SOPHOS
Security made simple.

SafeGuard Enterprise
Tools-Anleitung

Produktversion: 8.0

Inhalt

1 Einleitung

Diese Anleitung beschreibt die Anwendung der Tools, die für durch SafeGuard Enterprise geschützte Endpoints zur Verfügung stehen.

Sie finden die Tools im Tools Verzeichnis Ihrer SafeGuard Enterprise Software-Lieferung. Folgende Tools stehen zur Verfügung:

- SGNState - Anzeigen des Systemstatus
- SGNRollback - Rückgängigmachen von fehlgeschlagenen Installationen
- Schlüssel-Wiederherstellungstool RecoverKeys.exe - Wiederherstellen des Zugriffs auf Computer bei beschädigter POA
- Wiederherstellungstool be_restore.exe - Wiederherstellen von Windows 7 Systemen mit SafeGuard Disk Encryption (Master Boot Record)
- Wiederherstellungstool BLCRBackupRestoren.exe - Wiederherstellen von Windows 8 BitLocker Systemen (Sichern von ESP Inhalten, Wiederherstellen der Sicherung und Reparieren der NVRam Startreihenfolge)
- beinvvol.exe - sicheres Löschen von verschlüsselten Volumes
- opalinvdisk.exe - sicheres Löschen von selbst-verschlüsselnden Opal-Festplatten

Zielgruppe

Die Zielgruppe dieses Handbuchs bilden Administratoren, die mit SafeGuard Enterprise als Sicherheitsbeauftragte arbeiten.

2 Anzeigen des Systemstatus mit SGNState

SafeGuard Enterprise bietet mit **SGNState** ein Kommandozeilentool, das Informationen zum aktuellen Status (Verschlüsselungsstatus sowie weitere detaillierte Statusinformationen) einer SafeGuard Enterprise Installation auf einem Endpoint anzeigt.

Reporting

SGNState kann auch wie folgt verwendet werden:

- Der **SGNState** Rückgabecode kann am Server mit Drittanbieter-Werkzeugen ausgewertet werden.
- **SGNState /LD** gibt die Ausgabe für LANDesk formatiert zurück. Sie kann in einer Datei gespeichert werden.

Parameter

Sie können **SGNState** mit folgenden Parametern aufrufen:

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

- Parameter **/?** gibt Hilfeinformationen zu den verfügbaren SGNState Kommandozeilenparametern zurück.
- Parameter **/H Type** gibt zusätzliche Hilfeinformationen zu Laufwerkstypen zurück.
- Parameter **/H Status** gibt zusätzliche Hilfeinformationen zum Laufwerksstatus zurück.
- Wenn Sie SGNState mit dem Parameter **/L** aufrufen, erhalten Sie folgende Informationen:

  Betriebssystem
  Produktversion
  Verschlüsselungstyp [SGN | Opal | BitLocker | BitLocker-C/R | unbekannte oder frühere Version von SGN]
  Power On Authentication [yes | no | n/a]
  WOL (Wake on LAN status) [yes | no | n/a]
  Servername
  Zweiter Servername
  Anmeldemodus [SGN, no automatic logon | UID/PW | TOKEN/PIN | FINGERPRINT | BL (BitLocker)]
  Aktivierungsstatus des Clients [ENTERPRISE | OFFLINE]
  Letzte Datenreplikation [Datum, Zeit]
  Aktive zertifikatsbasierte Token-Anmeldung in POA [yes | no | n/a]
  Typ des Benutzerzertifikats [0 | 1 | 2 | 3 | n/a | ?]
  Rückgabecode [Rückgabecode]
  Laufwerksinformationen:

Name	Typ	Status	Algorithmus
<Name>	[HD-Part | ...]	[encrypted | not encrypted | ...]	[<Name des Algorithmus> | 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	

- Wenn Sie SGNState mit dem Parameter **/LD** aufrufen, erhalten Sie diese Informationen für LANDesk formatiert.

  Die Ausgabe ist ähnlich zur Ausgabe von **/L**, aber jede Zeile beginnt mit **Sophos SafeGuard**:

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

  ...

- Wenn Sie **SGNState** mit dem Parameter **/USERLIST** aufrufen, erhalten Sie zusätzlich eine Liste aller Benutzer die in der UMA vorhanden sind inklusive den Typen der zugeordneten Zertifikate.

  Zertifikatstyp

0	Dem Benutzer ist noch kein Zertifikat zugeordnet
1	P7 Zertifikat (zum Beispiel Token-Anmeldung mit P12 auf der SmartCard)
2	P12 Zertifikat
3	P7+P12 Zertifikate (normaler SGN-Benutzer)
n/a	Der Zertifikatstyp konnte nicht festgestellt werden
?	unbekannte Zertifikatskombination

- **Rückgabecode:**

0	Kein Volume ist verschlüsselt
1	zumindest ein Volume ist verschlüsselt
-1	Ein Fehler ist aufgetreten (zum Beispiel weil keine SafeGuard Enterprise Device Encryption installiert ist)

3 Fehlgeschlagene Installation mit SGNRollback rückgängig machen

Hinweis: SGNRollback sollte nur mit Windows 7 ohne BitLocker verwendet werden.

Sollte die Installation von SafeGuard Enterprise auf einem Endpoint fehlschlagen, so ist u. U. das Booten des betreffenden Computers nicht mehr möglich und es besteht kein Zugriff für die Remote-Administration.

SGNRollback repariert eine fehlgeschlagene SafeGuard Enterprise Installation auf einem Endpoint, wenn die folgenden Bedingungen zutreffen:

- Während des ersten Boot-Vorgangs nach der Installation blockiert die Power-on Authentication und der Computer kann nicht mehr gestartet werden.
- Die Festplatte ist nicht verschlüsselt.

SGNRollback macht die Auswirkungen einer fehlgeschlagenen Installation von SafeGuard Enterprise wie folgt rückgängig:

- SGNRollback ermöglicht das Booten des gesperrten Computers,
- entfernt SafeGuard Enterprise und
- und macht alle Änderungen an anderen Betriebssystemkomponenten rückgängig.

Starten Sie SGNRollback von einem Windows-basierten Recovery-System aus, WindowsPE oder BartPE.

3.1 Voraussetzungen

Voraussetzungen für die Anwendung von SGNRollback:

- SGNRollback kann auf den Recovery-Systemen WinPE und BartPE angewendet werden. Damit Sie SGNRollback verwenden können, integrieren Sie das Tool in das gewünschte Recovery-System. Weitere Informationen finden Sie in der Dokumentation zum jeweiligen Recovery-System.

  Wenn SGNRollback durch Autorun gestartet werden soll, muss der Administrator, der SGNRollback anwendet, die relevanten Einstellungen in WinPE (siehe Aktivieren von SGNRollback Autostart für Windows PE (Seite 8)) oder BartPE (siehe Aktivieren von SGNRollback Autostart für BartPE (Seite 8)) vornehmen.

- Die Festplattenverschlüsselung von SafeGuard Enterprise ist installiert.

Hinweis:

Die Migration von SafeGuard Easy zu SafeGuard Enterprise wird nicht unterstützt.

3.2 Starten von SGNRollback im Recovery-System

Sie können SGNRollback manuell starten oder es in den Autostart des Recovery-Systems einbinden.

3.2.1 Aktivieren von SGNRollback Autostart für Windows PE

Um den SGNRollback Autostart für Windows PE zu aktivieren, installieren Sie den Microsoft Windows Automated Installation Kit. Das Windows Preinstallation Environment Benutzerhandbuch beschreibt das Erstellen einer Windows PE Umgebung sowie das automatische Starten einer Applikation.

3.2.2 Aktivieren von SGNRollback Autostart für BartPE

1. Erstellen Sie mit BartPEBuilder Version 3.1.3 oder einer neueren Version ein PE Image. Weitere Informationen hierzu finden Sie in der BartPE Dokumentation.
2. Fügen Sie im BartPE Builder das Recovery Tool Verzeichnis im Feld **Custom** hinzu.
3. Erstellen Sie das Image.
4. Kopieren Sie die Datei AutoRun0Recovery.cmd vom SafeGuard Enterprise Medium in das Verzeichnis i386 der mit BartPE vorbereiteten Windows-Version.
5. Erstellen Sie eine AutoRun0Recovery.cmd mit den folgenden beiden Textzeilen:

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

6. Starten Sie das PEBuilder Tool von der Befehlszeile aus:

   ```
   Pebuilder -buildis
   ```

   Es wird eine neues ISO Image erstellt, das die Autorun-Datei enthält.

7. Speichern Sie das resultierende Image auf einem Recovery-Medium.

Wenn Sie dieses Image booten, wird SGNRollback automatisch gestartet.

3.3 Parameter

SGNRollback kann mit folgendem Parameter gestartet werden:

`-drv WinDrive`	Der Buchstabe des Laufwerks, auf dem sich die zu reparierende SafeGuard Enterprise Installation befindet. Dieser Parameter kann nur im Recovery-Modus verwendet werden. Er muss bei Multi-Boot-Systemen verwendet werden, um das korrekte Laufwerk anzugeben.

3.4 Fehlgeschlagene Installation mit SGNRollback rückgängig machen

Um die Auswirkungen einer fehlgeschlagenen SafeGuard Enterprise Installation auf einem Endpoint rückgängig zu machen, gehen Sie wie folgt vor:

1. Starten Sie den Computer von dem Recovery-Medium, das das Recovery-System einschließlich SGNRollback enthält.
2. Starten Sie SGNRollback im Recovery-System. Wurden für SGNRollback Autorun-Einstellungen definiert, startet das Tool automatisch. SGNRollback bereitet das Betriebssystem für die Deinstallation von SafeGuard Enterprise vor.
3. Sie werden nun dazu aufgefordert, das Recovery-Medium zu entfernen. Danach wird der Computer im abgesicherten Modus des Betriebssystems neu gestartet.

Alle vorgenommenen Änderungen werden rückgängig gemacht und SafeGuard Enterprise wird deinstalliert.

4 Wiederherstellen des Zugriffs auf Computer mit dem KeyRecovery Tool

Das KeyRecovery Tool dient zum Wiederherstellen des Zugriffs auf einen Computer in komplexen Recovery-Szenarien, z. B. wenn die Power-on Authentication beschädigt ist und der Computer von der SafeGuard Recovery Disk gestartet werden muss. Das Tool wird im Rahmen eines Challenge/Response Vorgangs gestartet.

Hinweis: Eine detaillierte Beschreibung des Tools finden Sie in der *SafeGuard Enterprise Administratorhilfe* im Abschnitt *Challenge/Response mit virtuellen Clients*.

5 Wiederherstellen von mit SafeGuard Festplattenverschlüsselung verschlüsselten Windows BIOS Systemen

Hinweis: Die folgende Beschreibung bezieht sich auf Windows BIOS Endpoints mit SafeGuard Festplattenverschlüsselung und SafeGuard Power-on Authentication.

SafeGuard Enterprise verschlüsselt Dateien und Laufwerke transparent. Darüber hinaus können auch Boot-Volumes verschlüsselt werden, so dass Entschlüsselungsfunktionalitäten wie Code, Verschlüsselungsalgorithmen und Verschlüsselungsschlüssel sehr früh in der Bootphase verfügbar sein müssen. Folglich kann auf verschlüsselte Informationen nicht zugegriffen werden, wenn entscheidende SafeGuard Enterprise Module nicht verfügbar sind oder nicht funktionieren.

5.1 Wiederherstellen eines beschädigten MBR

Die Power-on Authentication von SafeGuard Enterprise wird aus dem MBR einer Festplatte eines Computers geladen. Bei der Installation speichert SafeGuard Enterprise eine Kopie des Originals – in ihrem Zustand vor der Installation von Sophos SafeGuard – in seinem Kernel und modifiziert den PBR Loader von LBA 0. Der modifizierte MBR enthält bei LBA 0 die Adresse des ersten Sektors des SafeGuard Enterprise Kernels sowie seine Gesamtgröße.

Probleme mit dem MBR können mit dem SafeGuard Enterprise Tool **`be_restore.exe`** gelöst werden. Dieses Tool ist eine Win32-Anwendung und muss unter Windows laufen – nicht unter DOS.

Ein fehlerhafter MBR Loader verursacht ein unbootbares System. Er kann auf zwei Arten wiederhergestellt werden:

- Wiederherstellen des MBR aus einer Sicherungskopie,
- Reparatur des MBR

So stellen Sie einen beschädigen MBR wieder her:

1. Es wird empfohlen, eine Windows PE (Preinstalled Environment) CD zu erstellen.
2. Um das Tool **`be_restore.exe`** zu verwenden, werden einige zusätzliche Dateien benötigt. Sie finden das Tool sowie die benötigten Dateien in Ihrer SafeGuard Enterprise Software-Lieferung im Verzeichnis **`Tools\KeyRecovery and restore`**. Kopieren Sie alle Dateien in diesem Ordner auf einen USB-Stick. Legen Sie alle Dateien im **selben** Verzeichnis auf dem USB-Stick ab. Andernfalls kann das Tool nicht erfolgreich gestartet werden.

   Hinweis: Zum Starten von **`be_restore.exe`** in einer Windows PE-Umgebung ist die Windows-Datei OLEDLG.dll erforderlich. Diese Datei ist nicht im Ordner **`Tools\KeyRecovery and restore`** enthalten. Fügen Sie diese Datei aus einer Windows-Installation zum Recovery Tool Ordner auf Ihrer Recovery-CD hinzu.

3. Falls notwendig, passen Sie die Startreihenfolge im BIOS an und wählen Sie CD-ROM an erste Stelle.

Hinweis: Mit **be_restore.exe** lässt sich nur der MBR auf Disk 0 reparieren. Wenn Sie zwei Festplatten verwenden und das System von der anderen Festplatte gestartet wird, ist eine Wiederherstellung bzw. Reparatur nicht möglich. Dies ist auch der Fall, wenn Sie eine externe Festplatte verwenden.

5.2 Wiederherstellen einer zuvor gespeicherten MBR-Sicherung

Jeder SafeGuard Enterprise Endpoint speichert seinen **computereigenen** SafeGuard Enterprise MBR (LBA 0 der Boot-Festplatte nach der Modifizierung durch SafeGuard Enterprise) in der SafeGuard Enterprise Datenbank. Er kann aus dem SafeGuard Management Center in eine Datei exportiert werden.

Wiederherstellen einer zuvor gespeicherten MBR-Sicherung:

1. Klicken Sie im SafeGuard Management Center auf **Benutzer & Computer** und markieren Sie den betreffenden Computer im Navigationsbereich.
2. Klicken Sie mit der rechten Maustaste auf den Computer und wählen Sie **Eigenschaften > Computereinstellungen > Sicherung > Exportieren**, um den MBR zu exportieren. Das Ergebnis ist eine 512 Bytes große Datei mit der Dateinamenerweiterung .BKN, die den MBR enthält.
3. Kopieren Sie diese Datei und fügen Sie sie zu den anderen SafeGuard Enterprise Dateien auf dem USB-Stick hinzu.
4. Legen Sie nun die Windows PE Boot CD in das CD-Laufwerk ein, stecken Sie den USB-Stick ein und schalten Sie den Computer ein, um den Computer von der CD zu booten.
5. Wenn der Computer bereit ist, wechseln Sie im cmd-Dialog auf dem USB-Laufwerk in den Ordner, in dem sich die SafeGuard Enterprise Dateien befinden, und starten Sie **be_restore.exe**.
6. Wählen Sie **Restore MBR** für die Wiederherstellung aus einer Sicherungskopie und wählen Sie danach die .BKN-Datei aus.

Das Tool überprüft nun, ob die ausgewählte .BKN-Datei mit dem Computer übereinstimmt und stellt danach den gespeicherten MBR wieder her.

5.3 Reparatur des MBR ohne Sicherungskopie

Auch wenn lokal keine MBR-Backup Datei verfügbar ist, kann ein beschädigter MBR Loader von **be_restore.exe** repariert werden. **be_restore.exe** - **Repair MBR** lokalisiert den SafeGuard Enterprise Kernel auf der Festplatte, verwendet seine Adresse und erstellt den MBR Loader neu.

Das ist sehr vorteilhaft, zumal keine computerspezifische MBR-Backupdatei lokal vorhanden sein muss. Dieser Vorgang nimmt jedoch etwas mehr Zeit in Anspruch, da nach dem SafeGuard Enterprise Kernel auf der Festplatte gesucht wird.

Um die Reparatur-Funktion zu verwenden, treffen Sie die unter Wiederherstellen eines beschädigten MBR (Seite 11) Vorbereitungen, wählen aber **Repair MBR** beim Ausführen von **be_restore.exe** aus.

Werden mehrere Kernel gefunden, so verwendet **be_restore.exe** – **Repair MBR** den Kernel mit dem aktuellsten Zeitstempel.

5.4 Partitionstabelle

SafeGuard Enterprise erlaubt das Anlegen von neuen primären oder erweiterten Partitionen. Das ändert die Partitionstabelle auf der Festplatte mit der Partition.

Während der Wiederherstellung eines MBR Backups entdeckt das Tool, dass der aktuelle MBR bei LBA 0 und die wiederherzustellende MBR Backupdatei (*.BKN) verschiedene Partitionstabellen enthalten. In einem Dialog kann der Benutzer die Tabelle auswählen, die verwendet werden soll.

5.4.1 Reparatur eines MBR mit einer beschädigten Partitionstabelle

Eine beschädigte Partitionstabelle kann dazu führen, dass das Betriebssystem nach einer erfolgreichen POA-Anmeldung nicht gebootet werden kann.

Zur Behebung dieses Problems können Sie mit be_restore.exe eine zuvor gespeicherte MBR-Sicherung wiederherstellen oder den MBR ohne MBR-Sicherung reparieren.

Wenn Sie über eine Sicherung verfügen, gehen Sie wie für die Option **Restore MBR** beschrieben vor.

Wenn Sie keine Sicherung haben, gehen Sie wie folgt vor:

1. Legen Sie die Windows PE Boot CD ein, stecken Sie den USB Stick mit den SafeGuard Enterprise Dateien ein und schalten Sie den Computer ein, um von der CD zu booten.
2. Wenn der Computer bereit ist, wechseln Sie in der Eingabeaufforderung auf dem USB-Laufwerk in den Ordner, in dem sich die SafeGuard Enterprise Dateien befinden, und starten Sie **be_restore.exe**.
3. Wählen Sie **Repair MBR**. Wenn be_restore.exe einen Unterschied zwischen der Partitionstabelle des aktuellen MBR und des gespiegelten MBR entdeckt, wird ein Dialog zur Auswahl der zu verwendenden Partitionstabelle angezeigt.

   Bei dem gespiegelten MBR handelt es sich um den Original Microsoft MBR, der während der Konfiguration des SafeGuard Enterprise Client für die Wiederherstellung, z. B. bei einer Deinstallation des Client, gespeichert wird. Die Partitionstabelle in diesem gespiegelten MBR wird durch SafeGuard Enterprise aktualisiert, wenn in Windows Partitionsänderungen auftreten.

4. Wählen Sie **From Mirrored MBR**.

   Wichtig:

   Wählen Sie nicht **From Current MBR** aus, da sonst die beschädigte Tabelle aus dem aktuellen MBR verwendet wird. In diesem Fall kann das System weiterhin nicht gebootet werden. Darüber hinaus wird der gespiegelte MBR aktualisiert und wird somit auch korrupt.

5.5 Windows Disk Signature

Wann immer Windows auf einer Festplatte zum ersten Mal ein Dateisystem anlegt, erstellt es eine Signatur für diese Festplatte. Diese Signatur ist im MBR der Festplatte bei den Offsets 0x01B – 0x01BB gespeichert. Beachten Sie, dass beispielsweise die logischen Laufwerksbuchstaben der Festplatte von der Windows Disk Signature abhängen.

Deshalb ändern Sie nicht die Disk Signature, beispielsweise mit ("FDISK/MBR"). Andernfalls schaltet Windows beim nächsten Starten in einen aufwändigen Festplatten-Scan-Modus und stellt die Liste der Laufwerke wieder her.

Wann immer das unter SafeGuard Enterprise passiert, wird der Filtertreiber “BEFLT.sys” von SafeGuard Enterprise nicht geladen. Das verursacht ein nicht bootbares System: Der Computer zeigt einen Bluescreen ‘STOP 0xED “Unmountable Boot Volume”‘.

Um das unter SafeGuard Enterprise zu reparieren, muss die original Windows Disk Signature im MBR der Festplatte wiederhergestellt werden.

Das wird auch **`be_restore.exe`** erledigt.

Hinweis: Verwenden Sie kein anderes Tool um den MBR zu reparieren. Beispielsweise eine alte MS DOS FDISK.exe, die Sie zum erneuten Schreiben des MBR Loaders (“FDISK /MBR”) verwenden, könnte einen anderen MBR Loader ohne Windows Disk Signatur erstellen. Genauso wie er die Windows Disk Signature löscht, könnte der "neue" MBR Loader, der von einem alten Tool erstellt wurde, mit den heutigen Festplattengrößen nicht zurechtkommen. Bitte benutzen Sie immer aktuelle Versionen von Reparaturwerkzeugen.

5.6 Bootsektor

Der Bootsektor eines Volumes wird bei der Verschlüsselung gegen den SafeGuard Enterprise Bootsektor ausgetauscht. Der SafeGuard Enterprise Bootsektor enthält Informationen zu Speicherort und Größe des primären KSA und des Backup-KSA in Clustern und Sektoren bezogen auf den Beginn der Partition. Auch wenn der SafeGuard Enterprise Bootsektor zerstört ist, ist kein Zugriff auf verschlüsselte Volumes möglich. Das Tool be_restore kann den zerstörten Bootsektor wiederherstellen.

6 Wiederherstellen von Windows UEFI BitLocker Challenge/Response Systemen

Für die Wiederherstellung vom Windows UEFI BitLocker Systemen bietet Sophos das Wiederstellungstool **`BLCRBackupRestoren.exe`**. Mit diesem Werkzeug können Sie:

- BitLocker Challenge/Response bezogene Daten sichern.

  Hinweis: Das ist nur notwendig, wenn die automatische Sicherung fehlschlägt. (Log Event 3071: "Schlüssel-Backup konnte nicht auf der angegebenen Netzwerkfreigabe gespeichert werden.")

- Eine frühere Sicherung manuell wiederherstellen und die NVRAM Bootreihenfolge reparieren.

  Hinweis: Das ist nur notwendig, wenn Sie vermuten, dass BitLocker Challenge/Response-bezogene Daten beschädigt oder gelöscht wurden.

  `BLCRBackupRestoren.exe` muss von einer Windows PE Umgebung gestartet werden. Es ist auf der Sophos Virtual Client CD enthalten.

6.1 Aufruf des Kommandozeilen-Tools

Syntax

```
blcrbackuprestoren [-?] [-B [-T <Dateipfad>]] [-R [-K <Dateiname>]
[-S <Dateiname>]] [-I] [-D]
```

Optionen

- **`-?`**

  Hilfe anzeigen

- **`-B`**

  Backup (Sicherung)

- **`-T <Dateipfad>`**

  Optional existierender Zielpfad

- **`-R`**

  Restore (Wiederherstellen)

- **`-K <Dateiname>`**

  Optionaler Schlüssel Pfad\Dateiname

Die optionale Schlüsseldatei ist die .BKN Datei, die aus dem SafeGuard Management Center zu exportieren ist.

Um sie zu exportieren:

- Klicken Sie im SafeGuard Management Center auf **Benutzer & Computer** und markieren Sie den betreffenden Computer im Navigationsbereich.
- Klicken Sie mit der rechten Maustaste auf den Computer und wählen Sie **Eigenschaften > Computereinstellungen > Sicherung > Exportieren**.

Wenn BitLocker Challenge/Response-bezogene Daten erfolgreich gesichert wurden, ist die Option **`-R`** ausreichend.

- **`-S <Dateiname>`**

  Optionale Quelle Pfad\Dateiname

- **`-I`**

  Booteintrag installieren.

- **`-D`**

  Booteintrag löschen.

Hinweis:

Schlägt die automatische Wiederherstellung fehl, führen Sie die nachfolgenden Schritte aus, um eine auf einer Recovery Partition ohne zugewiesenen Laufwerksbuchstaben verfügbare Backup-Datei zu verwenden:

- Weisen Sie der Recovery Partition einen Laufwerksbuchstaben zu
- und geben Sie den absoluten Pfad zu der Backup-Datei an.

Es gibt immer nur eine Datei: **`<Laufwerksbuchstabe>:\SOPHOS\<Dateiname>.cps`**.

Beispiele

- **Sichern**
  - **`blcrbackuprestoren -b`** erstellt ein Archiv am Standardspeicherort.
  - **`blcrbackuprestoren -b -T <USBStick Laufwerk>:\Backup\`**legt ein Archiv auf einem externen Laufwerk an.
- **Restore (Wiederherstellen)**
  - **`blcrbackuprestoren -r`** extrahiert das Archiv vom Standardspeicherort.
  - **`blcrbackuprestoren -r -k X:\example\example.BKN`** extrahiert das Archiv vom Standardspeicherort und rekonstruiert die Schlüsseldatei.

7 Sicheres Löschen von verschlüsselten Volumes

Auf Computern mit SafeGuard Enterprise ermöglicht das Kommandozeilen-Tool **`beinvvol.exe`** das sichere Löschen von verschlüsselten Volumes (Festplatten, USB-Sticks usw.). Unser Kommandozeilen-Tool basiert auf dem DoD Standard 5220.22-M, mit dem das sichere Löschen von Schlüsselspeichern durchgeführt werden kann. Dieser Standard umfasst das siebenmalige Überschreiben mit zufälligen und alternativen Mustern.

Das Kommandozeilen-Tool kann auf Computern benutzt werden, für die Folgendes gilt:

- SafeGuard Enterprise ist installiert.
- Einige Volumes auf der Festplatte sind verschlüsselt.

Sie müssen dieses Tool in einem System ausführen, in dem der SafeGuard Enterprise Verschlüsselungstreiber nicht aktiv ist. Dadurch wird verhindert, dass Daten unbeabsichtigt gelöscht werden. Andernfalls funktioniert das Tool nicht und es wird eine Fehlermeldung angezeigt.

Hinweis: Wir empfehlen, Ihr System von einem externen Medium, z. B. einer Windows PE CD, zu starten und das Tool gemäß den Anweisungen der Kommandozeilen-Hilfe anzuwenden.

Nach dem sicheren Löschen der entsprechenden Ziel-Volumes sind diese nicht mehr lesbar.

Gemäß DoD Standard 5220.22-M löscht das Kommandozeilen-Tool die Boot-Sektoren und die SafeGuard Enterprise Key Storage Areas (Orginal-KSA und Sicherheitskopie) der einzelnen verschlüsselten Volumes durch siebenmaliges Überschreiben. Da keine Sicherungskopien der Data Encryption Keys der einzelnen Volumes in der SafeGuard Enterprise Datenbank gespeichert sind, sind die Volumes nach der Anwendung des Kommandozeilen-Tools vollständig abgeriegelt. Auch für Sicherheitsbeauftragte ist kein Zugriff mehr möglich.

Das Kommandozeilen-Tool gibt am Bildschirm noch Informationen über die Löschung aus. Unter anderem werden Name und Größe des Volumes sowie Informationen zu Boot-Sektoren und KSAs angezeigt. Diese Informationen können nach Wunsch in einer Datei gespeichert werden. Der Pfad zu dieser Datei sollte natürlich auf ein Volume verweisen, das nicht in den Löschvorgang einbezogen ist.

Hinweis: Nach dem Löschen können die Daten nicht wiederhergestellt werden.

7.1 Aufruf des Kommandozeilen-Tools

Syntax

- **`xl[volume]`**

  Zeigt Informationen über das/die Ziel-Volume(s) an. Wird kein Ziel-Volume angegeben, werden Informationen zu allen vorhandenen Volumes angezeigt.

- **`xi<volume>`**

  Zerstört das/die Ziel-Volume(s) wenn es/sie mit SafeGuard Enterprise verschlüsselt ist/sind. Das Ziel <Volume> muss für dieses Kommando angegeben werden.

- **<volume>**

  Gibt das Ziel-Volume = {a, b, c, ..., z, *} an.<*> steht für alle Volumes.

Optionen

- **-g0**

  Schaltet die Protokollierung aus.

- **-ga[file]**

  Protokollierungsmodus -append. Fügt die Einträge am Ende der Zieldatei ein oder erzeugt eine neue Datei wenn keine Protokollierungsdatei existiert.

- **-gt[file]**

  Logging mode -truncate. Kürzt die Ziel-Protkollierungsdatei, wenn bereits vorhanden. Andernfalls wird sie angelegt.

- **[file]**

  Gibt die Protokollierungsdatei an. Wird keine Datei angegeben, wird als Standarddatei "BEInvVol.log" unter dem aktuellen Pfad erzeugt. Sie dürfen die Protokollierungsdatei nicht auf dem Volume angeben, das zerstört wird!

- **-?, -h**

  Zeigt die Hilfe an.

Beispiele

```
> 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 Sicheres Löschen von selbst-verschlüsselnden Opal-Festplatten

Selbst-verschlüsselnde Festplatten bieten hardware-basierende Verschlüsselung der Daten, die auf die Festplatte geschrieben werden. Die Trusted Computing Group (TCG) hat den anbieter-unabhängigen Opal-Standard für selbst-verschlüsselnde Festplatten veröffentlicht. SafeGuard Enterprise unterstützt den Opal-Standard und bietet die Verwaltung von Endpoints mit selbst-verschlüsselnden Festplatten, die dem Opal-Standard entsprechen.

Weitere Informationen zu Opal-Festplatten finden Sie in der *SafeGuard Enterprise Administratorhilfe* im Kapitel *SafeGuard Enterprise und selbst-verschlüsselnde Opal-Festplatten*.

Für durch SafeGuard Enterprise geschützte Computer steht das Tool **`opalinvdisk.exe`** zur Verfügung.

8.1 Voraussetzungen und Empfehlungen

Für die Anwendung von **`opalinvdisk.exe`** gelten folgende Voraussetzungen und Empfehlungen:

- Vor der Anwendung von **`opalinvdisk.exe`** muss die Opal-Festplatte mit dem SafeGuard Enterprise Befehl **Entschlüsseln** aus dem Windows Explorer Kontextmenü auf dem Endpoint entsperrt werden. Weitere Informationen finden Sie in der *SafeGuard Enterprise Administratorhilfe* im Abschnitt *Berechtigung von Benutzern zum Entsperren von Opal-Festplatten* sowie in der SafeGuard Enterprise Benutzerhilfe im Abschnitt *System Tray Icon und Explorer-Erweiterungen auf Endpoints mit Opal-Festplatten.*
- Sie benötigen Administratorrechte.
- Wir empfehlen, **`opalinvdisk.exe`** in einer Windows PE Umgebung anzuwenden.
- Das Tool **`opalinvdisk.exe`** startet den optionalen Service **`RevertSP`** mit dem Parameter **`KeepGlobalRangeKey`** in der Einstellung **`False`**. Der durch **`RevertSP`** durchgeführte, eigentliche Löschvorgang ist von der jeweiligen Festplatte abhängig. Weitere Informationen finden Sie in Abschnitt 5.2.3 des Opal-Standards TCG Storage Security Subsystem Class: Opal, Specification Version 1.00, Revision 3.00 (verfügbar auf www.trustedcomputinggroup.org).

8.2 Ausführen von opalinvdisk.exe

1. Öffnen Sie eine Eingabeaufforderung und starten Sie **`opalinvdisk.exe`** mit Administratorrechten.

   Informationen zum Tool und seiner Anwendung werden angezeigt.

2. Geben Sie in die Eingabeaufforderung **opalinvdisk.exe <TargetDevice>** ein.

   Zum Beispiel: **opalinvdisk.exe PhysicalDrive0**

Wenn die notwendigen Voraussetzungen erfüllt sind, wird auf der in **<TargetDevice>** angegebenen Festplatte **RevertSP** gestartet. Sind die Voraussetzungen nicht erfüllt, oder unterstützt die Festplatte **RevertSP** nicht, so wird eine Fehlermeldung angezeigt.

9 Technischer Support

Technischen Support zu Sophos Produkten finden Sie hier:

- Besuchen Sie die Sophos Community unter community.sophos.com/ und suchen Sie nach Benutzern mit dem gleichen Problem.
- Besuchen Sie die Sophos Support-Knowledgebase unter www.sophos.com/de-de/support.aspx.
- Laden Sie die Produktdokumentation herunter unter www.sophos.com/de-de/support/documentation.aspx.
- Öffnen Sie ein Ticket bei unserem Support-Team unter https://secure2.sophos.com/de-de/support/contact-support/support-query.aspx.

10 Rechtliche Hinweise