

# SOPHOS

## SafeGuard® Disk Encryption Demo Guide

Document Version: 5.50

Document Date: 29. April 2010



## Contents

<b>1</b>	<b>Introduction</b>	<b>3</b>
<b>2</b>	<b>Requirements</b>	<b>4</b>
<b>3</b>	<b>Installing the evaluation software</b>	<b>5</b>
<b>4</b>	<b>What to expect once the software has been installed</b>	<b>6</b>
4.1	Windows XP	7
4.2	Vista and Windows 7	8
4.3	Hard drive encryption process	11
4.4	Configuring Local Self Help	11
4.5	Next time you reboot	14
4.6	Forgotten Password	15
<b>5</b>	<b>Removing the evaluation software</b>	<b>19</b>

# 1 Introduction

This document guides you through the evaluation version of the Sophos SafeGuard Disk Encryption client. The evaluation will enable you to test the SafeGuard full disk encryption process, including the installation and use of the pre-boot power-on authentication (POA). A pre-configured policy is provided. This policy cannot be edited within this demo version.

This demo serves as a common client demo for the following products which all use the same SafeGuard client engine:

- **Sophos SafeGuard Disk Encryption (SDE)**  
Full disk encryption solution for local hard drives. Provided as part of the Sophos Endpoint Security and Data Protection (ESDP) license. Encryption policy configuration is carried out using SafeGuard Policy Editor (which is not supplied in this evaluation version). For more information see:  
<http://www.sophos.com/products/enterprise/endpoint/security-and-control/>
- **SafeGuard Easy (SGE)**  
Similar to SDE, adding support for Lenovo fingerprint authentication and external harddrives as well as supporting a runtime environment to have two encrypted Windows installations in parallel on the same PC. Encryption policy configuration is carried out using SafeGuard Policy Editor (which is not supplied in this evaluation version). For more information see:  
<http://www.sophos.com/products/enterprise/encryption/safeguard-easy/>
- **SafeGuard Enterprise Device Encryption (SGN DE)**  
Flagship encryption product of Sophos, adding Active Directory integrated on-line central management, reporting, multi-factor authentication (via Lenovo fingerprint, smartcards or crypto tokens) and advanced key management for removable media encryption and port control. If you are interested in security beyond local disk encryption, SafeGuard Enterprise is the product to go for. This demo only shows the local full disk encryption client. A demo of the full SafeGuard Enterprise including the Management Center and all modules is alternatively available. It allows exploring all functions of the product and can be converted easily to a full version via a license key mechanism without reinstallation of any software necessary.  
Please contact a Sophos sales representative to receive this demo or more details on SafeGuard Enterprise, see also  
<http://www.sophos.com/products/enterprise/encryption/safeguard-enterprise/>

## 2 Requirements

The Sophos SafeGuard Disk Encryption installation requires:

- Windows XP SP2 or later (32 bit)
- Windows Vista SP1 (32 bit)
- Windows Vista SP1 (64 bit)
- Windows 7 (32 or 64 bit)
- Minimum 1 GB ram
- Minimum 1 GB of free disk space
- IDE/or SATA drive (no SCSI). See here for hardware compatibility information <http://www.sophos.com/support/knowledgebase/article/107781.html>
- If running Lenovo Rescue and Recovery, please ensure version 4.21 or later is in use.

If in doubt regarding the supported platform, you may run the installation, it will let you know if a problem is encountered and back out of the operation. Also please note that the 64 bit installer is a separate download from Sophos.com.

In addition prior to running the installation please ensure that you have administrative rights to the client machine where you are about to install the software.

*Note: this software is provided for evaluation purposes only and should not be used on production computers. To upgrade from demo to full version you will have to remove the demo software, see section 5 of this guide, and install the full version which includes a re-encryption of the PC where the demo was installed. As an alternative you may want to install the demo in a virtual machine and just restore this machine to an old snapshot after evaluation.*

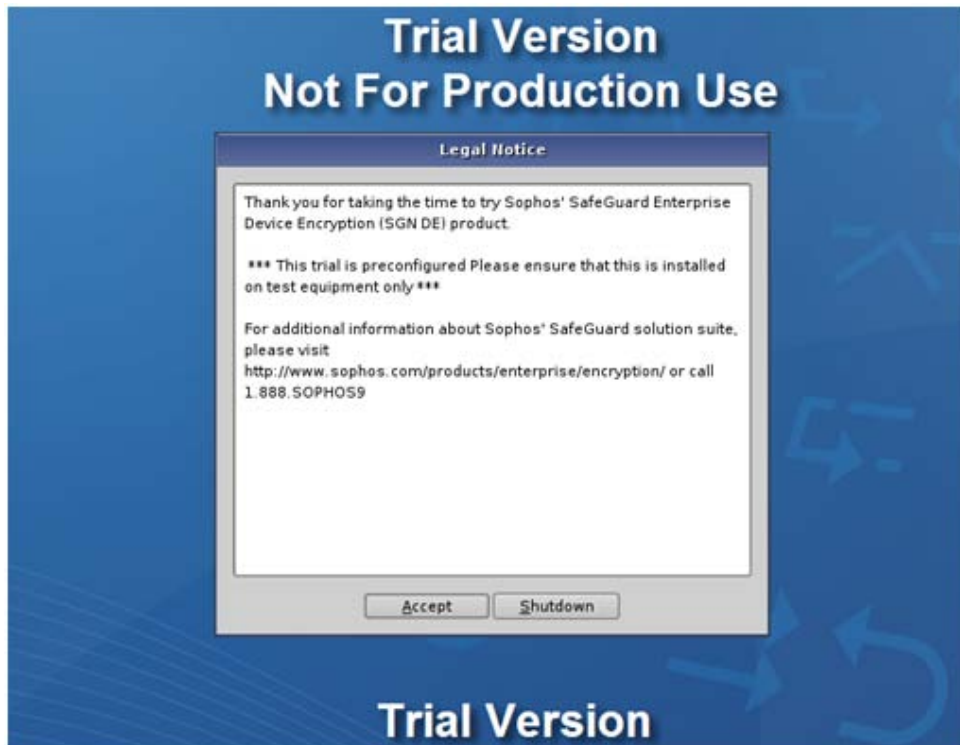
### 3 Installing the evaluation software

In order to install the software, please follow these steps:

1. Close any open applications and run the executable provided. Either “ssg\_55\_demo\_sfx.exe” for 32 bit systems or “ssg\_55\_demo\_64bit\_sfx.exe” for 64bit Vista and Windows 7.
2. During the install you will be prompted to accept the terms and conditions of the evaluation but no configuration choices are necessary. During the installation process, the installation files will be extracted to c:\SGNFiles or c:\SGNFiles64, depending on your system. The software will then be installed to C:\Program files\Sophos\SafeGuard Enterprise (Program Files(x86) on 64 bit machines).
3. Once the installation has been completed the system will automatically reboot, install a security module on the drive and perform a quick check disk scan. Please do not interrupt this process.
4. You will see a Sophos screen and an Auto-login message appear. The system will then boot to the Windows.

## 4 What to expect once the software has been installed

The first screen you will see is the legal notice screen (below). This is an optional policy feature that you can enable when you roll out SafeGuard encryption in your environment. In the full version of the product, the text is fully customizable. For now read and click OK.



## 4.1 Windows XP

### 4.1.1 If you already have a Windows password set

The Windows login screen will now be presented. Enter your Windows credentials and login to Windows. At this point SGN will synchronize your Windows Credentials with its Power on Authentication (POA) system. Note: SafeGuard Encryption uses your same Windows credentials for its power on authentication.

### 4.1.2 If you do not already have a Windows password set

If you did not have a Windows password configured, you will now be forced to do so. The following screen will be displayed:



If you have no password the "Old Password field" should be left blank.

In new password type a word or phrase that you can remember, repeat this in the confirmation box.

In new password type a word or phrase that you will remember, repeat this in the confirmation box. If you are unsure what password to set right now just type sophos.

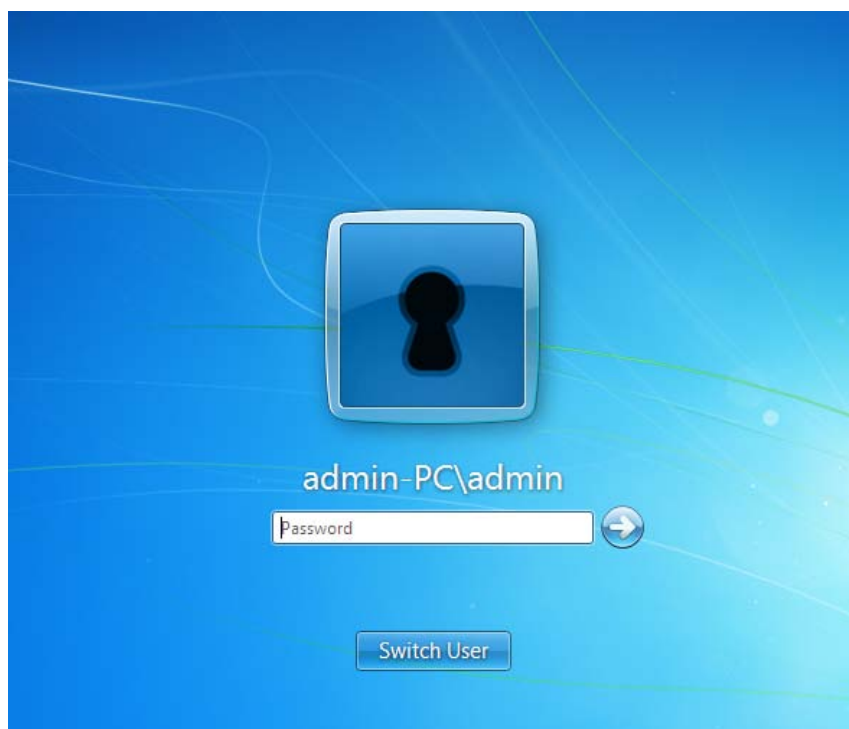
**Important: The password must be remembered in order to access the encrypted drive and boot the PC. You should configure Local Self Help now in order to have a recovery mechanism should you forget your credentials (see section 4.4).**

## 4.2 Vista and Windows 7

Windows 7 and Vista have a different authentication mechanism to XP. If you are using these operating systems then the following behavior can be expected.

### 4.2.1 If you already have a Windows password set

After the operating system loads you will be passed straight to the desktop just as before. Only this time you will be presented with the following screen:



Simply enter your password and the desktop will load, SafeGuard Disk Encryption will then synchronize your credentials. Next time you reboot you will be able to login to the Power on Authentication screen with these same credentials.

If for some reason you do not see the key-hole icon select “Switch user” and choose this icon before logging in.

### 4.2.2 If you do not already have a Windows password set

After you select OK on the legal text screen, Windows will load, and you will be taken directly to the desktop as normal. Due to the demo configuration we need to synchronize your Windows credentials with the Power on Authentication mechanism. Note: SafeGuard Encryption uses your same Windows credentials for its power on authentication).

To enable the synchronization, you will be prompted with the following window:



Sophos SafeGuard® Logon

Sophos SafeGuard® SOPHOS

Please enter your password to complete the logon.

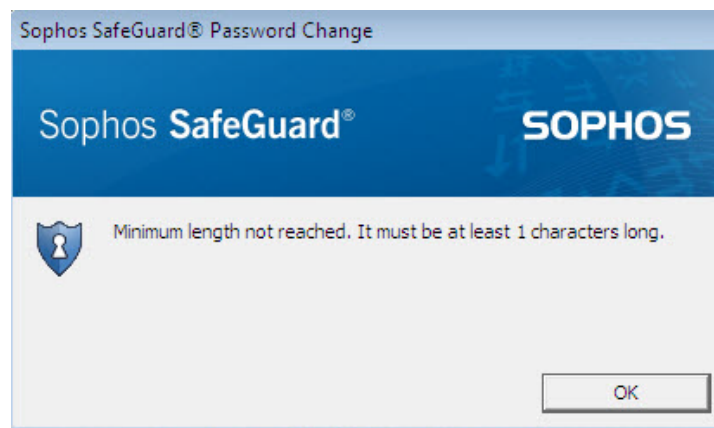
User name: Administrator

Domain: WIN-RG4D0JQO2IS

Password: |

OK Cancel

As you have no password simply select OK. You will now be presented with the following screen:



Sophos SafeGuard® Password Change

Sophos SafeGuard® SOPHOS

Minimum length not reached. It must be at least 1 characters long.

OK

This happens because SafeGuard Disk Encryption will not accept a zero length password. Click OK, and you will now be prompted to change your password:



Sophos SafeGuard® Password Change

Sophos SafeGuard® SOPHOS

User name: Administrator

Domain: WIN-RG4D0JQO2IS

Old Password: |

New Password: |

Confirmation: |

OK Cancel

If you have no password the “Old Password field” should be left blank.

In new password type a word or phrase that you will remember, repeat this in the confirmation box. If you are unsure what password to set right now just type sophos.

**Important: The password must be remembered in order to access the encrypted drive and boot the PC. You should configure Local Self Help now in order to have a recovery mechanism should you forget your credentials (see section 4.4).**

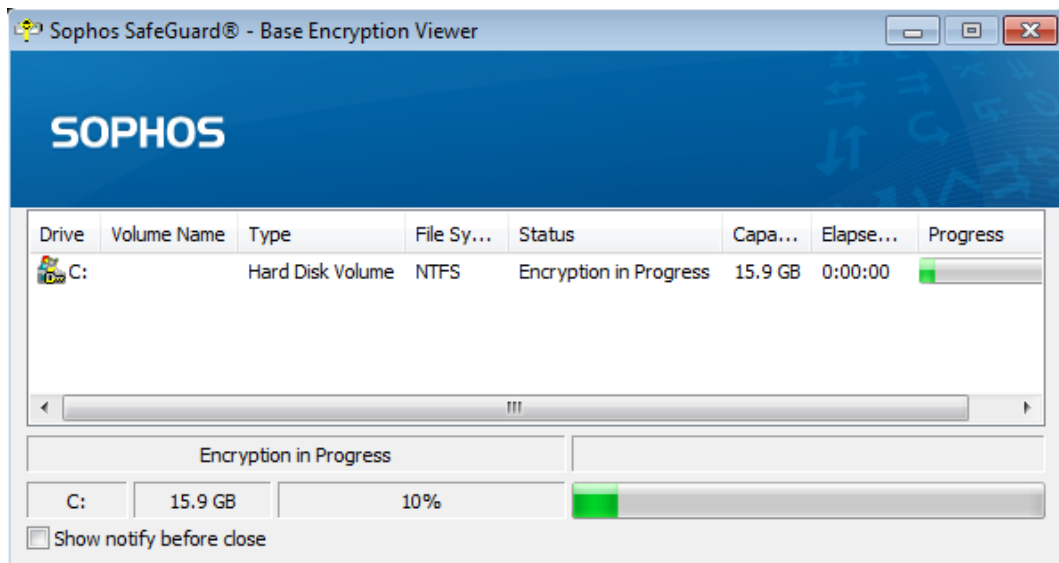
## 4.3 Hard drive encryption process

Once logged into Windows you will see a tab appear in the task bar:



Click on this to see the initial encryption progress.

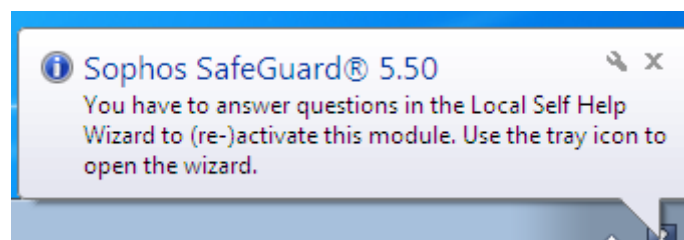
Please note that during the initial encryption time you may experience a slowdown in performance of the system.



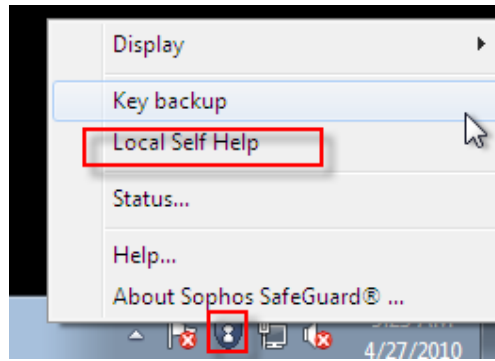
At this point you can continue to work, or shut down the PC and move about. The initial encryption process will continue where it left off if you choose to shut down.

## 4.4 Configuring Local Self Help

After logging into your desk top you will notice a pop up:



This is an advisory to let you know that you can now configure the Local Self Help. Local self help allows you to recover your forgotten login credentials by providing answers to questions to which you had previously provided answers to in the configuration process. To configure local Self Help, right click on the shield icon in your task bar and choose Local Self Help



Once selected you will be prompted to re-enter your credentials:

A screenshot of the 'Local Self Help' dialog box. It features the Sophos logo on a blue background. The form contains the following fields and options:

- User: admin@admin-PC
- Password: (empty)
- Local Self Help (LSH) State:
  - Enabled: Yes
  - Active: No

Buttons for 'Next >' and 'Cancel' are at the bottom right.

Enter your Windows username and password and then click next.

A screenshot of the 'Local Self Help' dialog box showing the 'Status Overview' screen. It includes the Sophos logo and the following text:

You have to answer at least 10 questions for Local Self Help to become active. Please be aware that you later have to re-type the answers in POA exactly the same way as you will answer them here initially.

Example: If you enter "Hotel" as an answer, you have to retype "Hotel". "hotel" is treated as an incorrect answer.

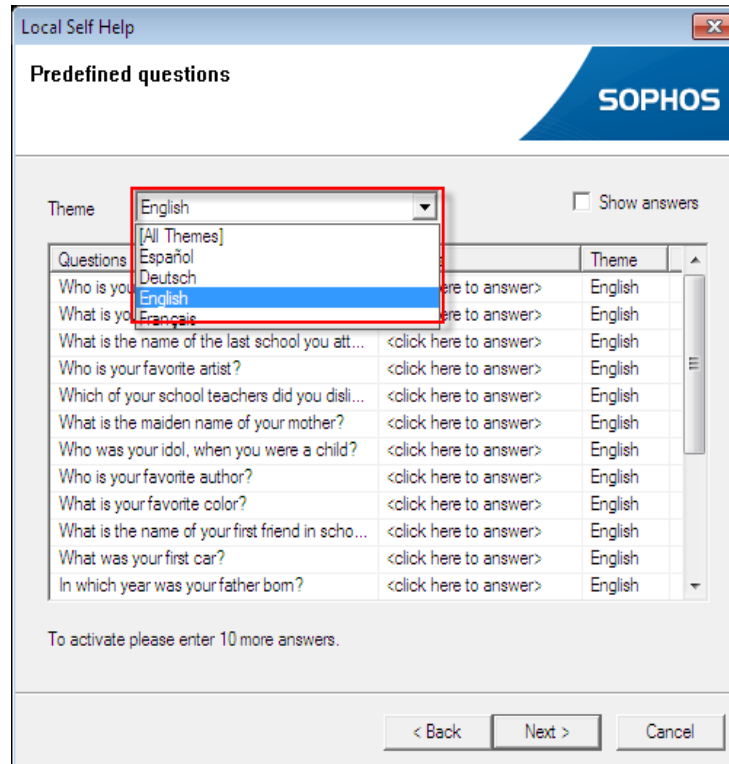
There are 0 (of 72) predefined questions answered.

Local Self help is not active for you.

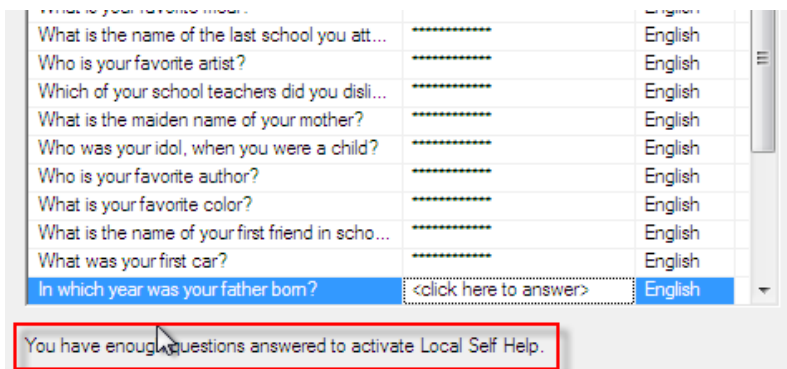
To activate please enter 10 more answers.

Buttons for 'Next >' and 'Cancel' are at the bottom right.

This screen provides a status click next.

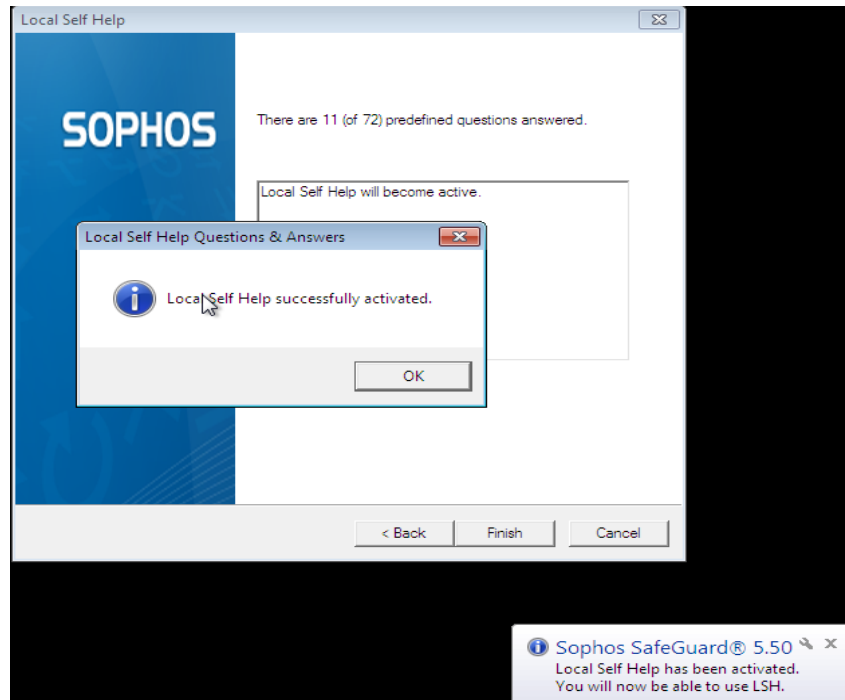


On the predefined questions screen choose a language theme; you may then begin to answer the questions. Please keep in mind that these answers will be case sensitive.



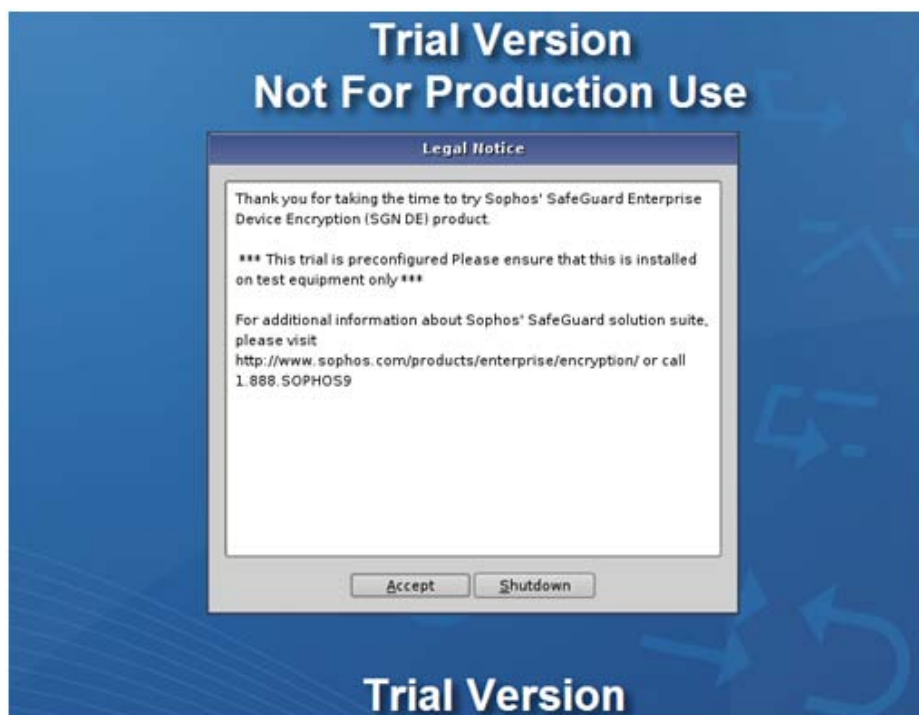
Once you have answered 10 questions you will notice the status at the bottom of the screen change.

Click next and then finish, finalizing the activation of Local Self Help.



## 4.5 Next time you reboot

When you next reboot the power on authentication will have been enabled. The first screen is the legal notice, just as before click accept to proceed. In the full product, both the legal text and the following screens seen here are customizable allowing you to minimize the visual impact of this security on your end users. Naturally in this demonstration version the impact is highly visible and not configurable:



Once you have passed the legal text screen you may now login to the power on authentication. Enter your credentials in the fields provided and click OK.



SafeGuard Disk Encryption will validate the credentials and then allow Windows to load. Until you enter a valid set of credentials the data on the drive will be inaccessible to anyone.

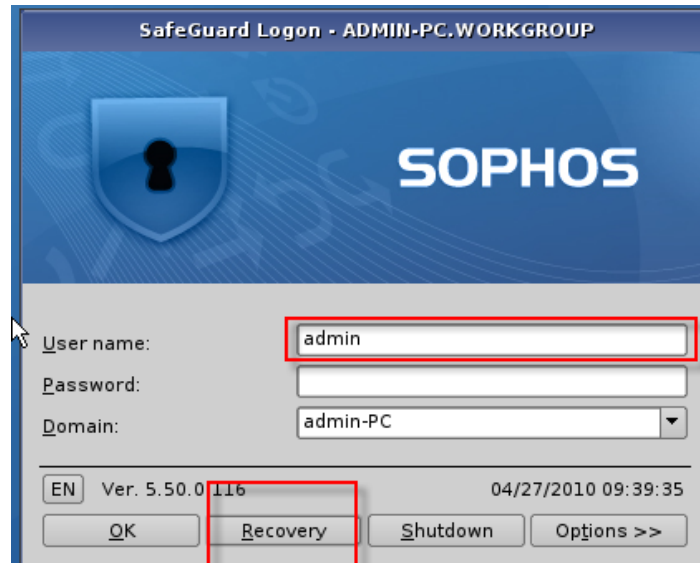
At this point there is nothing else that needs to be done to configure the software. The exact detail of what functionality is available in the full version will depend upon which version of the product, ESDP / SafeGuard Easy or SafeGuard Enterprise, you purchase. Full details can be found on the Sophos web site.

## 4.6 Forgotten Password

In the event that you have forgotten the password that you used to access Windows when configuring SafeGuard Disk Encryption, there are two recovery options available to you.

### 4.6.1 Local Self Help

If you have followed this guide then you will have configured the Local Self Help option. To recover your system in the event that you have forgotten your password, follow these steps:



First ensure that your username is entered correctly, and then choose Recovery. If you have configured Local Self Help but do not remember your username go to section 4.6.2



Now Choose Local Self Help, Challenge/response is not available to you in the demo version.

You will now be asked to answer five of the questions you answered during the configuration. These answers are case sensitive. You must answer all five correctly in order to proceed. If you get an answer wrong SafeGuard will treat this as a failed login attempt. No indication of which question was incorrectly answered will be provided.

Local Self Help - Question 4 of 5



# SOPHOS

Enter the answer to the question in the field provided below:

What is the maiden name of your mother?

  
  
 Hide answer

Password Recovery



# SOPHOS

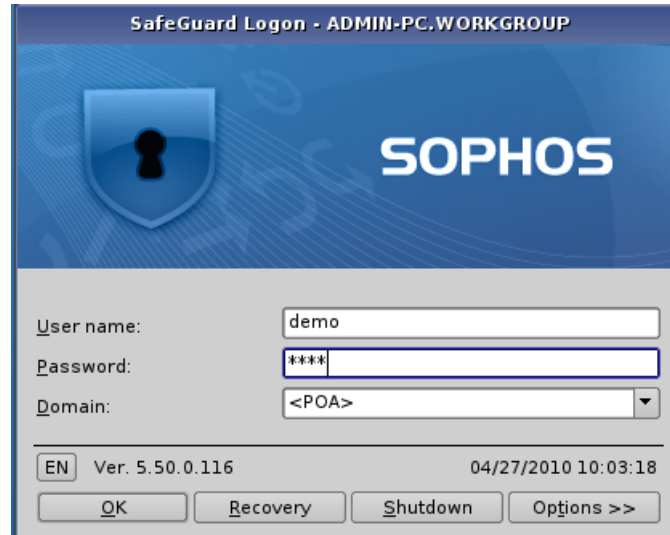
**Password Recovery**

The password will be shown/hidden if you click on the box below, press the space bar or Enter. It will be displayed for a maximum of 5 seconds. Afterwards the boot process will continue automatically. Please ensure that no one else can see your password. To continue booting the system, please press "OK".

Once successful you may now click the blue box to be reminded of your password or simply click OK to be allowed access to Windows.

## 4.6.2 Forgotten Username and Password

In the event that you have forgotten both your username and password, the demo has been preconfigured with a set of credentials to authenticate you at POA.



At the POA screen enter

User name: Demo,

Password: bob1

Domain: <POA>

Then select ok.

POA Authentication will now proceed bringing you to a Windows login screen. At this point you may try another Windows user to access the system. In the productive version, such recovery accounts can be configured by the administrator as an option. Usually user password recovery happens either via Local Self Help or Challenge / Response.

## 5 Removing the evaluation software

Once you have completed your evaluation you will want to move to a full version of the SafeGuard encryption solution. To do this you may simply choose to re-image your test machine, or first uninstall the software. To remove the software simply open add / remove programs and remove the “Sophos SafeGuard 5.50 client configuration” and then remove the “Sophos SafeGuard 5.50 Client”. When you remove the client you will see the drive begin to decrypt. It is recommended that you uninstall both packages at the same time and allow the drive to finish decrypting before rebooting.

If the system is rebooted during this process the un-installation will be cancelled, though the decryption will continue when the system is restarted. Once decryption has completed you will be able to reinitiate the removal of the SafeGuard encryption client.

Please use [Sophos.com](https://www.sophos.com) or contact your local sales representative if you interested in learning more about the SafeGuard product portfolio or want to order the full license version.

Boston, USA | Oxford, UK  
© Copyright 2010, Sophos Plc

*All registered trademarks and copyrights are understood and recognized by Sophos.  
No part of this publication may be reproduced, stored in a retrieval system, or transmitted by any form or by  
any means without the prior written permission of the publishers.*

**SOPHOS**  
[WWW.SOPHOS.COM](http://WWW.SOPHOS.COM)