

SOPHOS

Sophos SafeGuard Disk Encryption 5.50 Sophos SafeGuard Easy 5.50 Tools guide

Document date: April 2010



Content

- 1 About this guide 2
- 2 Displaying the system status with SGNState..... 3
- 3 Reverting an unsuccessful installation with SGNRollback 4
- 4 System recovery and the recovery tool BE_Restore.exe 8
- 5 Decommissioning encrypted volumes with BEInvVol.exe..... 12
- 6 Technical support..... 15
- 7 Copyright 16

1 About this guide

This guide explains the usage of Sophos SafeGuard tools provided in the tools directory of your Sophos SafeGuard software delivery for different procedures and usage scenarios.

The following tools are covered in this document:

- SGNState
- SGNRollback
- BE_Restore.exe
- BEInvVol.exe

Note: Additionally you will find the tool Recover Keys (RecoverKeys.exe) in the tools directory of your Client software delivery. The tool Recover Keys is used to start a Challenge/Response procedure to regain access to the computer in a complex recovery situation, e.g. when the POA is corrupted and the computer needs to be booted from the SafeGuard recovery disk. The tool is already present on the recovery disk and is additionally available in the tools directory. You will find a detailed description of the tool and as of an emergency in the SafeGuard Administrator's help, keyword Challenge/Response using Virtual Clients.

1.1 Intended audience

The intended audience for this guide are administrators working with Sophos SafeGuard as security officers.

2 Displaying the system status with SGNState

Sophos SafeGuard offers the command line tool SGNState for displaying information on the current status (encryption status and further detailed status information) of the Sophos SafeGuard installation on an endpoint computer.

You will find the tool in the Tools directory on your Sophos SafeGuard Client software folder.

2.1 Reporting

SGNState can also be used for reporting:

- The SGNState return code can be evaluated on the server using third-party management tools.
- SGNState /LD returns output that is formatted for LANDesk which can be diverted to a file.

2.2 Parameters

You can call SGNState with the following parameters:

SGNSTATE [/?] [/L] [/LD]

- Parameter /? returns help information on the available SGNState command line parameters.
- Parameter /L shows the following information:
 - Operating system
 - Installed Sophos SafeGuard version
 - POA type (Sophos SafeGuard)
 - POA status (on/off)
 - Wake on LAN status (on/off)
 - Server name
 - Logon mode
 - Client activation state
 - Date (and time) of the last data replication
 - Last policy received
 - Encryption status (encrypted/not encrypted), algorithm used for the individual volumes
- Parameter /LD returns this information formatted for LANDesk.

3 Reverting an unsuccessful installation with SGNRollback

In case of an unsuccessful attempt to install Sophos SafeGuard on an endpoint computer, it may occur that the computer can no longer boot and is inaccessible for remote administration.

For situations of this kind Sophos SafeGuard offers the tool SGNRollback.

SGNRollback automatically reverts the effects of an unsuccessful installation of Sophos SafeGuard by

- enabling the booting of the blocked computer in question,
- removing Sophos SafeGuard and
- undoing any modifications to the GINA and other system operating components.

SGNRollback is available as an executable in the tools directory of your Sophos SafeGuard Admin software folder and is started from a Windows-based recovery system, either Windows PE or BartPE.

3.1 Usage scenario

SGNRollback can repair an unsuccessful Sophos SafeGuard installation on an endpoint computer, if the following applies:

- The Power-on Authentication freezes during the first boot and the computer can no longer boot.
- The hard drive is not encrypted.

Note: A migration scenario from SafeGuard Easy to Sophos SafeGuard is not supported.

3.1.1 Further prerequisites

For using SGNRollback the following further prerequisites apply:

- SGNRollback works on the recovery systems WinPE and BartPE. To be able to use SGNRollback for recovery, integrate it into the required recovery system. Please refer to the relevant recovery system documentation for further information.

If SGNRollback is to be started via autorun, the administrator using SGNRollback has to define the relevant settings in WinPE (see [Enabling SGNRollback autostart for Windows PE](#), page 5) or BartPE (see [Enabling SGNRollback autostart for BartPE](#), page 6).

- Sophos SafeGuard Device Encryption is installed.

3.1.2 Supported operating systems

SGNRollback supports the following operating systems:

- Windows XP
- Windows Vista
- Windows 7

3.2 Starting SGNRollback in the recovery system

You can start SGNRollback manually or add it to the recovery system autostart.

3.2.1 Enabling SGNRollback autostart for Windows PE

To enable SGNRollback autostart for Windows PE, install the Microsoft Windows Automated Installation Kit. The Windows Preinstallation Environment User Guide describes how to build a Windows PE environment and how to autostart an application.

3.2.2 Enabling SGNRollback autostart for BartPE

To enable SGNRollback autostart for BartPE, do as follows:

1. Use the BartPEBuilder version 3.1.3 or higher to create a PE image. For further details refer to the BartPE documentation.
2. In the BartPE Builder, add the recovery tool folder in the **Custom** field.
3. Build the image.
4. Copy the file AutoRun0Recovery.cmd from the Sophos SafeGuard Media to the i386 folder of the BartPE-prepared Windows version.

5. Create an AutoRun0Recovery.cmd with the following two lines of text:

```
\Recovery\recovery.exe  
exit
```

6. Run the PEBuilder tool from the command line:

```
Pebuilder -buildis
```

A new iso image is built which includes the autorun file.

7. Save the resulting image on a recovery media.

When booting this image SGNRollback will start automatically.

3.3 Parameters

SGNRollback can be started with the following parameter:

<code>-drv WinDrive</code>	Indicates the letter of the drive the Sophos SafeGuard installation to be repaired is on. This parameter can only be used in recovery mode. It has to be used on multi-boot environments to indicate the correct drive.
----------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

3.4 Reverting an unsuccessful installation

To revert the effects of an unsuccessful Sophos SafeGuard installation on an endpoint computer, proceed as follows:

1. Boot the computer from the recovery media containing the recovery system including SGNRollback.
2. Start SGNRollback in the recovery system. If autorun applies, SGNRollback will start automatically. SGNRollback prepares the operating system for the uninstallation of Sophos SafeGuard.
3. You are now asked to remove the recovery media. After removing the media, the computer will be rebooted in safe mode of the operating system.

All modifications made are removed and Sophos SafeGuard is uninstalled.

4 System recovery and the recovery tool BE_Restore.exe

The Sophos SafeGuardboot process

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.

4.1 Restoring a corrupted MBR

The Sophos SafeGuard Power-on Authentication is loaded from the MBR on a computer's hard disk. When the installation is done, Sophos SafeGuard saves a copy of the original - as it was before the Sophos SafeGuard installation - in its kernel and modifies the BPR loader from LBA 0. In its LBA 0, the modified MBR contains the address of the first sector of the Sophos SafeGuard kernel and its total size.

Problems with the MBR can be resolved using the Sophos SafeGuard recovery tool BE_Restore.exe. This tool is a Win32 application and must run under Windows - not under DOS.

A faulty MBR loader will mean an unbootable system. It can be restored in two ways:

- Restoring the MBR from a backup,
- Repairing the MBR

For restoring a corrupted MBR successfully, some preparative steps are necessary:

1. We recommend that you create a Windows PE (Preinstalled Environment) CD.
2. To use the client recovery tool BE_Restore.exe several additional files are required. You will find the tool and the required files in your Client software folder under folder tools\KeyRecovery and Restore. Copy all files in this folder to a memory stick. Make sure to store all of them together in **the same** folder on your memory stick. Otherwise the recovery tool will not start properly.
3. If necessary adjust the boot sequence in the BIOS and select the CD-ROM to be first.

Note: BERestore can only restore or repair the MBR on disk 0. If you use two hard disks and the system is booted from the other hard disk, the MBR cannot be restored or repaired. This is also applies when using a removable hard disk.

4.1.1 Restoring a previously saved MBR backup

To restore a previously saved MBR backup, proceed as follows:

1. After the installation of Sophos SafeGuard on the endpoint computer you are prompted to specify a file location for saving the MBR backup. This produces a 512 byte file with the file extension .BKN, which contains the MBR.
2. Copy this file to the folder on the memory stick in which the other extra Sophos SafeGuard files are located.
3. Now insert the Windows PE Boot CD into the drive, plug in the memory stick with the Sophos SafeGuard files and switch the computer on to boot from the CD.
4. When the computer is ready, start the cmd-box, navigate to the directory on the memory stick where the Sophos SafeGuard files are located and run BE_Restore.exe.
5. Select **Restore MBR** to restore from a backup and select the .BKN file.

BE_Restore.exe. will now check, if the selected .BKN file matches the computer and will afterwards restore the saved MBR.

4.1.2 Repairing the MBR without backup

Even when there is no MBR backup file available locally, BE_Restore.exe can repair a damaged MBR loader. BE_Restore.exe - **Repair MBR** locates the Sophos SafeGuard kernel on the hard disk, uses its address, and recreates the MBR loader.

This is highly advantageous, especially as there is no need for a computer-specific MBR backup file locally. However, it takes a little more time because BE_Restore.exe - **Repair MBR** has to carry out a time-consuming search for the Sophos SafeGuard kernel on the hard disk.

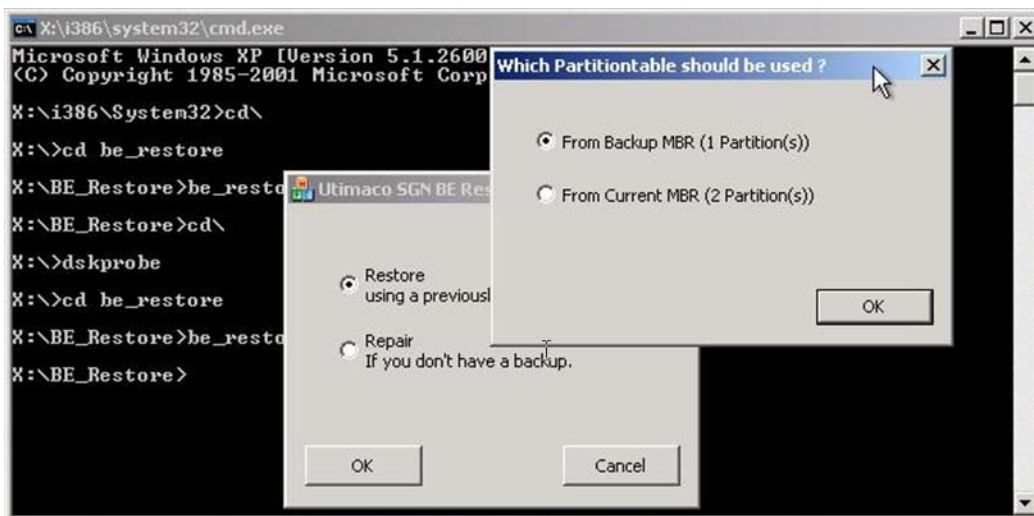
To use the repair function, proceed as described, however, select **Repair MBR** when running BE_Restore.exe.

If more than one kernel is found, BE_Restore.exe – **Repair MBR** uses the one with the most recent time stamp.

4.1.3 Partition table

Sophos SafeGuard allows the creation of new primary or extended partitions. This causes the partition table on the hard disk with the partition to be changed.

When restoring an MBR backup, BE_Restore will see that the current MBR contains different partition tables for the LBA 0 and the MBR backup file that is to be restored (*.BKN). In a dialog, the user can specify the procedure.



4.1.3.1 Repairing an MBR with a corrupt partition table

A corrupt partition table may result in a non-bootable operating system after successful POA logon.

You can resolve this problem using BE_Restore.exe to restore a previously saved MBR or repair the MBR without an MBR backup.

If you have a backup, proceed as described for option **Restore MBR**.

If you do not have a backup, do as follows:

1. Insert the Windows PE Boot CD into the drive, plug in the memory stick with the Sophos SafeGuard files and switch the computer on to boot from the CD.
2. When the computer is ready, start the cmd-box, navigate to the directory on the memory stick where the Sophos SafeGuard files are located and run BE_Restore.exe

3. Select **Repair MBR**. If BE_Restore.exe detects a difference between the partition table of the current MBR and the mirrored MBR, dialog for selecting the partition table to be used is displayed.

The mirrored MBR is the original Microsoft MBR saved during the Sophos SafeGuard Client setup for restoring purposes, e.g. in case of uninstalling the client. The partition table in this mirrored MBR is being kept up-to-date by Sophos SafeGuard, if any partition changes occur in Windows.

4. Select **From Mirrored MBR**.

If you select **From Current MBR**, the partition table from the current MBR - i.e. in this case a corrupt partition table - will be used. Not only will the system in this case remain non-bootable, but also the mirrored MBR will be updated and therefore also corrupted.

4.1.4 Windows Disk Signature

Whenever Windows creates a file system for the first time on a hard disk, it creates a signature for the hard disk. This signature is saved in the hard disk's MBR at the Offsets 0x01B – 0x01BB. Note that, for example, the logical drive letters of the hard disk depend on the Windows Disk Signature.

Example: The Windows Administrator uses the Windows hard disk manager to change the logical drive letters of the drives C:, D:, and E: to C:, F:, and Q. This deletes the Windows Disk Signature from the hard disk's MBR. After the next boot process, Windows drops into a time-consuming hard disk scan mode and restores the list of drives. The result is that the three drives have their original drive letters C:, D: and E again:

Whenever that occurs under Sophos SafeGuard, Sophos SafeGuard's filter driver “BEFLT.sys” is not loaded. This makes the system unbootable: The computer shows a blue screen ‘STOP 0xED “Unmountable Boot Volume”’.

To repair this under Sophos SafeGuard, the original Windows Disk Signature has to be restored in the hard disk's MBR.

This, too, is done by BE_Restore.exe.

Note: You should be very careful when using any other tool to repair the MBR! For example, an old MS DOS FDISK.exe, that you use to rewrite the MBR loader (“FDISK /MBR”) could create another MBR loader with no Windows Disk Signature. As well as the fact that an old tool can delete the Windows Disk Signature, the “new” MBR loader might not be compatible with the hard disk sizes commonly used today. You should always use up-to-date versions of repair tools.

5 Decommissioning encrypted volumes with BEInvVol.exe

For Sophos SafeGuard protected computers we provide command line tool BEInvVol.exe which can be used to safely decommission encrypted volumes (hard disks, USB sticks etc.) particularly in the case of the two key stores created and managed by Sophos SafeGuard. This command line tool permits easy decommissioning of all encrypted volumes. Our command line tool is based on DoD Standard 5220.22-M, which can be used to safely delete key stores. This standard consists of seven overwrite cycles with random and alternative patterns.

This command line tool can only be used on a computer on which Sophos SafeGuard is installed. Once the desired volume has been found, a warning message is displayed requiring the user to confirm the request. All key stores (primary & secondary) are then deleted. From this point on, they volume will no longer be readable.

According to DoD Standard 5220.22-M, the command line tool permanently purges the Sophos SafeGuard Key Storage Areas (original KSA and backup) of each encrypted volume by overwriting them seven times. As the random Data Encryption Keys of each volume are not backed up in the central database for Sophos SafeGuard Clients, the volumes are perfectly sealed afterwards. Even a Security Officer cannot regain access.

The command line tool also displays information on screen about the delete process. This includes for example the name of the volume, the size of the volume, key store information such as symbolic key name, date and time of the deletion, the user who carried out the deletion and the computer name on which the deletion was carried out. This information can be stored on any storage device, USB stick or on the network server.

Note: Data cannot be recovered after deletion.

5.1 Starting the command line tool

Syntax

- xl[volume]

List information for the target volume(s). If no target volume is specified, list info for all volumes.

- xi<volume>

Invalidate the target volume(s), if fully encrypted. The target <volume> must be specified for this command.

- <volume>

Specify the target volume = {a, b, c, ..., z, *}, with <*> meaning all volumes.

- ?, h

Display help.

Options

- -g0

Disable logging mechanism.

- -ga[file]

Logging mode -append. Append log entries at the end of the target log file or create it if it does not exist.

- -gt[file]

Logging mode -truncate. Truncate the target log file if it already exists or create it if it does not exist.

- [file]

Specify the target log file. If not specified the default target log-file is "BEInvVol.log" at the current path. Do not set this file on the same volume to be invalidated!

- -?, -h

Display help.

Examples

beinvvol -h

beinvvol xld

beinvvol xle -gac:\subdir\file.log

beinvvol xl* -gtc:\subdir\file.log

beinvvol xif -gt"c:\my subdir\file.log"

beinvvol xig -g0

beinvvol xi*

6 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.

7 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.