

Sophos SafeGuard Disk Encryption 4.60

startup guide

Document date: June 2009

Contents

1	About this guide	3
2	About disk encryption and Pre-Boot Authentication.....	3
3	How will encryption affect the way you manage the computer/network?	3
4	What are the key steps?	4
5	Check the system requirements	5
6	Carry out a trial installation	5
7	Assign administration rights	7
8	Install the administration tools	8
9	Configure the encryption software	8
10	Deploy the encryption software to end user computers.....	10
11	Recover a forgotten password	11
12	Recover access to the system	12
13	Get help with common tasks.....	12
14	Technical support	13
15	Copyright.....	13

1 About this guide

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

2 About disk encryption and Pre-Boot Authentication

Sophos SafeGuard Disk Encryption encrypts the entire contents of hard disks transparently. Users do not need to decide which data is to be encrypted and decryption takes place unnoticed.

Pre-Boot Authentication ensures that only a Sophos SafeGuard Disk Encryption user registered on a computer may log on to it. The keys required for encrypting and decrypting are calculated dynamically. They are encrypted and stored on the hard disk as well. These keys can only be used to start the operating system when the user logs on to the computer with the correct SDE credentials.

The benefits of Sophos SafeGuard Disk Encryption are:

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

3 How will encryption affect the way you manage the computer/network?

Note the following:

- You may generally use system management tools such as Microsoft SMS, Tivola, or NetInstall with Sophos SafeGuard Disk Encryption.
- Sophos SafeGuard Disk Encryption provides support for Lenovo Rescue and Recovery™. Imaging tools are not supported and not tested with Sophos SafeGuard Disk Encryption.
- Note that Sophos SafeGuard Disk Encryption needs to be specially configured for Wake-On-LAN. If you use Wake-On-LAN you will need to configure this capability via the **Advanced Settings**, see [Configure the encryption software](#) on page 8.
- You will need to set up a helpdesk for recovery in emergency cases. Sophos SafeGuard Disk Encryption provides user-friendly recovery in case the user has forgotten their password, see [Recover a forgotten password](#) on page 11.

You need to create a 'Helpdesk' user account with the right to change user settings. You can do this by using the **Advanced Settings** when you pre-configure the encryption software, see [Configure the encryption software](#) on page 8.

For detailed information see the Sophos SafeGuard Disk Encryption help and the following knowledgebase article: <http://www.sophos.com/support/knowledgebase/article/56457.html>.

- During installation you need to define an initial password for the default user (USER). End users will use this password to log on to Sophos SafeGuard Disk Encryption for the first time. They will then be prompted to change it when they first log on.
- Sophos SafeGuard Disk Encryption administration requires a specific SYSTEM password that you define during installation. Make a note of this password and keep it in a safe place, see [Install the administration tools](#) on page 8.
- To always be able to access the installation log file when you deploy the encryption software on the end user computers, ensure to save it to a UNC path on the network.

4 What are the key steps?

To protect your network, you configure SDE on the administrator's computer and deploy it to the end user computers. The key steps are:

- Check the system requirements.
- Carry out a trial installation
- Assign administration rights
- Install the administration tools
- Configure the encryption software
- Deploy the encryption software to end user computers

5 Check the system requirements

Hardware requirements

- Requires at least 25 MB free hard disk space. The minimum requirement is the same as that of the operating system in use.
- Supports a maximum of four hard disks per machine, and a maximum of eight partitions per hard disk.

Software requirements

The minimum requirements for supported 32 bit versions of the operating systems are as follows (tested service packs in brackets):

- Windows 2000 Professional Service Pack 4 (SP 4)
- Windows XP Home Edition Service Pack 2 (SP 3)
- Windows XP Professional Edition Service Pack 2 (SP 3)

Current service packs are recommended.

6 Carry out a trial installation

To get to know Sophos SafeGuard Disk Encryption, install the encryption software on a trial computer.

6.1 Prepare for installation

Before you start, you must:

- Close all open applications.
- Ensure that there is enough free hard disk space.
- Create a full data backup.
- Ensure partitions are fully formatted and a drive letter is assigned.
- Check hard disk(s) for errors with this command: `chkdsk %systemdrive% /F /V /L /X`
In some cases you might be prompted to restart the computer and run `chkdsk` again.

For further information see the following knowledgebase article:
<http://www.sophos.com/support/knowledgebase/article/57554.html>.

Note: If you want to install the software on a computer running in an Asian language (or any language that uses "double-byte" characters), read the release notes first.

6.2 Install the encryption software

1. Log on to your computer as an administrator.
2. Using the web address and download credentials provided by your system administrator, go to the Sophos website and download the standalone installer for your version of Windows.
3. Locate the installer in the folder where it was downloaded. Double-click the installer. In the installer window, click **Install** to extract the installer's contents to your computer and start the installation wizard. The **Sophos SafeGuard Disk Encryption Installer** guides you through the necessary steps.
4. Accept the default on the next dialogs.
5. In **Select Installation Type**, select **Encryption on this computer** and click **Next**.
6. In **Passwords** enter and confirm passwords for the two default SDE users: system user (the top-level administrator SYSTEM) and default user (USER).

Note: The password for the default user (USER) is the initial password that you are prompted to change at first logon to Sophos SafeGuard Disk Encryption.

Note: Make a note of the SYSTEM password and keep it in a safe place! If you lose it, you will not be able to access the computer any more in case of an emergency!

The default encryption and security settings (encryption of partition C: and activated Pre-Boot Authentication) are set automatically. To change the default settings, click **Show Advanced Settings** in **Passwords** and make your changes in the **Workstation Configuration** dialogs.
7. Accept the default on all further dialogs.

Installation is finished. Next you carry out post-installation tasks.

6.3 Carry out post-installation tasks

Do as follows:

1. Restart your computer. The Windows logon dialog is displayed.
2. Enter your Windows credentials.
Initial encryption will start automatically. This will take some time. You may continue working at your computer. The system kernel will be backed up automatically.
3. Restart the computer for a second time. The Sophos SafeGuard Disk Encryption Pre-Boot Authentication is displayed.
4. Enter the Sophos SafeGuard Disk Encryption user password defined during installation.
5. You are prompted to change this password.
6. You are prompted to enter your Windows credentials again.
7. Confirm to be automatically logged on to Windows. You are logged on to your computer.

Next time you start the computer you will only have to enter your SDE user password at the Pre-Boot Authentication and will be passed-through to Windows.

7 Assign administration rights

Before installation on your network, you should decide which user will have administration rights.

By default, installation will create two types of users:

- The **system user** (top-level administrator SYSTEM) has full rights to access and configure end user computers and to perform emergency tasks. Only the SYSTEM user can grant rights to other users.

Note: Only the system user should know the SYSTEM password and it should be kept in a safe place! If it is lost the end user computers cannot be accessed any more in case of an emergency!

- The **user only** has the right to log on to their computer and to change their SDE user password. Users do not have any administrative rights

However, you may need to create other user types with sufficient rights to carry out specific tasks. For example, you may want to give a helpdesk officer the right to change user settings. You can do this by using the **Advanced Settings** when you pre-configure the encryption software, see [Configure the encryption software](#) on page 8.

For detailed information see the Sophos SafeGuard Disk Encryption help and the following knowledgebase article: <http://www.sophos.com/support/knowledgebase/article/56457.html>.

8 Install the administration tools

To deploy the encryption software to end user computers, first install the SDE administration tools on an administrator's computer. Before you do this, you must:

- Close all open applications.
- Ensure that there is enough free hard disk space.

Note: If you want to install the software on a computer running in an Asian language (or any language that uses "double-byte" characters), read the release notes first.

To install the administration tools, do as follows:

1. Log on to your computer as an administrator.
2. Double-click the installer you downloaded before. In the installer window, click **Install** to extract the installer's contents to your computer and start the installation wizard. The **Sophos SafeGuard Disk Encryption Installer** guides you through the necessary steps.
3. Accept the default on the next dialogs.
4. In **Select Installation Type** select **Distribution to networked computers** and click **Next**.
5. Accept the defaults on all further dialogs.

Installation of the SDE administration tools is finished. Next you use the administration tools to configure Sophos SafeGuard Disk Encryption before it is installed on end user computers.

9 Configure the encryption software

Do as follows:

1. Open the **Configuration File Wizard** via the Sophos SafeGuard Disk Encryption folder in the **Start** menu.
2. In **Configuration File Type** select **Installation** and click **Next**.
3. In **Base Configuration File (optional)** accept the default and click **Next** to create a new file.

A base configuration file is a template of Sophos SafeGuard Disk Encryption settings that can be applied to multiple end user computers, allowing for automatic installation and consistent configuration.


4. In **Passwords** enter and confirm the passwords for the two standard SDE users on the end user computers: system user (top-level administrator SYSTEM) and default user (USER).

Note: The password for the default user (USER) is the initial password that end users are prompted to change at first logon to Sophos SafeGuard Disk Encryption.

Make a note of the SYSTEM password and keep it in a safe place! If you lose it you will not be able to access the end user computers any more in case of an emergency!

You should also set up a helpdesk user with the right to reset passwords. To do this, check the **Show Advanced Settings** box. Click **Next**.

Note: The advanced settings also allow you to change the default encryption and security settings (encryption of partition C: and activated Pre-Boot Authentication).

5. In **Workstation Configuration**, select **Users**. Then click the Create User icon .
6. In the **New User** dialog box, in **New User Name**, enter the name `Helpdesk`. The features assigned to user 'Helpdesk' are displayed. Set the options as follows:
 - **Issue abbreviated C/R code:** set to **Yes**.
 - **Password change allowed:** set to **No**.
 - **Password:** Click **Password**, then click [...] to configure a password. A dialog is displayed. Enter and confirm a new password for the helpdesk user.
 - **Rights:** Click **Rights**, then click [...]. In the **User Rights** dialog, double-click the **Change user settings** box so that the helpdesk user can set a new user password and allow a one time logon. Double-click **Uninstall** if you want the helpdesk user to be able to uninstall SDE.Click **Next**.
7. Save the file as a base configuration and accept the default storage location.
8. Click **Finish**.

The base configuration `Install.cfg` has been created. Next deploy the encryption software to the end user computers.

10 Deploy the encryption software to end user computers

Before you deploy the encryption software, prepare for installation on the end user computers, see [Prepare for installation](#) on page 5.

1. Use your own tools to create and distribute an installation package to be installed on the end user computers. The package must include:
 - installation package `SDE.msi` which you will find in the downloaded product folder
 - generated base configuration file `Install.cfg`
 - a script with the command line for the pre-configured installation
2. Create a folder `Software` on the administrator computer to use as a central store for all applications.
3. Create the script.

Script example:

```
msiexec /i C:\Software\Sophos\SDE.msi  
/L*VX \\%distributionserver%\Sophos\%computername%_SDE_inst.log  
CFGFILE=C:\Software\Sophos\Install.cfg /QN
```

```
/i C:\Software\Sophos\SDE.msi
```

Installs the Sophos SafeGuard Disk Encryption installation package from the specified storage location to the default installation directory `C:\Program Files\Sophos\SafeGuard Disk Encryption`. The following is installed by default: encryption of partition C: including activation of the Pre-Boot Authentication and Secure Automatic Logon to Windows.

```
/L*VX \\%distributionserver%\Sophos\%computername%_SDE_inst.log
```

Logs all warnings and error messages in the specified log file on the network and creates a useful log file that can be analyzed automatically by using `wilogutl.exe`.

```
CFGFILE=C:\Software\Sophos\Install.cfg
```

States the base configuration file to be applied on the end user computers.

```
/QN
```

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

4. Distribute the installation package to the end user computers.
5. Communicate the default SDE user password to the end users and inform them about post-installation tasks, see [Carry out post-installation tasks](#) on page 7.

Note:

If you want to encrypt the administrator computer with Sophos SafeGuard Disk Encryption as well, do either of the following:

- Run `setup.exe` with a **Modify** installation and installation type **Encryption on this computer**. Accept the defaults on all dialogs.
- Deploy the pre-configured installation created before to the administrator computer.

11 Recover a forgotten password

If the user forgets the SDE user password, the helpdesk officer may reset it via the Challenge/Response procedure as follows:

Prerequisite: The **Response Code Wizard** must have been installed on the helpdesk computer. The helpdesk officer must have the rights to change user settings and must be allowed to issue an abbreviated Challenge/Response code.

For detailed information see the Sophos SafeGuard Disk Encryption help.

To recover a forgotten password, do as follows:

1. The end user needs to start their computer. The Pre-Boot Authentication is displayed.
2. In the **Password** field, the end user needs to press [F9] on the keyboard.
3. A challenge code is displayed on the end user computer.
4. The end user calls the helpdesk and lets the helpdesk officer know the user ID and the challenge code.
5. The helpdesk officer opens the **Response Code Wizard** via the Sophos SafeGuard Disk Encryption folder in the **Start** menu.
6. The helpdesk officer authorizes the access to the end user computer.
7. The helpdesk confirms the end user ID and enters the challenge code.
8. The helpdesk officer grants the end user the right to reset the SDE user password. A response code will be generated.
9. The helpdesk officer passes the response code on to the end user.
10. The end user enters the response code below the challenge code.
11. The end user needs to reset the SDE user password and may continue working at the computer.

12 Recover access to the system

Note: Backup the system kernel at regular intervals and store the backup on an external medium or on the network to have an up-to-date-backup available at any time. You can do this by using the **Emergency Disk Wizard** in the Sophos SafeGuard Disk Encryption folder of the **Start** menu. For further information see the Sophos SafeGuard Disk Encryption help.

If the end user can no longer log on to the computer because of a system error, see the following knowledgebase article: <http://www.sophos.com/support/knowledgebase/article/56456.html>.

13 Get help with common tasks

This section tells you where to find information on how to carry out common tasks.

Refer to the Sophos SafeGuard Disk Encryption help for all further information.

Task	Chapter in Sophos SafeGuard Disk Encryption help
Log on to Sophos SafeGuard Disk Encryption	System boot and logon, Logging on as a default user
Change your Sophos SafeGuard Disk Encryption user password	System boot and logon, Changing the SDE password via the F10 key
Lock your computer	Sophos SafeGuard Disk Encryption workstation lock
Assign administration rights	Creating user profiles
Change the Sophos SafeGuard Disk Encryption configuration	Administration overview
Encrypt further hard drive partitions	Encryption, Configuring encryption
Get help for resetting a forgotten password	System boot and logon, Help function for resetting forgotten passwords via the [F9] key
Give help for resetting a forgotten password	Remote maintenance (Challenge/Response)
Recover access to the system	Saving the system kernel and creating emergency media

14 Technical support

For technical support, visit <http://www.sophos.com/support>.

If you contact technical support, provide as much information as possible, including the following:

- Sophos software version number(s)
- Operating system(s) and patch level(s)
- The exact text of any error messages

15 Copyright

Copyright © 1992 - 2009 Utimaco Safeware AG - a member of the Sophos group

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 Sophos Group.

SafeGuard is a registered trademark of Utimaco Safeware AG - a member of the Sophos group.

Patent rights of Ascom Tech Ltd. given in EP, JP, US. IDEA is a trademark of Ascom, Tech Ltd.

All other product and company names mentioned are trademarks or registered trademarks of their respective owners and are recognized as such.