SOPHOS

Security made simple.

SafeGuard Enterprise tools guide

Product version: 8.0

Contents

1 About this guide

This guide explains the use of the encryption tools provided for SafeGuard Enterprise protected endpoints.

You can find the tools in the Tools directory of your SafeGuard Enterprise software delivery. The following tools are provided:

- SGNState tool - display system status
- SGNRollback tool - revert unsuccessful installations
- KeyRecovery tool RecoverKeys.exe - recover access to computers when the POA is corrupt
- Restore tool be_restore.exe - restore Windows 7 SafeGuard disk encryption systems (Master Boot Record)
- Restore tool BLCRBackupRestoren.exe - restore Windows 8 BitLocker Systems (back up ESP contents, restore backup and repair NVRam boot order)
- Decommissioning tool beinvvol.exe - decommission encrypted volumes
- Decommissioning tool opalinvdisk.exe - decommission self-encrypting Opal-compliant hard drives

Intended audience

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

2 Displaying the system status with SGNState

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

Reporting

SGNState can also be used as follows:

- 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 saved to a file.

Parameters

You can call **SGNState** with the following parameters:

SGNState [/?] [/H/Type|Status] [/L] [/LD] [/USERLIST]

- Parameter **/?** returns help information about the available SGNState command-line parameters.
- Parameter **/H Type** returns additional help information about drive types.
- Parameter **/H Status** returns additional help information about drive status.
- Parameter **/L** shows the following information:

  Operating system
  Product version
  Encryption type [SGN | Opal | BitLocker | BitLocker-C/R | unknown or earlier version of SGN]
  Power On Authentication [yes | no | n/a]
  WOL (Wake on LAN status) [yes | no | n/a]
  Server name
  Second Server name
  Logon mode [SGN, no automatic logon | UID/PW | TOKEN/PIN | FINGERPRINT | BL (BitLocker)]
  Client activation state [ENTERPRISE | OFFLINE]
  Last data replication [date, time]
  Enforced cert-based token logon in POA [yes | no | n/a]
  User certificate type [0 | 1 | 2 | 3||n/a|?]
  Return code [return code]

Volume info:

Name	Type	Status	Algorithm
<name>	[HD-Part | ...]	[encrypted | not encrypted | ...]	[<algorithm name> | n/a | ...]
	...	...	
	FLOPPY	not accessible	
	REMOV.PART	stopped because of a failure	
	REM_PART	encryption starting	
	HD-PART	encryption in progress	
	UNKNOWN	decryption starting	
		decryption in progress	
		not prepared	

- Parameter **`/LD`** returns this information formatted for LANDesk.

  The output is similar to the output of **`/L`**, but each line begins with **Sophos SafeGuard**:

  Sophos SafeGuard - Encryption state <name> = [encrypted | not encrypted | not prepared...]

  ...

- If you call **`SGNState`** with parameter **`/USERLIST`**, additionally a list of all users in the UMA and the types of certificates assigned to them is displayed,

  Certificate type:

0	no certificate is assigned to the user
1	P7 certificate (for example Token logon with P12 on SmartCard)
2	P12 certificate
3	P7+P12 certificatee (normal SGN user)
n/a	the certificate type cannot be determined
?	unknown certificate combination

- **Return code**

0	no volume has been encrypted
1	at least one volume is encrypted
-1	an error has occurred (for example, no SafeGuard Enterprise device encryption is installed)

3 Reverting an unsuccessful installation with SGNRollback

Note: SGNRollback should only be used with Windows 7 without BitLocker.

If there is an unsuccessful attempt to install SafeGuard Enterprise on an endpoint, the computer may be unable to boot and may be inaccessible for remote administration.

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

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

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

- Enabling the blocked computer to boot,
- Removing SafeGuard Enterprise and
- Undoing any modifications to other operating system components.

Start SGNRollback from a Windows-based recovery system, either WindowsPE or BartPE.

3.1 Prerequisites

Prerequisites for using SGNRollback:

- 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 see the relevant recovery system documentation for further information.

  If SGNRollback is to be started by autorun, the administrator using SGNRollback has to define the relevant settings in WinPE as described in Enabling SGNRollback autostart for Windows PE (page 8) or BartPE as described in Enabling SGNRollback autostart for BartPE (page 8).

- SafeGuard Enterprise full disk encryption is installed.

Note:

Migration from SafeGuard Easy to SafeGuard Enterprise is not supported.

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

1. Use the BartPEBuilder version 3.1.3 or later to create a PE image. For further details, see 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 SafeGuard Enterprise 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 recovery media.

When booting this image SGNRollback will start automatically.

3.3 Parameters

SGNRollback can be started with the following parameter:

`-drv WinDrive`	Indicates the letter of the drive the SafeGuard Enterprise installation to be repaired is on. This parameter can only be used in recovery mode. It has to be used on multi-boot systems to indicate the correct drive.

3.4 Reverting an unsuccessful installation

To revert the effects of an unsuccessful SafeGuard Enterprise installation on an endpoint:

1. Start 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 SafeGuard Enterprise.
3. You are prompted to remove the recovery media. After you remove the media, the computer will be restarted in safe mode of the operating system.

All modifications are undone and SafeGuard Enterprise is uninstalled.

4 Recovering access to computers with the KeyRecovery tool

The KeyRecovery tool is used to regain access to a computer in a complex recovery situation, for example when the POA is corrupted and the computer needs to be started from the SafeGuard recovery disk. The tool is started in the context of a Challenge/Response procedure.

Note: You can find a detailed description of the tool in the *SafeGuard Enterprise administrator help*, section *Challenge/Response using Virtual Clients*.

5 Restoring Windows BIOS SafeGuard full disk encryption systems

Note: The following description applies to Windows BIOS endpoints with SafeGuard full disk encryption and SafeGuard Power-on Authentication.

SafeGuard Enterprise encrypts files and drives transparently. Boot volumes 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 SafeGuard Enterprise modules are unavailable or do not work.

5.1 Restoring a corrupted MBR

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

Problems with the MBR can be resolved using the SafeGuard Enterprise restore 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.

To restore a corrupted MBR successfully, prepare as follows:

1. We recommend that you create a Windows PE (Preinstalled Environment) CD.
2. To use the restore tool **`be_restore.exe`** several additional files are required. You can find the tool and the required files in your SafeGuard Enterprise software delivery under **`Tools\KeyRecovery and restore`**. Copy all files in this folder to a memory stick. Make sure that you store all of them together in **the same** folder on your memory stick. Otherwise the restore tool will not start properly.

   Note: In order to start **`be_restore.exe`** in a Windows PE environment, the Windows file OLEDLG.dll is required. This file is not included in the **`Tools\KeyRecovery and restore`** folder. Add this file from a Windows installation to the recovery tool folder on your recovery CD.
3. If necessary, adjust the boot sequence in the BIOS and select the CD-ROM to be first.

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

5.2 Restoring a previously saved MBR backup

Every SafeGuard Enterprise endpoint saves its **own computer's** SafeGuard Enterprise MBR (LBA 0 of the boot hard disk after being modified by SafeGuard Enterprise) in the SafeGuard Enterprise Database. It can be exported from the SafeGuard Management Center to a file.

To restore a previously saved MBR backup:

1. In the SafeGuard Management Center, click **Users and Computers** and select the relevant computer in the navigation area.
2. Right-click the computer and select **Properties > Machine Settings > Backup > Export**, to export the MBR. This produces a 512 byte file with the file extension .BKN, which contains the MBR.
3. Copy this file to the folder on the memory stick in which the other extra SafeGuard Enterprise files are located.
4. Now insert the Windows PE Boot CD into the drive, plug in the memory stick with the SafeGuard Enterprise files and switch the computer on to boot from the CD.
5. When the computer is ready, start the cmd-box, navigate to the directory on the memory stick where the SafeGuard Enterprise files are located and run **`be_restore.exe`**.
6. Select **Restore MBR** to restore from a backup and select the .BKN file.

The tool now checks if the selected .BKN file matches the computer and afterwards restores the saved MBR.

5.3 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 SafeGuard Enterprise 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 the SafeGuard Enterprise kernel on the hard disk is searched for.

To use the repair function, prepare as described in Restoring a corrupted MBR (page 11), but 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.

5.4 Partition table

SafeGuard Enterprise allows the creation of new primary or extended partitions. This changes the partition table on the hard disk with the partition.

When restoring an MBR backup, the tool detects 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 select which table to use.

5.4.1 Repairing an MBR with a corrupted partition table

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

You can resolve this problem by 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 the **Restore MBR** option.

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 SafeGuard Enterprise files and switch the computer on to boot from the CD.
2. When the computer is ready, go to the command prompt, navigate to the directory on the memory stick where the SafeGuard Enterprise 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, a dialog for selecting the partition table to be used is displayed.

   The mirrored MBR is the original Microsoft MBR saved during the SafeGuard Enterprise Client setup to enable you to restore it, for example if you uninstall the client. The partition table in this mirrored MBR is being kept up-to-date by SafeGuard Enterprise, if any partition changes occur in Windows.

4. Select **From Mirrored MBR**.

   Important:

   Do not select **From Current MBR**. If you do, the corrupted partition table from the current MBR 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.

5.5 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.

Therefore do not change the Disk Signature, for example by using ("FDISK/MBR"). Otherwise Windows goes into a time-consuming hard disk scan mode during the next startup process and restores the list of drives.

Whenever that occurs under SafeGuard Enterprise, SafeGuard Enterprise'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 SafeGuard Enterprise, the original Windows Disk Signature has to be restored in the hard disk's MBR.

This is done by **be_restore.exe.**

Note: Do not use 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 deleting the Windows Disk Signature, the "new" MBR loader created by an old tool might not be compatible with the hard disk sizes commonly used today. You should always use up-to-date versions of repair tools.

5.6 Boot sector

During the encryption process a volume's boot sector is swapped for the SafeGuard Enterprise boot sector. The SafeGuard Enterprise boot sector holds information about the location and the size of the primary and backup KSA. The location is identified in clusters and sectors referenced from the start of the partition. Even if the SafeGuard Enterprise boot sector is damaged, encrypted volumes cannot be accessed. The be_restore utility can restore the damaged boot sector.

6 Restoring Windows UEFI BitLocker Challenge/Response systems

For restoring Windows UEFI BitLocker systems, Sophos offers the restore tool **`BLCRBackupRestoren.exe`**. With this tool, you can:

- Back up BitLocker Challenge/Response-related data

  Note: This is only necessary if the automatic backup failed (log event 3071: "Key backup could not be saved to the specified network share.")

- Manually restore a previously created backup and repair the NVRAM boot order.

  Note: This is only necessary if you suspect that BitLocker Challenge/Response-related data was corrupted or deleted.

  `BLCRBackupRestoren.exe` needs to be started from a Windows PE environment. It is included on the Sophos Virtual Client CD.

6.1 Starting the command line tool

Syntax

```
blcrbackuprestoren [-?] [-B [-T <Filepath>]] [-R [-K <Filename>] [-S <Filename>]] [-I] [-D]
```

Options

- **`-?`**

  Display help

- **`-B`**

  Backup

- **`-T <Filepath>`**

  Optional existing Target Path

- **`-R`**

  Restore

- **`-K <Filename>`**

  Optional Key Path\Filename

The optional key file is the .BKN file that needs to be exported from the SafeGuard Management Center.

To export it:

- In the SafeGuard Management Center, click **Users and Computers** and select the relevant computer in the navigation area.
- Right-click the computer and select **Properties > Machine Settings > Backup > Export**.

If BitLocker Challenge/Response-related data has been backed up successfully, option **`-R`** is sufficient.

- **`-S <Filename>`**

  Optional Source Path\Filename

- **`-I`**

  Install boot entry.

- **`-D`**

  Delete boot entry.

Note:

If the automatic restore fails, then, in order to use a backup file available on a recovery partition without a drive letter assigned, you need to

- assign a drive letter to the recovery partition
- and then provide the fully-qualified path to the backup file.

There is always only one file: **`<drive-letter>:\SOPHOS\<file name>.cps`**.

Examples

- **Back up**
  - **`blcrbackuprestoren -b`** creates an archive at the default location.
  - **`blcrbackuprestoren -b -T <USBStick drive>:\Backup\`** creates an archive on an external drive.
- **Restore**
  - **`blcrbackuprestoren -r`** extracts the archive from the default location.
  - **`blcrbackuprestoren -r -k X:\example\example.BKN`** extracts the archive from the default location and reconstructs key file.

7 Decommissioning encrypted volumes

For SafeGuard Enterprise-protected computers we provide the command-line tool **beinvvol.exe** which can be used to safely decommission encrypted volumes (hard disks, USB sticks etc.). 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 is intended to be used on computers for which the following applies:

- SafeGuard Enterprise is installed.
- Some hard disk volumes have been encrypted.

You have to run this tool within a system where the SafeGuard Enterprise encryption driver is not active. This is to prevent data from being decommissioned by accident. Otherwise, the tool does not work and an error message is displayed.

Note: We recommend that you start your system from an external medium like a Windows PE CD and use the tool according to the instructions available in the command line help.

After the relevant target volumes have been decommissioned, they are no longer readable.

According to DoD Standard 5220.22-M, the command-line tool permanently purges the boot sectors and the SafeGuard Enterprise 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 SafeGuard Enterprise Clients, the volumes are perfectly sealed afterwards. Even a security officer cannot regain access.

The command-line tool also displays information about the available volumes on screen. This includes, for example, the name of the volume, the size of the volume and information about boot sectors and KSAs. This information can optionally be stored in a file. The path to this file should, of course, point to a volume that is not being decommissioned.

Note: Data cannot be recovered after deletion.

7.1 Starting the command-line tool

Syntax

- **xl[volume]**

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

- **xi<volume>**

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

- **<volume>**

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

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. You must not specify the log file on the volume that is going to be invalidated!

- **-?, -h**

  Display help.

Examples

```
> beinvvol -h
> beinvvol xld
> beinvvol xle -ga"c:\subdir\file.log"
> beinvvol xl* -gt"c:\subdir\file.log"
> beinvvol xif -gt"c:\my subdir\file.log"
> beinvvol xig -g0
> beinvvol xi*
```

8 Decommissioning self-encrypting, Opal-compliant hard drives

Self-encrypting hard drives offer hardware-based encryption of data when they are written to the hard disk. The Trusted Computing Group (TCG) has published the vendor-independent Opal standard for self-encrypting hard drives. SafeGuard Enterprise supports the Opal standard and offers management of endpoints with self-encrypting, Opal-compliant hard drives.

For further information about Opal-compliant hard drives, see the *SafeGuard Enterprise administrator help*, chapter *SafeGuard Enterprise and self-encrypting Opal-compliant hard drives*.

For SafeGuard Enterprise-protected computers we provide the command-line tool **`opalinvdisk.exe`**.

8.1 Prerequisites and recommendations

For using **`opalinvdisk.exe`**, the following prerequisites and recommendations apply:

- Before you use **`opalinvdisk.exe`**, the Opal-compliant hard disk has to be decrypted with the SafeGuard Enterprise **Decrypt** command from the Windows Explorer context menu on the endpoint. For further information, see the *SafeGuard Enterprise administrator help*, section *Enable users to unlock Opal-compliant hard drives* and the *SafeGuard Enterprise user help*, section *System Tray Icon and Explorer extensions on endpoints with Opal-compliant hard drives.*
- You need administrator rights.
- We recommend that you use **`opalinvdisk.exe`** in a Windows PE environment.
- The tool **`opalinvdisk.exe`** starts the optional service **`RevertSP`** with parameter **`KeepGlobalRangeKey`** set to **`False`**. The actual decommissioning procedure carried out by **`RevertSP`** depends on the specific hard drive. For further information, refer to section 5.2.3 of the Opal standard TCG Storage Security Subsystem Class: Opal, Specification Version 1.00, Revision 3.00, which is available at www.trustedcomputinggroup.org.

8.2 Running opalinvdisk.exe

1. Open a command prompt and start **`opalinvdisk.exe`** with administrator rights.

   Tool and usage information is displayed.

2. At the command prompt, enter **`opalinvdisk.exe <TargetDevice>`**.

   For example: **`opalinvdisk.exe PhysicalDrive0`**

If the necessary prerequisites are fulfilled, **RevertSP** is started on the hard drive specified in **<TargetDevice>**. If the prerequisites are not fulfilled or the hard drive does not support **RevertSP**, an error message is displayed.

9 Technical support

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

- Visit the Sophos Community at community.sophos.com/ and search for other users who are experiencing the same problem.
- Visit the Sophos support knowledgebase at www.sophos.com/en-us/support.aspx.
- Download the product documentation at www.sophos.com/en-us/support/documentation.aspx.
- Open a ticket with our support team at https://secure2.sophos.com/support/contact-support/support-query.aspx.

10 Legal notices