

SOPHOS

simple + secure

SafeGuard Enterprise Tools-Anleitung

Produktversion: 5.60
Stand: April 2011



Inhalt

1	Einleitung.....	3
2	Anzeigen des Systemstatus mit SGNState.....	4
3	Fehlgeschlagene Installation mit SGNRollback rückgängig machen.....	5
4	Systemwiederherstellung mit dem Recovery Tool BE_Restore.exe.....	8
5	Sicheres Löschen von verschlüsselten Volumes mit BEInvVol.exe.....	12
6	Sicheres Löschen von selbst-verschlüsselnden Opal-Festplatten.....	14
7	Technischer Support.....	16
8	Rechtliche Hinweise.....	17

1 Einleitung

Dieses Handbuch beschreibt die Anwendung der SafeGuard Enterprise Tools, die Sie im tools Verzeichnis Ihrer SafeGuard Enterprise Software-Lieferung finden.

Die folgenden Tools sind im Handbuch beschrieben:

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

Hinweis:

Im tools Verzeichnis Ihrer Client Software-Lieferung finden Sie zusätzlich noch das Tool Recover Keys (RecoverKeys.exe). Dieses Tool dient zum Starten eines Challenge/Response Vorgangs in komplexen Recovery-Szenarien, z. B. wenn die Power-on Authentication beschädigt ist und der Computer von der SafeGuard Recovery Disk gebootet werden muss. Das Tool ist bereits auf der Recovery Disk enthalten und steht zusätzlich im tools Verzeichnis zur Verfügung. Eine detaillierte Beschreibung des Tools und seiner Anwendung für Recovery-Vorgänge finden Sie in der SafeGuard Administrator Hilfe unter dem Stichwort Challenge/Response mit virtuellen Clients.

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-Computer anzeigt.

Sie finden das Tool SGNState im tools Verzeichnis des SafeGuard Enterprise Client Software-Ordners.

Reporting

SGNState kann auch zu Reporting-Zwecken genutzt werden:

- Der Return Code von SGNState kann serverseitig von Third-Party Management Tools ausgewertet werden.
- SGNState /LD liefert eine für LANDesk formatierte Ausgabe, die in eine Datei umgeleitet werden kann.

Parameter

SGNState kann mit folgenden Parametern aufgerufen werden:

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

- Wenn Sie SGNState mit dem Parameter /? aufrufen, erhalten Sie Hilfeinformationen zu den verfügbaren SGNState Kommandozeilenparametern.
- Wenn Sie SGNState mit dem Parameter /L aufrufen, erhalten Sie folgende Informationen:
 - Betriebssystem
 - Installierte SafeGuard Enterprise Version
 - POA-Typ (BitLocker oder SafeGuard Enterprise)
 - POA-Status (an/aus)
 - Wake on LAN Status (an/aus)
 - Servername
 - Anmeldemodus
 - Datum (und Uhrzeit) der letzten Datenreplikation
 - Verschlüsselungsstatus (verschlüsselt/nicht verschlüsselt), für die einzelnen Volumes verwendeter Algorithmus
- Wenn Sie SGNState mit dem Parameter /LD aufrufen, erhalten Sie diese Informationen für LANDesk formatiert.

3 Fehlgeschlagene Installation mit SGNRollback rückgängig machen

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

Für Notfälle dieser Art bietet SafeGuard Enterprise das Tool SGNRollback.

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

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

SGNRollback steht als Programm im tools Verzeichnis des SafeGuard Enterprise Admin Software-Ordners zur Verfügung und wird von einem Windows-basierenden Recovery-System (Windows PE oder BartPE) aus gestartet.

3.1 Anwendungsszenario

SGNRollback repariert eine fehlgeschlagene SafeGuard Enterprise Installation auf einem Endpoint-Computer, 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.

Hinweis:

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

Weitere Voraussetzungen

Für die Anwendung von SGNRollback gelten folgende weitere Voraussetzungen:

- 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 6)) oder BartPE ([siehe Aktivieren von SGNRollback Autostart für BartPE](#) (Seite 6)) definieren.

- SafeGuard Enterprise Device Encryption ist installiert.

Unterstützte Betriebssysteme

SGNRollback unterstützt die folgenden Betriebssysteme:

- Windows XP
- Windows Vista
- Windows 7

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

Um den SGNRollback Autostart für BartPE zu aktivieren, gehen Sie wie folgt vor:

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 ein 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 Umgebungen eingesetzt 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-Computer rückgängig zu machen, gehen Sie wie folgt vor:

1. Booten 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 Systemwiederherstellung mit dem Recovery Tool BE_Restore.exe

Der Bootprozess von SafeGuard Enterprise

SafeGuard Enterprise verschlüsselt Dateien und Laufwerke transparent. Darüber hinaus können auch Bootlaufwerke 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.

4.1 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 MBR 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 Recovery-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 beschädigten MBR wieder her:

1. Es wird empfohlen, eine Windows PE (Preinstalled Environment) CD zu erstellen.
2. Um das Client Recovery-Tool **BE_Restore.exe** zu verwenden, werden einige zusätzliche Dateien benötigt. Sie finden das Tool sowie die benötigten Dateien im Client Software-Ordner im Verzeichnis **toolsKeyRecovery** and **Restore**. Kopieren Sie alle Dateien in diesem Ordner auf einen USB-Stick. Kopieren Sie alle Dateien in diesem Verzeichnis in **dasselbe** Verzeichnis auf einen USB-Stick. Andernfalls kann das Recovery- Tool nicht erfolgreich gestartet werden.
3. Falls notwendig, passen Sie die Bootreihenfolge im BIOS an und wählen Sie die Windows PE Boot-CD an die erste Position.

Hinweis:

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

4.1.1 Wiederherstellen einer zuvor gespeicherten MBR-Sicherung

Jeder SafeGuard Enterprise Client 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.

So stellen Sie den MBR aus einer zuvor gespeicherten Sicherungskopie wieder her:

1. Klicken Sie im SafeGuard Management Center auf **Benutzer & Computer** und markieren Sie den betreffenden Computer im Navigationsbereich.
2. Wählen Sie im Kontextmenü des Computers (Rechtsklick) **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.

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

4.1.2 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 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. Jedoch benötigt es etwas mehr Zeit, weil **BE_Restore.exe - Repair MBR** eine aufwändige Suche nach dem Sophos SafeGuard Kernel auf der Festplatte durchführen muss.

Um die Reparatur-Funktion zu verwenden, gehen Sie wie beschrieben vor und wählen Sie beim Ausführen von **BE_Restore.exe** die Option **Repair MBR**.

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

4.1.3 Partitionstabelle

SafeGuard Enterprise erlaubt das Anlegen von neuen primären oder erweiterten Partitionen. Dies verursacht eine veränderte Partitionstabelle der Festplatte, auf der sich die Partition befindet.

Während der Wiederherstellung eines MBR Backups bemerkt BE_Restore, dass der aktuelle MBR bei LBA 0 und die wiederherzustellende MBR Backupdatei (*.BKN) verschiedene Partitionstabellen enthalten. Sie können in einem Dialog die erforderliche Vorgehensweise bestimmen.

4.1.3.1 Reparatur eines MBR mit einer korrupten Partitionstabelle

Eine korrupte 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**.

Hinweis:

Wenn Sie die Option **From Current MBR** wählen, wird die Partitionstabelle des aktuellen MBR, d.h. in diesem Fall eine korrupte Partitionstabelle, verwendet. In diesem Fall kann das System weiterhin nicht gebootet werden. Darüber hinaus wird der gespiegelte MBR aktualisiert und wird somit auch korrupt.

4.1.4 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.

Beispiel: Der Windows Administrator benutzt den Windows Festplatten-Manager um die logischen Laufwerksbuchstaben der Laufwerke C:, D:, und E: in C:, F:, und Q zu ändern. Dabei wird die Windows Disk Signature aus dem MBR der Festplatte gelöscht. Nach dem nächsten Startvorgang fällt Windows in einen aufwändigen Festplatten-Scan Modus und stellt die Liste

der Laufwerke wieder her. Als Ergebnis besitzen die drei Laufwerke wieder ihre originalen Laufwerksbuchstaben C:, D: und E:.

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 von **BE_Restore.exe** erledigt.

Hinweis:

Sie sollten mit jedem anderen Werkzeug zur Reparatur des MBR sehr vorsichtig sein! 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. Neben der Tatsache, dass ein altes Werkzeug die Windows Disk Signatur löscht, kann es auch möglich sein, dass der „neue“ MBR Loader mit den heute üblichen Festplattengrößen nicht zurecht kommt. Bitte benutzen Sie immer aktuelle Versionen von Reparaturwerkzeugen.

5 Sicheres Löschen von verschlüsselten Volumes mit BEInvVol.exe

Für SafeGuard Enterprise geschützte Computer steht das Kommandozeilen-Tool **BEInvVol.exe** zur Verfügung, mit dem das sichere Löschen von verschlüsselten Volumes (Festplatten, USB-Sticks usw.) ermöglicht wird. 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 per Zufall 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 (Original-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.

5.1 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.<*> für alle Volumes.

Optionen

■ **-g0**

Schaltet die Protokollierung aus.

■ **-ga[file]**

Protokollierungsmodus anhängen. Fügt die Einträge am Ende der Zielfeile ein oder erzeugt eine neue Datei wenn keine Protokollierungsdatei existiert.

■ **-gt[file]**

Logging mode -truncate. Kürzt die Ziel-Protokollierungsdatei, 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. Erzeugen Sie diese Datei nicht auf demselben Volume, das Sie unbrauchbar machen wollen.

■ **-?, -h**

Zeigt die Hilfe an.

Beispiele

> **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 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 Endpoint-Computern mit selbst-verschlüsselnden Festplatten, die dem Opal-Standard entsprechen.

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

Für SafeGuard Enterprise geschützte Computer steht das Kommandozeilen-Tool **opalinvdisk.exe** zur Verfügung. Dieses Tool startet einen optionalen Service von Opal-Festplatten (**RevertSP** mit Parameter **KeepGlobalRangeKey** in der Einstellung **False**). **RevertSP** löscht Opal-Festplatten sicher durch Wiederherstellen des Originalzustands und Löschen der Schlüssel. Weitere Informationen zu **RevertSP** 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).

6.1 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-Computer entsperrt werden. Weitere Informationen finden Sie in der SafeGuard Enterprise Administrator-Hilfe 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 Endpoint-Computern 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).

6.2 Ausführen von **opalinvdisk.exe**

1. Öffnen Sie eine Kommandozeile und starten Sie **opalinvdisk.exe** mit Administratorrechten. Informationen zum Tool und seiner Anwendung werden angezeigt.

2. Geben Sie auf der Kommandozeile **opalindisk.exe** <TargetDevice> ein.

Zum Beispiel: **opalindisk.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.

7 Technischer Support

Technischen Support zu Sophos Produkten können Sie wie folgt abrufen:

- Rufen Sie das SophosTalk-Forum unter <http://community.sophos.com/> auf und suchen Sie nach Benutzern mit dem gleichen Problem.
- Durchsuchen Sie die Sophos Support-Knowledgebase unter <http://www.sophos.de/support/>.
- Laden Sie Dokumentation zu den Produkten unter <http://www.sophos.de/support/docs/> herunter.
- Senden Sie eine E-Mail an den technischen Support support@sophos.de und geben Sie die Versionsnummer(n), Betriebssystem(e) und Patch Level Ihrer Sophos Software sowie ggf. den genauen Wortlaut von Fehlermeldungen an.

8 Rechtliche Hinweise

Copyright © 1996 - 2011 Sophos Group. Alle Rechte vorbehalten. SafeGuard ist ein eingetragenes Warenzeichen von Sophos Group.

Sophos ist ein eingetragenes Warenzeichen von Sophos Limited, Sophos Group bzw. Utimaco Safeware AG. Alle anderen erwähnten Produkt- und Unternehmensnamen sind Warenzeichen oder eingetragene Warenzeichen der jeweiligen Inhaber.

Diese Publikation darf weder elektronisch oder mechanisch reproduziert, elektronisch gespeichert oder übertragen, noch fotokopiert oder aufgenommen werden, es sei denn, Sie verfügen entweder über eine gültige Lizenz, gemäß der die Dokumentation in Übereinstimmung mit dem Lizenzvertrag reproduziert werden darf, oder Sie verfügen über eine schriftliche Genehmigung des Urheberrechtsinhabers.

Copyright-Informationen von Drittanbietern finden Sie in der Datei Disclaimer and Copyright for 3rd Party Software.rtf in Ihrem Produktverzeichnis.