the computer.

Policies should be reset in the SafeGuard Policy Editor to correspond to the previous configuration of the SafeGuard Easy/Sophos SafeGuard Disk Encryption computer.

26.6.1 Removable media migration

Note: Removable media migration is not applicable to Sophos SafeGuard Disk Encryption with ESDP.

Encrypted removable media remain encrypted as well, but the keys have to be converted to a format that is compatible with Sophos SafeGuard.

Note: Therefore, after conversion, an encrypted data medium can only be read with SafeGuard Enterprise and only at the one endpoint computer where it was converted during migration!

To be able to decrypt removable media or add and remove keys for removable media encryption the user first needs to detach the media from the computer and reinsert it again.

When accessing removable media after migration, the user needs to actively confirm the transformation of the encryption keys into a Sophos SafeGuard compatible format. The appropriate policy for volume based encryption has to be present on the computer before conversion. Otherwise the keys will not be converted.

The user is prompted to confirm the conversion for any removable media. An appropriate message is displayed.

- If the user confirms the conversion, full access to the migrated data is possible.
- If the user rejects the conversion, the migrated data can still be opened for reading and writing.

Newly added removable media are encrypted, as with any Sophos SafeGuard computer, if the appropriate policy configuration is present on the endpoint computer.

27 Technical support

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

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

28 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.