

# SOPHOS

## Sophos SafeGuard Disk Encryption 5.50 Sophos SafeGuard Easy 5.50 Administrator-Hilfe

Stand: November 2010



# Inhaltsverzeichnis

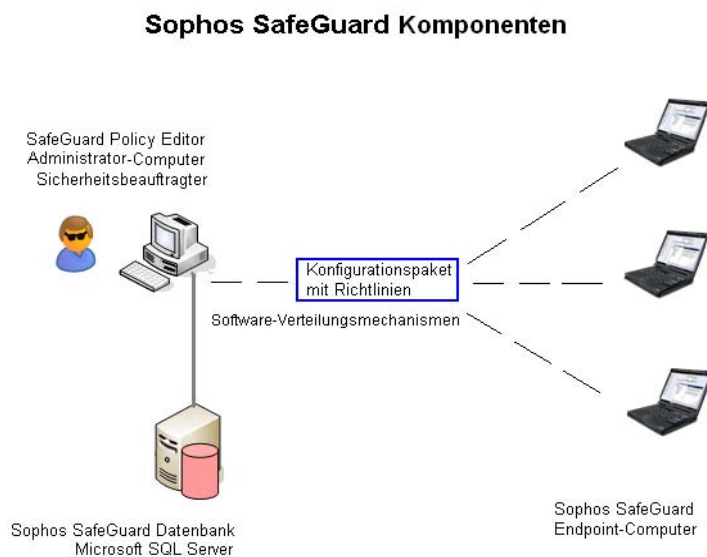
1	Sophos SafeGuard Überblick.....	3
2	SafeGuard Policy Editor .....	5
3	Sophos SafeGuard auf Endpoint-Computern.....	8
4	Datenverschlüsselung.....	9
5	Erste Schritte.....	13
6	Installation .....	20
7	Sophos SafeGuard auf einem Computer mit mehreren Betriebssystemen installieren .....	41
8	Am SafeGuard Policy Editor anmelden.....	44
9	Mit Richtlinien arbeiten .....	45
10	Mit Konfigurationspaketen arbeiten .....	50
11	Unternehmenszertifikat und Master Security Officer Zertifikat exportieren .....	52
12	Korrupte SafeGuard Policy Editor Installation wiederherstellen.....	54
13	Korrupte Datenbankkonfiguration wiederherstellen .....	55
14	Administrative Zugangsoptionen für Endpoint-Computer .....	57
15	Standardrichtlinien .....	70
16	Richtlinieneinstellungen .....	80
17	SafeGuard Data Exchange.....	118
18	Die Power-on Authentication (POA) .....	121

19	Recovery-Optionen.....	131
20	Recovery über Local Self Help.....	133
21	Recovery über Challenge/Response.....	139
22	Systemwiederherstellung.....	156
23	Deinstallation von Sophos SafeGuard auf Endpoint-Computern verhindern.....	159
24	Sophos SafeGuard aktualisieren.....	160
25	Migration von Sophos SafeGuard 5.5x auf SafeGuard Enterprise .....	164
26	Migration SafeGuard Easy 4.x/Sophos SafeGuard Disk Encryption 4.x auf Sophos SafeGuard 5.5x .....	167
27	Technischer Support.....	177
28	Copyright .....	178

# 1 Sophos SafeGuard Überblick

Sophos SafeGuard ist eine umfassende Datensicherheitslösung, die Informationen auf einem Endpoint-Computer durch ein richtlinienbasiertes Verschlüsselungskonzept zuverlässig schützt.

Die Verwaltung erfolgt über den SafeGuard Policy Editor. Mit dem SafeGuard Policy Editor werden Richtlinien angelegt und verwaltet. Darüber hinaus bietet der SafeGuard Policy Editor Recovery-Funktionen. Die Richtlinien werden in Konfigurationspaketen an die Endpoint-Computer verteilt. Auf Benutzerseite sind Datenverschlüsselung und Schutz vor Angreifern die primären Sicherheitsfunktionen von Sophos SafeGuard. Sophos SafeGuard fügt sich dabei nahtlos in die gewohnte Benutzerumgebung ein und lässt sich leicht und intuitiv bedienen. Die Sophos SafeGuard eigene Authentisierung, die Power-on Authentication (POA), sorgt für den umfassenden Zugriffsschutz und bietet komfortable Unterstützung bei der Wiederherstellung von Anmeldeinformationen.



## 1.1 Produkt-Bundles

Sophos SafeGuard ist in verschiedenen Produkt-Bundles verfügbar: SGE (SafeGuard Easy) und ESDP (Endpoint Security and Data Protection). Ab Version 5.50 ist SGE der neue Produktname für SafeGuard Enterprise Standalone. Die beiden Bundles bieten unterschiedliche Module und Funktionen. Module und Funktionen, die für ESDP nicht zur Verfügung stehen, sind in diesem Handbuch durch entsprechende Hinweise gekennzeichnet.

## 1.2 Sophos SafeGuard Komponenten

Sophos SafeGuard besteht aus folgenden Komponenten:

Komponente	Beschreibung
SafeGuard Policy Editor	Sophos SafeGuard Management-Werkzeug zur Erstellung von Richtlinien für die Verschlüsselung und Authentisierung. Während der Erstkonfiguration kann ein Satz von Standard-Richtlinien sowie ein Standard-Konfigurationspaket für Endpoint-Computer erstellt werden. Der SafeGuard Policy Editor bietet außerdem Recovery-Funktionen, mit deren Hilfe sich der Zugang zu Endpoint-Computern wieder herstellen lässt, wenn Benutzer zum Beispiel ihr Kennwort vergessen haben.
Sophos SafeGuard Datenbank	Die Sophos SafeGuard Datenbank enthält alle relevanten Daten zu den Richtlinieneinstellungen für die Endpoint-Computer.
Sophos SafeGuard Software auf Endpoint-Computern	Software zur Datenverschlüsselung auf Endpoint-Computern.

## **2 SafeGuard Policy Editor**

Der SafeGuard Policy Editor ist das Verwaltungswerkzeug für durch Sophos SafeGuard geschützte Computer, die lokal verwaltet werden.

Der SafeGuard Policy Editor wird auf dem Computer installiert, auf dem Sie die administrativen Aufgaben ausführen möchten. Als Sicherheitsbeauftragter benutzen Sie den SafeGuard Policy Editor zur Verwaltung von Sophos SafeGuard Richtlinien und zur Festlegung von Konfigurationseinstellungen für Endpoint-Computer. Die Richtlinien und Einstellungen werden in Konfigurationspakete exportiert und auf den Endpoint-Computern implementiert. Es können mehrere dieser Konfigurationspakete erzeugt und dann über Third-Party-Mechanismen verteilt werden. Die Verteilung der Pakete kann während der Installation der Sophos SafeGuard Verschlüsselungssoftware erfolgen. Um die Einstellungen auf den Endpoint-Computern nachträglich zu ändern, können neue Konfigurationspakete erstellt und verteilt werden.

Der SafeGuard Policy Editor bietet außerdem Recovery-Funktionen, mit deren Hilfe sich der Zugang zu Endpoint-Computern wieder herstellen lässt, wenn Benutzer zum Beispiel ihr Kennwort vergessen haben.

## 2.1 Features

Zur Vereinfachung der Verwaltung bietet SafeGuard Policy Editor folgende Features:

- **Standardkonfiguration:** Per Default kann während der Erstkonfiguration des SafeGuard Policy Editor ein Konfigurationspaket mit vorkonfigurierten empfohlenen Richtlinien für die Endpoint-Computer erstellt werden. Sollten die Standardrichtlinien nicht alle Ihre spezifischen Anforderungen abdecken, können Sie im SafeGuard Policy Editor Ihre eigenen Richtlinien erstellen.
- **Administrative Zugangsoptionen:** Für Zugangsanforderungen für die Durchführung von administrativen Aufgaben auf den Endpoint-Computern nach der Installation bietet Sophos SafeGuard als administrative Zugangsoptionen Service Accounts und POA Access Accounts.
- **Schlüssel für die Verschlüsselung:** Für SafeGuard Device Encryption (volume-basierende Verschlüsselung) wird ein automatisch generierter Computerschlüssel verwendet. Für SafeGuard Data Exchange (dateibasierende Verschlüsselung) werden vom Benutzer local generierte Schlüssel verwendet. SafeGuard Data Exchange ist im Produkt-Bundle mit ESDP (Endpoint Security and Data Protection) nicht verfügbar.
- **Local Self Help:** Für Recovery-Vorgänge (zum Beispiel, wenn der Benutzer sein Kennwort vergessen hat) bietet Sophos SafeGuard die bequeme und benutzerfreundliche Recovery-Option Local Self Help. Mit Local Self Help können sich Benutzer, die ihr Kennwort vergessen haben, auch ohne Helpdesk-Hilfestellung wieder an ihrem Computer anzumelden.
- **Challenge/Response mit Helpdesk-Hilfestellung:**

Das Challenge/Response-Verfahren mit Helpdesk-Hilfestellung kann von Benutzern angefordert werden, wenn sie ihr Kennwort vergessen oder zu häufig falsch eingegeben haben. Das Verfahren lässt sich außerdem für Recovery-Vorgänge bei einer korrupten POA anwenden. Das Challenge/Response-Verfahren basiert auf spezifischen Schlüssel-Recovery-Dateien, die automatisch bei der Konfiguration des Sophos SafeGuard Endpoint-Computers generiert werden.

## 2.2 Datenbank

Die Sophos SafeGuard Richtlinien werden in einer SQL-Datenbank auf dem Administrator-Computer abgelegt. Steht keine vorhandene SQL Server Instanz zur Verfügung, so werden Sie während der Installation des Sophos SafeGuard Policy Editor dazu aufgefordert, Microsoft SQL Server 2005 Express zu installieren. Zu diesem Zweck ist Microsoft SQL Server 2005 Express in Ihrer Produktlieferung enthalten.

## 2.3 Upgrade

Sie können einen Upgrade auf SafeGuard Enterprise mit zentraler Verwaltung durchführen, um den vollen Funktionsumfang von SafeGuard Enterprise zu nutzen.

## 2.4 Protokollierung

Für durch Sophos SafeGuard geschützte Computer findet die Protokollierung in der Windows-Ereignisanzeige statt.

## 2.5 Unterschiede zum SafeGuard Management Center

Aufgrund des zentralen Management Servers bietet das SafeGuard Management Center erweiterte Verwaltungsmöglichkeiten, zum Beispiel:

- Active Directory Import mit Benutzer- und Domänenverwaltung
- Zentrale Protokollierung
- Definierbare administrative Rollen

Das SafeGuard Management Center steht mit SafeGuard Enterprise zur Verfügung.

**Hinweis:** Für Sophos SafeGuard Computer, die keine Verbindung zu einem SafeGuard Enterprise Server haben, können Sie im SafeGuard Management Center ebenfalls Einstellungen definieren und Konfigurationspakete erstellen.

## 3 Sophos SafeGuard auf Endpoint-Computern

Datenverschlüsselung und Schutz vor Angreifern sind die primären Sicherheitsfunktionen von Sophos SafeGuard. Sophos SafeGuard fügt sich dabei nahtlos in die gewohnte Benutzerumgebung ein und lässt sich leicht und intuitiv bedienen. Die Sophos SafeGuard eigene Authentisierung, die Power-on Authentication (POA), sorgt für umfassenden Zugriffsschutz und bietet komfortable Unterstützung bei der Wiederherstellung von Anmeldeinformationen.

### 3.1 Unterstützte Module

Für Endpoint-Computer stehen folgende Module zur Verfügung:

#### ■ SafeGuard Device Encryption

- **Volume-basierende Verschlüsselung:** Alle Daten auf den angegebenen Volumes (z. B. Boot-Laufwerk, Festplatte, Partitionen) werden transparent verschlüsselt (einschließlich Boot-Dateien, Swapfiles, Ruhezustand-Dateien, temporäre Dateien, Verzeichnisinformationen usw.), ohne dass der Benutzer seinen normale Vorgehensweise ändern oder Sicherheitsaspekte beachten muss.
- **Power-on Authentication:** Die Benutzeranmeldung an das Gerät findet unmittelbar nach dem Einschalten statt. Nach erfolgreicher POA erfolgt die Anmeldung am Betriebssystem automatisch.

#### ■ SafeGuard Data Exchange

Einfacher Datenaustausch mit Wechselmedien auf allen Plattformen ohne Neuverschlüsselung.

- **Dateibasierende Verschlüsselung :** Es werden alle mobilen beschreibbaren Medien inklusive externe Festplatten und USB Sticks transparent verschlüsselt.

**Hinweis:** Dieses Modul wird mit ESDP (Endpoint Security and Data Protection) nicht unterstützt.

## 4 Datenverschlüsselung

Das Kernstück von Sophos SafeGuard ist die Verschlüsselung von Daten auf unterschiedlichen Datenträgern. Die Verschlüsselung kann volume- oder dateibasierend durchgeführt werden, mit unterschiedlichen Schlüsseln und Algorithmen.

**Hinweis:** Die dateibasierende Verschlüsselung wird mit ESDP (Endpoint Security and Data Protection) nicht unterstützt.

Dateien werden transparent verschlüsselt. Wenn Benutzer Dateien öffnen, bearbeiten und speichern, werden Sie nicht zur Ver- oder Entschlüsselung aufgefordert.

Während der Erstkonfiguration des SafeGuard Policy Editor wird standardmäßig eine Richtliniengruppe mit vordefinierten Einstellungen für die Verschlüsselung und die Authentisierung erstellt, siehe [Standardrichtlinien](#), Seite 70.

Sie können die Einstellungen für die Verschlüsselung in einer Sicherheitsrichtlinie vom Typ **Geräteschutz** festlegen. Für weitere Informationen, siehe, siehe [Mit Richtlinien arbeiten](#), Seite 45 und siehe [Geräteschutz](#), Seite 100.

### 4.1 Volume-basierende Verschlüsselung

Mit der volume-basierenden Verschlüsselung werden alle Daten auf einem Volume (einschließlich Boot-Dateien, Pagefiles, Hibernation Files, temporäre Dateien, Verzeichnisinformationen usw.) verschlüsselt. Benutzer müssen sich in ihrer Arbeitsweise nicht anpassen oder auf Sicherheit achten.

**Hinweis:** Wenn für ein Volume oder einen Volume-Typ eine Verschlüsselungsrichtlinie existiert und die Verschlüsselung des Volumes schlägt fehl, darf der Benutzer nicht auf das Volume zugreifen.

#### 4.1.1 Schnelle Initialverschlüsselung

Die schnelle Initialverschlüsselung ist ein Spezialmodus für die volume-basierende Verschlüsselung. Dieser Modus reduziert den Zeitraum, der für die initiale Verschlüsselung (oder die endgültige Entschlüsselung) von Volumes auf Endpoint-Computern benötigt wird. Dies wird dadurch erreicht, dass nur auf den Festplattenspeicherplatz zugegriffen wird, der tatsächlich in Gebrauch ist.

Für die schnelle Initialverschlüsselung gelten folgende Voraussetzungen:

- Die schnelle Initialverschlüsselung funktioniert nur auf NTFS-formatierten Volumes.
- Bei NTFS-formatierten Volumes mit einer Cluster-Größe von 64 KB kann die schnelle Initialverschlüsselung nicht angewendet werden.

**Hinweis:** Dieser Modus kann zu einem unsicherem Zustand führen, wenn die Platte vor ihrer aktuellen Verwendung bereits in Gebrauch war. Nicht verwendete Sektoren können noch Daten enthalten. Daher ist die schnelle Initialverschlüsselung standardmäßig deaktiviert.

Um die schnelle Initialverschlüsselung zu aktivieren, wählen Sie die Einstellung **Schnelle Initialverschlüsselung** in einer Richtlinie vom Typ **Geräteschutz**.

**Hinweis:** Für die Entschlüsselung eines Volumes wird unabhängig von der gewählten Richtlinieneinstellung immer die schnelle Initialverschlüsselung verwendet. Für die Entschlüsselung gelten ebenfalls die angegebenen Einschränkungen.

#### 4.1.2 Volume-basierende Verschlüsselung und die Windows 7 Systempartition

Für Windows 7 Professional, Enterprise und Ultimate wird auf den Endpoint-Computern eine Systempartition angelegt, der kein Laufwerksbuchstabe zugeordnet ist. Diese Systempartition kann von Sophos SafeGuard nicht verschlüsselt werden.

#### 4.1.3 Volume-basierende Verschlüsselung und Unidentified File System Objects

Unidentified File System Objects sind Volumes, die von SafeGuard Enterprise nicht eindeutig als verschlüsselt oder unverschlüsselt identifiziert werden können. Existiert für ein Unidentified File System Volume eine Verschlüsselungsrichtlinie, so wird der Zugriff auf das Volume verweigert. Existiert keine Verschlüsselungsrichtlinie, so kann der Benutzer auf das Volume zugreifen.

**Hinweis:** Existiert für ein Unidentified File System Object eine Verschlüsselungsrichtlinie, bei der die Richtlinieneinstellung **Schlüssel für die Verschlüsselung** auf eine Option eingestellt ist, die die Schlüsselauswahl ermöglicht (z. B. **Beliebiger Schlüssel im Schlüsselring des Benutzer**), so entsteht zwischen der Anzeige des Schlüsselauswahldialogs und der Verweigerung des Zugriffs auf das Volume eine zeitliche Lücke. Während dieser Zeit kann auf das Volume zugegriffen werden. So lange der Schlüsselauswahldialog nicht vom Benutzer bestätigt wird, besteht Zugriff auf das Volume. Um dies zu vermeiden, geben Sie einen vorausgewählten Schlüssel für die Verschlüsselung an. Für weitere Informationen zur relevanten Richtlinieneinstellung, siehe [Geräteschutz](#), Seite 100. Diese zeitliche Lücke entsteht auch dann für mit dem Endpoint-Computer verbundene Unidentified File System Objects, wenn der Benutzer zu dem Zeitpunkt, an dem die Verschlüsselungsrichtlinie wirksam wird, bereits Dateien auf dem Volume geöffnet hat. In diesem Fall, kann nicht gewährleistet werden, dass der Zugriff auf das Volume verweigert wird, da dies zu Datenverlust führen könnte.

#### 4.1.4 Verschlüsselung von Volumes mit aktivierter Autorun-Funktionalität

Wenn Sie auf Volumes, für die die Autorun-Funktionalität aktiviert ist, eine Verschlüsselungsrichtlinie anwenden, so können folgende Probleme auftreten:

- Das Volume wird nicht verschlüsselt.
- Wenn es sich bei dem Volume um ein Unidentified File System Object (siehe [Volume-basierende Verschlüsselung und Unidentified File System Objects](#), Seite 10), so wird der Zugriff nicht verweigert.

### 4.2 Dateibasierende Verschlüsselung

**Hinweis:** Die dateibasierende Verschlüsselung wird mit ESDP (Endpoint Security and Data Protection) nicht unterstützt.

Die dateibasierende Verschlüsselung stellt sicher, dass alle Daten verschlüsselt sind (außer Boot Medium und Verzeichnisinformationen). Mit dateibasierender Verschlüsselung lassen sich auch optische Medien wie CD/DVD verschlüsseln. Außerdem können Daten mit Fremdrechnern, auf denen SafeGuard Enterprise nicht installiert ist, ausgetauscht werden (soweit von der Richtlinie erlaubt).

**Hinweis:** Mit “Dateibasierender Verschlüsselung” verschlüsselte Daten können nicht komprimiert werden. Umgekehrt können auch komprimierte Dateien nicht dateibasierend verschlüsselt werden.

**Hinweis:** Boot-Volumes werden niemals dateibasierend verschlüsselt. Sie sind automatisch von einer dateibasierenden Verschlüsselung ausgenommen, auch wenn eine entsprechende Regel definiert ist.

Um dateibasierende Verschlüsselung auf Endpoint-Computer anzuwenden, erstellen Sie eine Richtlinie vom Typ **Geräteschutz** und wählen Sie bei **Verschlüsselungsmodus für Medien** die Einstellung **Dateibasierend**. Für weitere Informationen, siehe [Geräteschutz](#), Seite 100.

#### 4.2.1 Anwendungen von der Verschlüsselung ausnehmen

Sie können für Anwendungen festlegen, dass sie vom Sophos SafeGuard Filter-Treiber ignoriert werden sollen. Damit sind sie von der transparenten Ver-/Entschlüsselung ausgenommen.

Ein Beispiel hierfür ist ein Backup- Programm. Damit die Daten beim Erstellen eines Backups nicht entschlüsselt werden, kann diese Anwendung von der Verschlüsselung/Entschlüsselung ausgenommen werden. Die Daten werden verschlüsselt gesichert.

Als typischer Anwendungsfall können Backup-Programme zum Beispiel als unberücksichtigt definiert werden, damit sie immer die verschlüsselten Daten lesen und sichern.

Anwendungen, die bei gleichzeitiger Verwendung mit Sophos SafeGuard Funktionsstörungen auslösen können, aber keine Verschlüsselung erfordern, können generell von der Verschlüsselung ausgenommen werden.

Sie können Anwendungen von der Verschlüsselung/Entschlüsselung in einer Richtlinie vom Typ **Geräteschutz** mit dem Ziel **Lokale Datenträger** ausnehmen. Zur Angabe von **Unberücksichtigten Anwendungen** wird der vollständige Name der ausführbaren Datei (optional inklusive Pfadinformation) verwendet.

Für weitere Informationen, siehe [Geräteschutz](#), Seite 100.

## 5 Erste Schritte

Dieses Kapitel erklärt die notwendigen Vorbereitungsmaßnahmen für eine erfolgreiche Installation von Sophos SafeGuard.

### 5.1 Strategie für den Einsatz von Sophos SafeGuard

Vor der Installation und Konfiguration von Sophos SafeGuard auf Endpoint-Computern ist es empfehlenswert, eine Strategie unter Berücksichtigung der spezifischen Anforderungen und der verfügbaren Optionen festzulegen.

Bei der Festlegung der Strategie für den Einsatz von Sophos SafeGuard auf Endpoint-Computern, sollten folgende Optionen berücksichtigt werden:

#### 5.1.1 Richtlinien

Für Richtlinien bietet Sophos SafeGuard folgende Optionen:

##### ■ Standardrichtlinien

Sophos SafeGuard bietet vordefinierte Standardrichtlinien für die schnelle und einfache Umsetzung von Richtlinien auf Endpoint-Computern. Während der Erstkonfiguration des SafeGuard Policy Editor wird standardmäßig eine Richtlinienengruppe mit vordefinierten Einstellungen für die Verschlüsselung und die Authentisierung erstellt. Für die Konfiguration von Endpoint-Computern wird automatisch ein Konfigurationspaket mit diesen Standardrichtlinien erstellt.

Für Details zu Standardrichtlinien und die vordefinierten Einstellungen, siehe [Standardrichtlinien](#), Seite 70.

##### ■ Definition eigener Richtlinien

Sollten die Standardrichtlinien nicht alle Ihre spezifischen Anforderungen abdecken, können Sie im SafeGuard Policy Editor Ihre eigenen Richtlinien erstellen.

Für Details zum Erstellen von Richtlinien, siehe [Mit Richtlinien arbeiten](#), Seite 45. Für Details zur Umsetzung von Richtlinien auf Endpoint-Computern, siehe [Mit Konfigurationspaketen arbeiten](#), Seite 50.

Für eine detaillierte Beschreibung aller verfügbaren Richtlinien und Einstellungen, siehe [Richtlinieneinstellungen](#), Seite 80.

## 5.1.2 Administrative Zugangsoptionen

Für Zugangsanforderungen für die Durchführung von administrativen Aufgaben auf den Endpoint-Computern nach der Installation bietet Sophos SafeGuard administrative Zugangsoptionen für zwei verschiedene Szenarien:

### ■ Service Accounts für die Anmeldung an Windows

Mit Service Accounts können sich Benutzer (z. B., Mitarbeiter des IT-Teams, Rollout-Beauftragte) zur Ausführung administrativer Aufgaben nach der Installation von Sophos SafeGuard an Endpoint-Computern anmelden (Windows-Anmeldung), ohne die Power-on Authentication zu aktivieren und ohne, dass sie als Benutzer zum Computer hinzugefügt werden.

Service Account Listen werden den Endpoint-Computern über Richtlinien zugewiesen. Service Account Listen sollten bereits im ersten Sophos SafeGuard Konfigurationspaket, das im SafeGuard Policy Editor für die Konfiguration des Sophos SafeGuard Endpoint-Computers erstellt wird, zugewiesen werden. Um Service Account Listen zu ändern, können Sie ein neues Konfigurationspaket erstellen und es an die Endpoint-Computer verteilen.

Für weitere Details zu Service Account Listen, siehe [Service Account Listen für die Windows-Anmeldung](#), Seite 58.

### ■ POA Access Accounts für die Anmeldung an die POA

POA Access Accounts sind vordefinierte lokale Benutzerkonten, die die Anmeldung an Endpoint-Computern (z. B., durch Mitarbeiter des IT-Teams) zur Durchführung administrativer Aufgaben nach der Aktivierung der POA ermöglichen.

Sie können POA Access Accounts im SafeGuard Policy Editor anlegen, diese in POA Access Account Gruppen gruppieren und die Gruppen über Sophos SafeGuard Konfigurationspakete den Endpoint-Computern zuweisen.

Für weitere Details zu POA Access Accounts, siehe [POA Access Accounts für die POA-Anmeldung](#), Seite 64.

### 5.1.3 Recovery-Optionen

Für Recovery-Vorgänge (z. B., wenn Benutzer ihr Kennwort vergessen haben) bietet Sophos SafeGuard folgende Recovery-Optionen:

#### ■ Recovery für die Anmeldung über Local Self Help

Local Self Help ermöglicht es Benutzern, die Ihr Kennwort vergessen haben, sich selbständig und ohne Unterstützung des Helpdesk an ihrem Computer anzumelden. Um wieder Zugang zu ihrem Computer zu erhalten, beantworten die Benutzer einfach eine Reihe von vordefinierten Fragen in der Power-on Authentication.

In den Standardrichtlinien ist Local Self Help standardmäßig aktiviert und konfiguriert. Wenn Sie die Standardkonfiguration nicht verwenden, müssen Sie Local Self Help über eine Richtlinie aktivieren und die vom Endbenutzer zu beantwortenden Fragen definieren.

Für weitere Details zu Local Self Help, siehe [Recovery über Local Self Help](#), Seite 133.

#### ■ Recovery über Challenge/Response

Das Challenge/Response Recovery-Verfahren ist ein sicheres und effizientes Recovery-System, das Benutzer unterstützt, die sich an ihrem Computer nicht mehr anmelden oder nicht auf verschlüsselte Daten zugreifen können. Für das Challenge/Response Verfahren ist die Unterstützung durch einen Helpdesk erforderlich.

In den Standardrichtlinien ist Challenge/Response standardmäßig aktiviert. Wenn Sie die Standardkonfiguration nicht verwenden, müssen Sie Challenge/Response über eine Richtlinie aktivieren. Für Daten-Recovery-Vorgänge müssen zunächst im SafeGuard Policy Editor spezifische Dateien (virtuelle Clients) erstellt werden.

Für Details zum Challenge/Response Verfahren, siehe [Recovery über Challenge/Response](#), Seite 139.

## 5.2 Systemvoraussetzungen

Genauere Informationen über Systemvoraussetzungen für Hardware, Software, Service Packs and Speicherplatzbedarf während der Installation und im Betrieb entnehmen Sie bitte der Startup-Anleitung.

## **5.2.1 Besondere Systemvoraussetzungen für Endpoint-Computer**

- Wenn auf dem Computer Intel Advanced Host Controller Interface (AHCI) benutzt wird, so muss sich die Boot-Festplatte in Slot 0 oder Slot 1 befinden. Sie können bis zu 32 Festplatten einlegen. Sophos SafeGuard läuft nur auf den ersten beiden Slot-Nummern.
- Dynamische Festplatten und GUID Partitionstabellen (GPT)-Platten werden nicht unterstützt. Die Installation bricht in diesem Fall ab. Wenn diese Platten nachträglich im System auftauchen, werden sie nicht unterstützt.
- Systeme mit Festplatten, die über einen SCSI Bus angeschlossen sind, werden vom Sophos SafeGuard Device Encryption Modul nicht unterstützt.

## **5.3 Installation vorbereiten**

Vor der Installation von Sophos SafeGuard sind folgende vorbereitende Maßnahmen empfehlenswert.

### **5.3.1 Allgemeine Vorbereitung**

- Um die Software zu installieren und mit dem SafeGuard Policy Editor zu arbeiten, benötigen Sie Windows-Administratorenrechte.
- Schließen Sie alle geöffneten Anwendungen.
- Stellen Sie sicher, dass genügend Festplattenspeicher frei ist. Informationen hierzu finden Sie in der Startup-Anleitung.
- Lesen Sie die Freigabemitteilung.

### **5.3.2 Vorbereitung für die Verschlüsselung**

- Auf den Endpoint-Computern muss ein Benutzerkonto angelegt und aktiv sein.
- Erstellen Sie eine vollständige Sicherungskopie der Daten auf dem Endpoint-Computer.
- Sophos bietet Ihnen eine Hardware- Konfigurationsdatei, um die Konflikte zwischen der POA and der von Ihnen verwendeten Endpoint Computer-Hardware zu minimieren. Diese Datei ist im Installationspaket der Verschlüsselungssoftware enthalten.

Wir empfehlen, vor jeder größer angelegten Installation oder Aktualisierung von Sophos SafeGuard die aktuelle Version dieser Hardware-Konfigurationsdatei zu installieren. Die Datei wird monatlich aktualisiert und steht hier zum Download zur Verfügung: <ftp://ftp.ou.utimaco.de/>

Für weitere Information, siehe [In der Power-on Authentication unterstützte Hotkeys](#), Seite 127 sowie den folgenden Artikel in unserer Wissensdatenbank:

<http://www.sophos.com/support/knowledgebase/article/65700.html>

- Untersuchen Sie die Festplatte(n) auf Fehler. Benutzen Sie dazu folgenden Befehl:

```
chkdsk %systemdrive% /F /V /L /X
```

Unter Umständen werden Sie dazu aufgefordert, den Computer neu zu starten und chkdsk noch einmal auszuführen. Weitere Informationen zu diesem Thema erhalten Sie in der Wissensdatenbank: <http://www.sophos.com/support/knowledgebase/article/107081.html>.

- Verwenden Sie das Windows-Tool „defrag“, um nach fragmentierten Boot-Dateien, Daten-Dateien und Ordnern auf lokalen Volumes zu suchen und diese zu konsolidieren. Weitere Informationen hierzu finden Sie in unserer Wissensdatenbank: <http://www.sophos.com/support/knowledgebase/article/109226.html>
- Deinstallieren Sie Third-party Boot-Manager, z. B. “Bootmanager PRO”, “boot-us”.
- Wenn Sie ein Imaging/Clone Programm verwendet haben, empfehlen wir, den MBR „neu“ zu schreiben. Für die Installation von Sophos SafeGuard benötigen Sie einen sauberen Master Boot Record. Möglicherweise ist der MBR aber durch den Einsatz von Image/Clone-Programmen nicht mehr in einwandfreiem, ursprünglichen Zustand.

Säubern Sie deshalb den Master Boot Record, indem Sie von einer Windows-CD unter Anwendung des Befehls FIXMBR neu starten. Weitere Informationen finden Sie unter: <http://www.sophos.com/support/knowledgebase/article/108088.html>

- Wenn die Bootpartition von FAT nach NTFS konvertiert wurde, der Computer aber noch nicht neu gestartet wurde, sollten Sie Sophos SafeGuard nicht installieren. Möglicherweise wird die Installation nicht beendet, da das Dateisystem zum Zeitpunkt der Installation noch FAT ist, jedoch zum Zeitpunkt der Aktivierung NTFS vorgefunden wird. In diesem Fall müssen Sie den Computer einmalig neu starten, bevor Sophos SafeGuard installiert wird.

## 5.4 Sprache der Benutzeroberfläche

Sie können die Sprache der Benutzeroberfläche während der Installation des SafeGuard Policy Editor sowie von Sophos SafeGuard am Endpoint-Computer steuern.

### 5.4.1 Sprache während der Installation

Die Sprache der Installations- und Konfigurationsassistenten wird automatisch an die Spracheinstellungen des Betriebssystems angepasst. Deutsch, Englisch, Französisch und Japanisch werden für die Installations- und Konfigurationsassistenten unterstützt. Wenn die Betriebssystemsprache für die Assistenten nicht verfügbar ist, wird standardmäßig Englisch benutzt.

### 5.4.2 Sprache des SafeGuard Policy Editor

Die Sprache des SafeGuard Policy Editor definieren Sie im SafeGuard Policy Editor:

- Öffnen Sie das Menü Extras > Optionen > Allgemein. Aktivieren Sie **Benutzerdefinierte Sprache verwenden** und wählen Sie eine verfügbare Sprache aus.
- Starten Sie den SafeGuard Policy Editor neu und er wird in der ausgewählten Sprache angezeigt.

### 5.4.3 Sprache von Sophos SafeGuard am Endpoint-Computer

Die Sprache von Sophos SafeGuard am Endpoint-Computer steuern Sie über den Richtlinientyp Allgemein im SafeGuard Policy Editor (Einstellung Anpassung > Sprache am Client:

- Wenn die Sprache des Betriebssystems gewählt wird, richtet sich die Produktsprache nach der Spracheinstellung des Betriebssystems. Steht die entsprechende Betriebssystemsprache in Sophos SafeGuard nicht zur Verfügung, wird standardmäßig die englische Version von Sophos SafeGuard angezeigt.
- Wenn eine der zur Verfügung stehenden Sprachen gewählt wird, werden die Sophos SafeGuard Produktanteile auf dem Endpoint-Computer in der ausgewählten Sprache angezeigt.

## **5.5 Interaktion mit anderen SafeGuard-Produkten**

Beachten Sie folgende Informationen zur Interaktion von Sophos SafeGuard mit anderen SafeGuard-Produkten.

### **5.5.1 Interaktion mit SafeGuard LAN Crypt**

Bitte beachten Sie:

- SafeGuard LAN Crypt 3.7x und Sophos SafeGuard 5.50 können auf demselben Computer installiert werden und sind voll kompatibel.
- Versionen von SafeGuard LAN Crypt vor 3.7x und Sophos SafeGuard 5.5x können nicht auf demselben Computer eingesetzt werden.

Wenn Sie versuchen, Sophos SafeGuard 5.50 auf einem Computer mit einer SafeGuard LAN Crypt Installation der Version 3.6x oder einer früheren Version zu installieren, wird der Setup abgebrochen. Eine entsprechende Fehlermeldung wird angezeigt.

### **5.5.2 Interaktion mit SafeGuard PrivateCrypto und SafeGuard PrivateDisk**

Sophos SafeGuard 5.5x und die Standalone-Produkte SafeGuard PrivateCrypto ab Version 2.30 und SafeGuard PrivateDisk ab Version 2.30 können zusammen mit Sophos SafeGuard 5.5x auf demselben Computer eingesetzt werden.

### **5.5.3 Interaktion mit SafeGuard Removable Media**

Das Modul SafeGuard Data Exchange und SafeGuard Removable Media können nicht zusammen auf einem Computer installiert werden. Prüfen Sie, bevor Sie das Modul SafeGuard Data Exchange auf einem Computer installieren, ob SafeGuard Removable Media bereits installiert ist. In diesem Fall müssen Sie SafeGuard Removable Media zuerst deinstallieren, bevor Sie SafeGuard Data Exchange auf dem Computer installieren.

**Hinweis:** SafeGuard Data Exchange steht mit ESDP nicht zur Verfügung.

## 6 Installation

Das Einrichten von Sophos SafeGuard umfasst folgende Schritte:

	Aufgabe	Installationpaket/-Tool	
		ESDP	SGE
1	<b>Computer für Sophos SafeGuard Administration einrichten</b>		
	Installieren Sie den SafeGuard Policy Editor.	SDEPolicyEditor.msi	SGNPolicyEditor.msi
	Erstkonfiguration im SafeGuard Policy Editor und Erstellung einer Standardkonfiguration für die Verschlüsselungssoftware.	SafeGuard Policy Editor Konfigurationsassistent	
2	<b>Sophos SafeGuard Verschlüsselungssoftware anpassen (optional)</b>		
	Definieren Sie weitere Konfigurationseinstellungen über benutzerdefinierte Richtlinien (z. B. Service Account Listen).	SafeGuard Policy Editor, Bereich Richtlinien	
	Erzeugen Sie weitere Konfigurationspakete (MSI) mit benutzerdefinierten Richtlinien.	SafeGuard Policy Editor, Konfigurationspakete	
3	<b>Sophos SafeGuard Verschlüsselungssoftware auf Endpoint-Computern einrichten</b>		
	Endpoint-Computer mit nötigen Voraussetzungen für die korrekte Installation der Verschlüsselungssoftware versehen.	SGxClientPreinstall.msi	SGxClientPreinstall.msi
	Um Sophos SafeGuard Device Encryption (volume-basierende Verschlüsselung) anzuwenden, installieren Sie:	SDEClient.msi oder	SGNClient.msi <b>Hinweis:</b> In diesem Paket kann zusätzlich Sophos SafeGuard Data Exchange (dateibasierende Verschlüsselung) manuell aktiviert werden.
	Um nur Sophos SafeGuard Data Exchange (dateibasierende Verschlüsselung) anzuwenden, installieren Sie:	mit ESDP nicht verfügbar	SGNClient_withoutDE.msi

Aufgabe	Installationpaket/-Tool	
	ESDP	SGE
Installieren Sie das/die Konfigurationspaket(e) auf den Endpoint-Computern.	Generiertes <Konfigurationspaket>.msi	

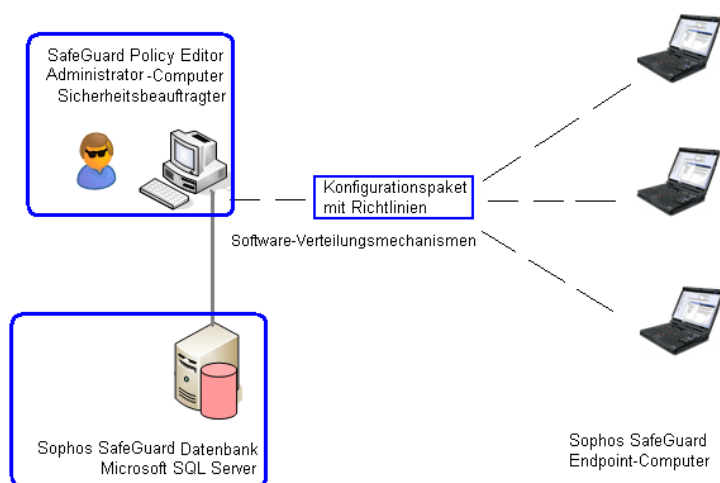
**Hinweis:** Wenn das Betriebssystem des Endpoint-Computers Windows 7 64 Bit oder Windows Vista 64 Bit ist, können Sie auch die 64 Bit-Variante des "Client" .msi Pakets installieren, wenn vorhanden (<Paketname>\_x64.msi).

## 6.1 SafeGuard Policy Editor installieren

Folgende Voraussetzungen müssen erfüllt sein:

- Sie benötigen Windows-Administratorrechte.
- Wenn Sie einen bereits installierten Microsoft SQL Datenbankserver benutzen möchten, benötigen Sie die notwendigen SQL Zugriffsrechte und Konto-Daten.
- .NET Framework 3.0 Service Pack 1 müssen auf dem Administrator-Computer installiert sein. Beides steht auf <http://www.microsoft.com/downloads> zum kostenlosen Download zur Verfügung.

### Sophos SafeGuard Komponenten



Um die Verschlüsselungs-Software auf den Endpoint-Computern einzurichten, installieren Sie erst den SafeGuard Policy Editor auf einem Administrator-Computer. Sie können auch eine erstmalige Installation des SafeGuard Policy Editor auf einem Windows Server durchführen. Später können Sie die Software auf mehreren Administrator-Computern installieren, die alle eine Verbindung mit der zentralen Sophos SafeGuard Datenbank auf dem Server herstellen. Für den Zugriff auf jede SafeGuard Policy Editor Instanz wird dasselbe Konto benutzt.

1. Wenn Sie ESDP-Kunde sind, klicken Sie auf SDEPolicyEditor.msi doppelt. Wenn Sie SGE-Kunde sind, klicken Sie auf SGNPolicyEditor.msi doppelt. Ein Assistent führt Sie durch die notwendigen Installationsschritte.
2. Klicken Sie im Willkommen-Fenster auf **Weiter**.
3. Akzeptieren Sie die Lizenzvereinbarung.
4. Bestätigen Sie den Installationspfad.

Die Sophos SafeGuard Richtlinieneinstellungen werden in einer SQL Datenbankinstanz gespeichert. Steht keine vorhandene SQL Datenbankinstanz zur Verfügung, so werden Sie während der Installation des SafeGuard Policy Editor dazu aufgefordert, Microsoft SQL Server 2005 Express zu installieren. In diesem Fall werden Ihre Windows-Anmeldeinformationen als SQL Benutzerkonto verwendet.

5. Klicken Sie auf **Beenden**, um die Installation abzuschließen.

The SafeGuard Policy Editor ist auf dem Administrator-Computer installiert. Im nächsten Schritt führen Sie die Erstkonfiguration im SafeGuard Policy Editor durch.

## **6.2 Erstkonfiguration im SafeGuard Policy Editor Konfigurationsassistent durchführen**

Sie müssen über Windows Administratorrechte verfügen.

1. Starten Sie nach der Installation den SafeGuard Policy Editor. Der Konfigurationsassistent wird gestartet und führt Sie durch die notwendigen Konfigurationsschritte.
2. Klicken Sie im Fenster **Willkommen** auf **Weiter**.

## 6.2.1 Datenbank konfigurieren

Zum Speichern aller Sophos SafeGuard Verschlüsselungsrichtlinien und Einstellungen wird eine Datenbank verwendet. Der Workflow richtet sich danach, ob Sie bei einer Erstinstallation eine neue Datenbank anlegen oder eine bereits vorhandene Datenbank verwenden. Die Verwendung einer bereits vorhandenen Datenbank kann sich als nützlich erweisen, wenn Sie zusätzliche Instanzen des SafeGuard Policy Editor installieren möchten, um zum Beispiel Helpdesk-Mitarbeitern die Durchführung von Challenge/Response-Verfahren zu ermöglichen.

1. Führen Sie auf der Seite **Datenbank** einen der folgenden Schritte aus:

- Wählen Sie bei einer Erstinstallation die Option **Eine neue Datenbank erstellen**.
- Bei einer zusätzlichen Installation, oder wenn Sie eine zuvor bereits angelegte Datenbank verwenden möchten, wählen Sie **Eine bestehende Datenbank verwenden**. Wählen Sie unter **Datenbankname** den Namen der Datenbank aus der Liste.

2. Führen Sie unter **Datenbankeinstellungen** einen der folgenden Schritte aus:

- Wenn nur die vorinstallierte Microsoft SQL Express Instanz verfügbar ist, wird die Instanz bereits unter **SQL Server Instanz** angezeigt. Ihre Windows-Anmeldeinformationen werden als SQL Zugangskonto verwendet. Klicken Sie auf **Weiter**.
- Wenn Sie eine bereits vorhandene Datenbank verwenden, oder mehrere SQL Server Instanzen installiert sind, klicken Sie auf **Ändern**, um die gewünschte auszuwählen. Es wird ein Dialog angezeigt, in dem Sie die Verbindung zum ausgewählten Server konfigurieren. Nach Abschluss der Konfiguration werden die ausgewählten Einstellungen hier angezeigt. Klicken Sie auf **Weiter**.

Die Verbindung zum Datenbankserver ist hergestellt.

### 6.2.1.1 Weitere Schritte für die Datenbank-Konfiguration durchführen

Gehen Sie wie folgt vor:

1. Wählen Sie im Dialog **Datenbankverbindung** unter **Datenbankserver** den gewünschten SQL Datenbankserver aus der Liste. Alle auf Ihrem Computer oder in Ihrem Netzwerk verfügbaren Datenbankserver werden angezeigt (die Liste wird alle 12 Minuten aktualisiert). Aktivieren Sie **SSL verwenden**, um die Verbindung zu diesem Datenbankserver mit SSL zu sichern.
2. Wählen Sie unter **Authentisierung** die Art der Authentisierung, die für den Zugriff auf die Datenbank verwendet werden soll:
  - Aktivieren Sie **Windows NT Authentisierung benutzen**, um Ihre Windows-Anmeldeinformationen zu verwenden.

**Hinweis:** Verwenden Sie diese Art der Authentisierung, wenn Ihr Computer Teil einer Domäne ist. Unter Umständen ist hier jedoch eine zusätzliche Konfiguration erforderlich, da der Benutzer dazu berechtigt sein muss, eine Verbindung mit der Datenbank herzustellen.

- Aktivieren Sie **SQL Server Authentisierung benutzen**, um mit Ihren SQL Anmeldeinformationen auf die Datenbank zuzugreifen. Sie werden dazu aufgefordert, Ihre Anmeldeinformationen einzugeben und zu bestätigen. Falls notwendig, erhalten Sie diese Informationen von Ihrem SQL Administrator.

**Hinweis:** Verwenden Sie diese Art der Authentisierung, wenn sich Ihr Computer nicht in einer Domäne ist. Aktivieren Sie **SSL verwenden**, um die Verbindung zum und vom Datenbankserver zu sichern. SSL-Verschlüsselung erfordert jedoch eine funktionsfähige SSL-Umgebung auf dem Computer, auf dem sich die ausgewählte SQL Datenbank befindet, die Sie vorab einrichten müssen. Weitere Informationen finden Sie hier: <http://www.sophos.de/support/knowledgebase/article/108339.html>. Mit der SQL Authentisierung lässt sich später ein Upgrade auf das SafeGuard Management Center auf einfache Art und Weise durchführen.

3. Klicken Sie auf **Verbindung prüfen**. Wenn die Verbindung zur SQL-Datenbank hergestellt ist, wird eine entsprechende Erfolgsmeldung ausgegeben.
4. Bestätigen Sie zweimal mit **OK**.

## 6.2.2 Sicherheitsbeauftragten-Zertifikate erzeugen (neue Datenbank)

Bei einer Erstinstallation und beim Anlegen einer neuen Datenbank wird ein Sicherheitsbeauftragter für die Authentisierung angelegt. Pro Installation wird jeweils nur ein Sicherheitsbeauftragtenkonto angelegt. Als Sicherheitsbeauftragter melden Sie sich am SafeGuard Policy Editor an, um Sophos SafeGuard Richtlinien zu erstellen und die Verschlüsselungssoftware für die Endbenutzer zu konfigurieren. Für Details zur Wiederherstellung einer korrupten Datenbankkonfiguration, siehe [Korrupte Datenbankkonfiguration wiederherstellen](#), Seite 55

1. Auf der Seite **Sicherheitsbeauftragter** ist der Name des Sicherheitsbeauftragten bereits eingeblendet.  
Für Installationen mit ESDP lautet der Name des Sicherheitsbeauftragten immer Administrator. Für alle anderen Installationen wird der aktuelle Benutzername angezeigt.
2. Geben Sie ein Kennwort ein, mit dem Sie sich später am SafeGuard Policy Editor anmelden  
Bestätigen Sie das Kennwort.

Verwahren Sie dieses Kennwort an einem sicheren Ort. Ohne das Kennwort können Sie nicht auf den SafeGuard Policy Editor zugreifen. Unter Umständen benötigt das Helpdesk Team Zugriff auf dieses Benutzerkonto für die Durchführung von Challenge/Response-Verfahren.

3. Klicken Sie auf **Weiter**.

Das neu angelegte Sicherheitsbeauftragten-Zertifikat ist im Zertifikatsspeicher abgelegt. Im nächsten Schritte wird das Unternehmenszertifikat erzeugt.

### **6.2.3 Sicherheitsbeauftragten-Zertifikat importieren (vorhandene Datenbank)**

Wenn Sie eine bereits vorhandene Datenbank benutzen, muss das Sicherheitsbeauftragten-Zertifikat importiert werden. Sie können nur vom SafeGuard Policy Editor generierte Zertifikate importieren. Durch eine PKI (z. B. Verisign) erstellte Zertifikate sind nicht zulässig.

1. Klicken Sie auf der Seite **Sicherheitsbeauftragter** auf **Importieren**, um das Sicherheitsbeauftragten-Zertifikat zu importieren.
2. Suchen Sie nach dem gewünschten Zertifikat und bestätigen Sie Ihre Auswahl mit **Öffnen**.
3. Geben Sie das Kennwort für die ausgewählte Schlüsseldatei ein, das Sie zur Anmeldung an den SafeGuard Policy Editor verwendet haben.
4. Bestätigen Sie das Zertifikat mit **Ja**.
5. Geben Sie das Kennwort für die Anmeldung an den Sophos SafeGuard Policy Editor ein und bestätigen Sie es.
6. Klicken Sie auf **Weiter** und dann auf **Beenden**, um die Erstkonfiguration abzuschließen.

Die Erstkonfiguration im SafeGuard Policy Editor ist abgeschlossen.

### **6.2.4 Unternehmenszertifikat erzeugen**

Das Unternehmenszertifikat dient zum Schutz der Richtlinieneinstellungen in der Datenbank und auf den mit Sophos SafeGuard geschützten Computern. Für Informationen zur Wiederherstellung einer korrupten Datenbankkonfiguration, siehe [Korrupte Datenbankkonfiguration wiederherstellen](#), Seite 55.

1. Geben Sie auf der Seite **Unternehmen** einen **Unternehmensnamen** ein. Vergewissern Sie sich, dass **Zertifikat automatisch erstellen** aktiviert ist.

Bei einer Erstinstallation und wenn Sie eine neue Datenbank angelegt haben, ist **Zertifikat automatisch erstellen** bereits aktiviert. Für den Namen gilt eine Begrenzung auf 64 Zeichen.

2. Klicken Sie auf **Weiter**.

Das neu angelegte Unternehmenszertifikat wird in der Datenbank gespeichert.

## 6.2.5 Sicherungskopien von Zertifikaten erstellen

Für Recovery-Vorgänge müssen Sicherungskopien der erzeugten Sicherheitsbeauftragten- und Unternehmenszertifikate an einem sicheren Speicherort erstellt werden.

1. Geben Sie auf der Seite **Zertifikat-Sicherungskopie** einen Speicherort für die Sicherungskopien der Zertifikate ein.
2. Bestätigen Sie den Speicherort mit **Weiter**.

Am angegebenen Speicherort werden Sicherungskopien der Zertifikate erstellt.

**Hinweis:** Darüber hinaus empfehlen wir, die Zertifikate direkt nach der Erstkonfiguration an einen Speicherort zu exportieren, auf den im Notfall Zugriff besteht, z. B. auf einen USB-Stick. Sie benötigen diese Dateien, um eine zerstörte Installation oder Datenbank wiederherzustellen, siehe [Unternehmenszertifikat und Master Security Officer Zertifikat exportieren](#), Seite 52.

## 6.2.6 Standardrichtlinien erzeugen

Um den Verwaltungsaufwand zu reduzieren, stehen Standardrichtlinien zur Verfügung, die empfohlene Konfigurationseinstellungen abdecken. Während der Erstkonfiguration lässt sich ein Konfigurationspaket (MSI) erstellen, das diese Standardrichtlinie enthält. Für detaillierte Informationen zu Standardrichtlinien, siehe [Standardrichtlinien](#), Seite 70.

**Hinweis:** Die Standardrichtlinien lassen sich nur während der Erstkonfiguration des SafeGuard Policy Editor erstellen. Sie können die Standardrichtlinien jedoch je nach Anforderung später ändern oder neue benutzerdefinierte Richtlinien anlegen.

1. Stellen Sie auf der Seite **Standardrichtlinie** sicher, dass die Option **Standardrichtlinie erzeugen** aktiviert ist.
2. Geben Sie einen Speicherort für das Konfigurationspaket (MSI), das mit den Standardrichtlinien erstellt wird, an oder bestätigen Sie den Standardpfad.
3. Bestätigen Sie mit **Weiter**.

Die Richtliniengruppe wird im **Richtlinien** Navigationsbereich des SafeGuard Policy Editor angezeigt. Das Konfigurationspaket wird im SafeGuard Policy Editor unter **Konfigurationspakete** angezeigt. Installieren Sie das Paket bei der Installation der Verschlüsselungssoftware auf den Endpoint-Computern. Wenn die Standardkonfiguration nicht Ihren Wünschen entspricht, können Sie zusätzliche Richtlinien erstellen, ein Konfigurationspaket dafür erstellen und dieses an die Endpoint-Computer verteilen.

## 6.2.7 Recovery-Schlüssel-Speicher anlegen

Für Recovery-Vorgänge für mit Sophos SafeGuard geschützte Computer müssen dem Helpdesk spezifische Schlüssel-Recovery-Dateien zur Verfügung stehen, zum Beispiel, wenn Benutzer ihr Kennwort vergessen haben. Auf jedem durch Sophos SafeGuard geschützten Computer wird eine Schlüssel-Recovery-Datei während der Installation von Sophos SafeGuard erzeugt.

Für die Durchführung eines Challenge/Response-Verfahrens ist es unerlässlich, die Datei in einer Netzwerkfreigabe abzulegen, um Sie dem Helpdesk zur Verfügung zustellen, und dem Helpdesk die entsprechenden Zugriffsrechte zu geben. Die Schlüssel-Recovery-Datei ist mit dem Unternehmenszertifikat verschlüsselt. Sie können Sie daher unbesorgt auf dem Netzwerk oder auf externen Medien ablegen.

1. Akzeptieren Sie auf der Seite **Recovery-Schlüssel** die **Standard-Einstellungen für die Netzwerkfreigabe**.

Dadurch werden die Netzwerkfreigabe SafeGuardRecoveryKeys\$ sowie ein Verzeichnis auf dem lokalen Computer angelegt. Hier werden die Recovery-Schlüssel automatisch gespeichert. Die Netzwerkfreigabe ist so konfiguriert, dass nur neue Dateien an den Speicherort geschrieben werden können. Je nach Anforderung können Sie den lokalen Pfad ändern. Die Netzwerkfreigabe muss sich auf einem Laufwerk befinden, das mit NTFS formatiert ist. Mit NTFS können die Zugriffsberechtigungen gemäß den jeweiligen Anforderungen eingestellt werden. Ist die Option **Einstellungen für die Netzwerkfreigabe** nicht aktiviert, so werden Sie auf dem verschlüsselten Computer aufgefordert, einen Speicherort für die Schlüssel-Recovery-Datei anzugeben.

**Hinweis:** Die Sophos SafeGuard Software versucht für ca. 4 Minuten, eine Verbindung zur Netzwerkfreigabe herzustellen. Schlägt dies fehl, so wird auf dem Computer eine Balloon-Meldung angezeigt und ein Fehler wird protokolliert. Bei jeder neuen Windows-Anmeldung wird wieder ein Versuch unternommen, bis eine Verbindung hergestellt ist, oder die Recovery-Schlüssel-Dateien manuell auf dem Computer gesichert werden.

2. Weisen Sie auf der Seite **Recovery-Schlüssel** dem Helpdesk die notwendigen Zugriffsrechte für die Recovery-Schlüssel-Netzwerkfreigabe zu: Bestätigen Sie die Standard-Berechtigungen mit **Weiter**. Der Zugriff auf die Recovery-Schlüssel wird über eine neue Windows-Gruppe mit der Bezeichnung „SafeGuardRecoveryKeyAccess“ verwaltet. Standardmäßig werden alle Mitglieder der Gruppe der lokalen Administratoren zu dieser Gruppe hinzugefügt. **Hinweis:** In einer Domänenumgebung umfasst dies auch die Gruppe der Domänenadministratoren, die wiederum ein Mitglied der Gruppe der lokalen Administratoren ist. Um die Gruppenmitglieder einzusehen oder zu ändern, klicken Sie auf **Berechtigungen**.

Im SafeGuard Policy Editor können Sie mehrere Richtlinien-Konfigurationspakete erstellen, z. B. ein Paket für Computer innerhalb einer Domänenumgebung und ein zusätzliches Paket für Standalone-Computer.

3. Klicken Sie auf **Weiter**.

Die Berechtigungen für die Netzwerkfreigabe werden gesetzt. Für weitere Informationen zu den Berechtigungen für die Netzwerkfreigabe, siehe [Berechtigungen für die Netzwerkfreigabe festlegen](#), Seite 28.

## 6.2.8 Berechtigungen für die Netzwerkfreigabe festlegen

1. Führen Sie unter **Berechtigungen für Netzwerkfreigabe** einen der beiden folgenden Schritte aus:
  - Klicken Sie auf **Lokale Mitglieder hinzufügen**, um lokale Mitglieder mit administrativen Rechten für Recovery-Vorgänge hinzuzufügen.
  - Klicken Sie auf **Globale Mitglieder hinzufügen**, um globale Mitglieder mit administrativen Rechten für Recovery-Vorgänge hinzuzufügen.

2. Klicken Sie auf **OK**.

Die Gruppe "SafeGuardRecoveryKeyAccess" wird auf dem lokalen Computer erzeugt. Diese Gruppe enthält alle Mitglieder, die unter **Berechtigungen für Netzwerkfreigabe** angezeigt werden.

Die folgenden NTFS Berechtigungen werden automatisch im angegebenen lokalen Verzeichnis gesetzt:

- **Alle:** Dateien erzeugen- Auf Sophos SafeGuard Computer, für die der angemeldete Benutzer der Besitzer ist, können Dateien hinzugefügt werden. Es ist nicht erlaubt, Verzeichnisse zu durchsuchen, Dateien zu lesen oder zu löschen. Die Berechtigung, "Dateien erzeugen" steht über Erweiterte Sicherheitseinstellungen eines Verzeichnisses zur Verfügung.
- **SafeGuardRecoveryKeyAccess:** Ändern - Alle im Dialog **Berechtigungen** aufgeführten Benutzer haben das Recht, Dateien zu lesen, zu löschen und hinzuzufügen.
- **Administratoren :** Vollständige Kontrolle

Sophos SafeGuard entfernt auch die Vererbung von Berechtigungen in dem Verzeichnis, so dass die oben erwähnten Berechtigungen nicht versehentlich überschrieben werden können.

Die Netzwerkfreigabe SafeGuardRecoveryKeys\$ wird mit folgenden Berechtigungen versehen:

- **Alle:** Volle Kontrolle

**Hinweis:** Diese Berechtigungen sind die Schnittmenge zwischen NTFS und Share-Berechtigungen. Da die NTFS Berechtigungen restriktiver sind, gelten diese.

Wenn Sie eine Netzwerkfreigabe manuell erstellen möchten, empfehlen wir, die oben angegebenen Berechtigungen zu setzen. Achten Sie in diesem Fall darauf, die Vererbung von Berechtigungen manuell zu deaktivieren.

## 6.2.9 Erstkonfiguration abschließen

1. Klicken Sie auf **Beenden**, um die Konfiguration abzuschließen. Sobald der Konfigurationsassistent geschlossen ist, wird der SafeGuard Policy Editor gestartet.

Die Erstkonfiguration im SafeGuard Policy Editor ist abgeschlossen. Zwei Dateien mit den Bezeichnungen Networkshare.xml und ConfigurationOutput.xml werden im Temp-Pfad gespeichert. Die Datei Networkshare.xml enthält die Konfigurationseinstellungen aus den Seiten des Assistenten. In der Datei ConfigurationOutput.xml werden alle Ereignisse protokolliert, die während der Verarbeitung der Konfigurationseinstellungen aufgetreten sind. Die Ereignisse werden auf der letzten Seite des SafeGuard Policy Editor Konfigurationsassistenten angezeigt.

## 6.3 Konfigurieren zusätzlicher Instanzen des SafeGuard Policy Editor

Sie können zusätzliche Instanzen des SafeGuard Policy Editor konfigurieren, um dem Sophos SafeGuard Helpdesk Team den Zugriff für die Durchführung von Recovery-Aufgaben zu ermöglichen.

1. Starten Sie den SafeGuard Policy Editor auf dem entsprechenden Computer. Der Konfigurationsassistent wird gestartet und führt Sie durch die notwendigen Schritte.
2. Bestätigen Sie die **Willkommen**-Seite mit **Weiter**.
3. Aktivieren Sie auf der **Datenbank**-Seite die Option **Vorhandene Datenbank verwenden**. Wählen Sie unter **Datenbankeinstellungen** den relevanten Datenbanknamen aus der Liste aus. Klicken Sie auf **Ändern**, um die SQL-Server-Instanz auszuwählen, die Sie benutzen möchten. Es wird ein Dialog angezeigt, in dem Sie die Verbindung zur ausgewählten Instanz konfigurieren müssen.
4. Wählen Sie im Dialog **Datenbankverbindung** unter **Datenbankserver** die erforderliche SQL-Datenbankinstanz aus der Liste aus. Alle auf Ihrem Computer oder Netzwerk verfügbaren Datenbankserver werden angezeigt. (Die Liste wird alle 12 Minuten aktualisiert.) Aktivieren Sie **SSL verwenden**, um die Verbindung zu diesem Datenbankserver mit SSL abzusichern. Dies kann sich als nützlich erweisen, wenn die Maschinenzertifikate vor der Installation von Sophos SafeGuard auf dem Datenbankserver implementiert werden.
5. Wählen Sie unter **Authentisierung** die Art der Authentisierung, die für den Zugriff auf die Datenbank benutzt werden soll:
  - Aktivieren Sie **Windows NT Authentisierung verwenden**, um Ihre Windows-Anmelddaten zu verwenden.

**Hinweis:** Verwenden Sie diese Art der Anmeldung, wenn Ihr Computer Teil einer Domäne ist. In diesem Fall sind jedoch u. U. zusätzliche Konfigurationsschritte notwendig, da der Benutzer dazu berechtigt sein muss, eine Verbindung mit der Datenbank herzustellen.

- Aktivieren Sie **SQL Server Authentisierung verwenden**, um mit Ihren SQL-Anmeldeinformationen auf die Datenbank zuzugreifen. Sie werden dazu aufgefordert, Ihre Anmeldeinformationen einzugeben und zu bestätigen. Falls nötig, erhalten Sie diese von Ihrem SQL-Administrator.

**Hinweis:** Verwenden Sie diese Art der Anmeldung, wenn Ihr Computer keiner Domäne angehört. Stellen Sie in diesem Fall sicher, dass die Option **SSL verwenden** aktiviert ist, um die Verbindung zum und vom Datenbankserver abzusichern. Hierzu ist jedoch auf dem Computer, auf dem sich die ausgewählte SQL-Datenbank befindet, eine funktionierende SSL-Umgebung notwendig. Diese müssen Sie vorab anlegen. Weitere Informationen hierzu finden Sie in unserer Wissensdatenbank: <http://www.sophos.de/support/knowledgebase/article/108339.html>.

6. Klicken Sie auf **Verbindung prüfen**. Wenn die Verbindung zur SQL-Datenbank hergestellt ist, wird eine entsprechende Erfolgsmeldung angezeigt.
7. Bestätigen Sie zweimal mit **OK**, um auf die **Datenbank**-Seite zurückzukehren. Klicken Sie dann auf **Weiter**.
8. Wählen Sie auf der **Sicherheitsbeauftragter**-Seite **Importieren**, um das mit der ausgewählten Datenbank verbundene Sicherheitsbeauftragten-Zertifikat zu importieren. Suchen Sie nach dem erforderlichen Zertifikat und bestätigen Sie es mit **Öffnen**.  
Es können nur Zertifikate importiert werden, die durch den SafeGuard Policy Editor generiert wurden. Zertifikate, die von einer PKI (z.B. Verisign) erstellt wurden, sind nicht zulässig.
9. Geben Sie das Kennwort für den Zertifikatsspeicher ein.
10. Klicken Sie auf **Weiter** und danach auf **Beenden**, um den SafeGuard Policy Editor Konfigurationsassistenten abzuschließen.

## 6.4 Sophos SafeGuard auf Endpoint-Computern einrichten

Je nach Installation stehen auf den Endpoint-Computern unterschiedliche Sophos SafeGuard Module zur Verfügung, siehe *Sophos SafeGuard auf Endpoint-Computern*, Seite 8.

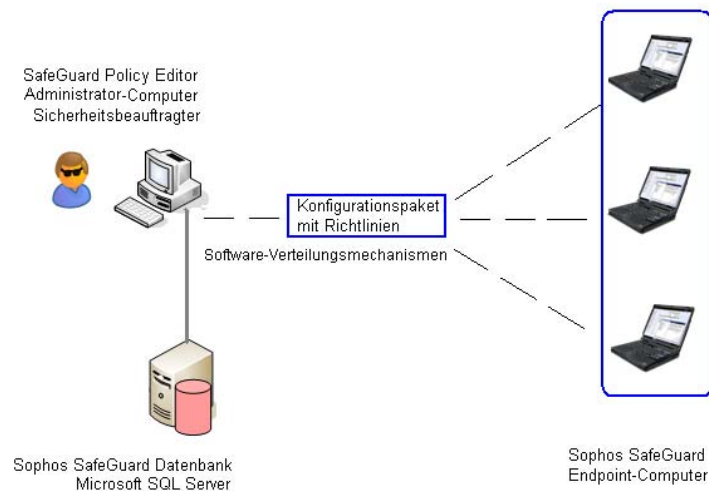
Für die Installation und das Einrichten von Sophos SafeGuard auf Endpoint-Computern gibt es verschiedene Methoden:

Sicherheitsbeauftragte können Sophos SafeGuard lokal auf den Endpoint-Computern einrichten, oder die Installation und Erstkonfiguration der Endpoint-Computer im Rahmen einer zentralisierten Software-Verteilung vornehmen. Dadurch wird eine standardisierte Installation auf mehreren Computern erreicht.

Die verschiedenen Optionen für das Installieren und Einrichten der Software werden auch in folgendem Knowledgebase-Artikel beschrieben: <http://www.sophos.de/support/knowledgebase/article/108426.html>

Informationen zum Verhalten des Computers nach der Installation von Sophos SafeGuard finden Sie in der Startup-Anleitung (Kapitel *Erste Anmeldung nach der Installation von Sophos SafeGuard*) sowie in der Benutzerhilfe (Kapitel *Erste Anmeldung nach der Installation von Sophos SafeGuard, Exemplarische Anmeldung eines Benutzers an der POA und Datenverschlüsselung*).

### Sophos SafeGuard Komponenten



#### 6.4.1 Einschränkungen

- Wenn auf dem Computer Intel Advanced Host Controller Interface (AHCI) benutzt wird, so muss sich die Boot-Festplatte in Slot 0 oder Slot 1 befinden. Sie können bis zu 32 Festplatten einlegen. Sophos SafeGuard läuft nur auf den ersten beiden Slot-Nummern.
- Dynamische Festplatten und GUID Partitionstabellen (GPT)-Platten werden nicht unterstützt. Die Installation bricht in diesem Fall ab. Wenn diese Platten nachträglich im System auftauchen, werden sie nicht unterstützt.
- Systeme mit Festplatten, die über einen SCSI Bus angeschlossen sind, werden vom Sophos SafeGuard Device Encryption Modul nicht unterstützt.

## 6.4.2 Endpoint-Computer lokal einrichten

Wenn Sie erst eine Probeinstallation auf einem Endpoint-Computer durchführen möchten, ist es sinnvoll, Sophos SafeGuard zunächst lokal zu installieren.

Bevor Sie die Verschlüsselungssoftware installieren, führen Sie erst die vorbereitenden Schritte für die Installation auf dem Endpoint-Computer durch (siehe [Installation vorbereiten](#), Seite 16).

1. Melden Sie sich an dem Computer als Administrator an.
2. Installieren Sie das vorbereitende MSI-Paket SGxClientPreinstall.msi, das den Endpoint-Computer mit den nötigen Voraussetzungen für eine erfolgreiche Installation der Verschlüsselungs-Software ausstattet, zum Beispiel mit den relevanten DLLs.  
**Note:** Alternativ können Sie auch vcredist\_x86.exe installieren, das Sie hier herunterladen können: <http://www.microsoft.com/downloads/details.aspx?FamilyID=766a6af7-ec73-40ff-b072-9112bab119c2> oder sicherstellen, dass sich MSVCR80.dll, Version 8.0.50727.4053 im Verzeichnis Windows\WinSxS auf dem Computer befindet.
3. Klicken Sie auf dem relevanten „Client“-MSI-Paket doppelt, um den Installationsassistenten der Verschlüsselungssoftware zu starten. Dieser führt Sie durch die notwendigen Schritte. Installieren Sie eines der folgenden Pakete:

Sophos SafeGuard Disk Encryption	Sophos SafeGuard Easy
SDEClient.msi für die 32-Bit-Variante SDEClient_x64.msi für die 64-Bit-Variante	SGNClient.msi für die 32-Bit-Variante SGNClient_x64.msi für die 64-Bit-Variante SGNClient_withoutDE.msi nur für SafeGuard Data Exchange, 32-Bit-Variante SGNClient_withoutDE_x64.msi nur für SafeGuard Data Exchange, 64-Bit-Variante

4. Übernehmen Sie in den folgenden Dialogen die Standardeinstellungen.
5. Falls Sie dazu aufgefordert werden, wählen Sie den Installationstyp. Wenn Sie SGNClient.msi oder SGNClient\_x64.msi installieren, führen Sie einen der folgenden Schritte aus:
  - Wählen Sie **Vollständig**, um sowohl Device Protection als auch Data Exchange zu installieren.
  - Wählen Sie **Typisch**, um nur Device Encryption zu installieren.
  - Wählen Sie **Angepasst**, um Features gemäß Ihren Anforderungen zu aktivieren.

Das Feature **Data Exchange** ist mit ESDP nicht verfügbar.

6. Übernehmen Sie in allen weiteren Dialogen die Standardeinstellungen.

Sophos SafeGuard ist auf dem Endpoint-Computer installiert.

7. Konfigurieren Sie die Verschlüsselungssoftware gemäß Ihren Anforderungen im SafeGuard Policy Editor:

- Verwenden Sie die vordefinierten Standardrichtlinien, die Sie während der Erstkonfiguration im SafeGuard Policy Editor Konfigurationsassistenten erstellt haben, für die schnelle und einfache Umsetzung von Sicherheitsrichtlinien auf dem Endpoint-Computer.
- Sollten die Standardrichtlinien nicht alle Ihre spezifischen Anforderungen abdecken, erstellen Sie Ihre eigenen Richtlinien im SafeGuard Policy Editor und erstellen Sie dafür ein neues Konfigurationspaket. (siehe *Mit Richtlinien arbeiten*, Seite 45). Für Details zur Verteilung und Umsetzung von Richtlinien auf den Endpoint-Computern, siehe *Mit Konfigurationspaketen arbeiten*, Seite 50.

So kann es zum Beispiel zur Umsetzung Ihrer Strategie für den Einsatz von Sophos SafeGuard notwendig sein, einen administrativen Zugang für Mitarbeiter des IT-Teams auf den Computer einzurichten. Hierzu müssen Sie eine spezifische Richtlinie definieren und dafür ein neues Konfigurationspaket erstellen, in dem diese enthalten sind.

8. Installieren Sie das relevante Konfigurationspaket (MSI) auf dem Computer.

Sophos SafeGuard ist auf dem Computer eingerichtet. Informationen zum Verhalten des Computers nach der Installation von Sophos SafeGuard finden Sie in der Benutzerhilfe (Kapitel *Erste Anmeldung nach der Installation von Sophos SafeGuard, Exemplarische Anmeldung eines Benutzers an der POA und Datenverschlüsselung*).

### 6.4.3 Endpoint-Computer zentral einrichten

Durch das zentrale Einrichten von Endpoint-Computern wird eine standardisierte Installation auf mehreren Computern erreicht. Bevor Sie die Verschlüsselungs-Software einrichten, führen Sie erst die vorbereitenden Schritte für die Installation auf dem Endpoint-Computer durch, siehe [Installation vorbereiten](#), Seite 16.

1. Erstellen Sie mit Hilfe Ihrer eigenen Tools ein Paket, das auf den Endpoint-Computern installiert werden soll. Das Paket muss folgende Komponenten enthalten:

- **Vorbereitendes Sophos SafeGuard Installationspaket**

Installieren Sie SGxClientPreinstall.msi. Das Paket stattet die Endpoint-Computer mit den nötigen Voraussetzungen für eine erfolgreiche Installation der Verschlüsselungs-Software aus, zum Beispiel mit der benötigten DLL MSVCR80.dll, Version 8.0.50727.4053.

**Hinweis:** Wenn dieses Paket nicht installiert wird, bricht die Installation der Verschlüsselungs-Software ab.

- **Installationspaket mit Sophos SafeGuard Verschlüsselungs-Software**

Sie finden dieses Installationspaket im Produktordner, den Sie von der Sophos Webseite heruntergeladen haben oder auf der Produkt-CD.

Für Informationen zu den verfügbaren Installationspaketen, siehe [Installation](#), Seite 20

- **Konfigurationspaket(e)**

Konfigurieren Sie die Verschlüsselungs-Software nach Ihren Wünschen:

Verwenden Sie das Konfigurationspaket mit vordefinierten Standardrichtlinien, das während der Erstkonfiguration im SafeGuard Policy Editor Konfigurationsassistenten erstellt wurde.

- Sollten die Standardrichtlinien nicht alle Ihre spezifischen Anforderungen abdecken, erstellen Sie Ihre eigenen Richtlinien und erzeugen Sie dafür ein Konfigurationspaket im SafeGuard Policy Editor (siehe [Mit Richtlinien arbeiten](#), Seite 45). Für Details zur Verteilung und Umsetzung von Richtlinien auf den Endpoint-Computern, siehe [Mit Konfigurationspaketen arbeiten](#), Seite 50.

So kann es zum Beispiel zur Umsetzung Ihrer Strategie für den Einsatz von Sophos SafeGuard notwendig sein, den administrativen Zugang für Mitarbeiter des IT-Teams auf den Computern einzurichten. Hierzu müssen Sie eine spezifische Richtlinie definieren und sie in einem Konfigurationspaket an den Computer übertragen.

#### ■ Skript mit Befehlen für die automatische Installation

Verwenden Sie den Windows Installer Befehl `msiexec`, um das Skript zu erstellen. Für weitere Informationen zu `msiexec` siehe *Kommando für zentrale Installation*, Seite 36 oder [http://msdn.microsoft.com/en-us/library/aa367988\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/aa367988(VS.85).aspx).

2. Erstellen Sie ein Verzeichnis mit der Bezeichnung Software als zentralen Speicherort für alle Anwendungen.
3. Erstellen Sie das Skript: Geben Sie das Windows Installer Kommando `msiexec` mit den entsprechenden Parametern an der Kommandozeile ein.
4. Verteilen Sie dieses Paket über unternehmenseigene Software-Verteilungsmechanismen an die Endpoint-Computer.

Zusätzliche Konfiguration kann erforderlich sein, damit sich die POA auf jeder Hardware-Plattform korrekt verhält. Die meisten Hardware-Konflikte lassen sich mit Hilfe von "Hotkeys"-Funktionalitäten beheben, die in die POA integriert sind. Hotkeys können nach der Installation konfiguriert werden, entweder in der POA selbst oder über eine zusätzliche Konfigurationseinstellung, die dem `msiexec` Installationstool mitgegeben wird. Für weitere Informationen, siehe *In der Power-on Authentication unterstützte Hotkeys*, Seite 127 sowie die folgenden Wissensdatenbank-Artikel:

<http://www.sophos.com/support/knowledgebase/article/107781.html>

<http://www.sophos.com/support/knowledgebase/article/107785.html>

#### 6.4.3.1 Kommando für zentrale Installation

Verwenden Sie zur zentralen Installation von Sophos SafeGuard auf den Endpoint-Computern die Windows Installer Komponente „`msiexec`“. „`msiexec`“ ist in Windows, XP, Vista und Windows 7 bereits integriert und führt eine vorgefertigte Sophos SafeGuard Installation automatisch aus. Da auch die Quelle und das Ziel für die Installation angegeben werden können, besteht die Möglichkeit zur einheitlichen Installation an mehreren Endpoint-Computern.

Weitere Informationen zu `msiexec` finden Sie unter: [http://msdn.microsoft.com/en-us/library/aa367988\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/aa367988(VS.85).aspx).

#### Kommandozeilensyntax

```
msiexec /i <Pfad+msi Paketname> /qn ADDLOCAL=ALL | <Features>  
<Parameter>
```

Die Kommandozeilensyntax setzt sich folgendermaßen zusammen:

- Windows Installer Parameter, die z.B. Warnungen und Fehlermeldungen während der Installation in eine Datei protokollieren.
- Sophos SafeGuard Features, die installiert werden sollen, z. B. volume-basierende Verschlüsselung.
- Sophos SafeGuard Parameters, z. B. zur Spezifikation des Installationsverzeichnisses.

### Kommandooptionen

Alle verfügbaren Optionen können Sie über msixexec.exe in der Eingabeaufforderung abrufen. Im Folgenden sind wichtige Optionen beschrieben.

Option	Beschreibung
/i	Gibt an, dass es sich um eine Installation handelt.
/qn	Installiert ohne Benutzerinteraktion und zeigt keine Benutzeroberfläche an.
ADDLOCAL=	Listet die Features auf, die installiert werden. Wird die Option nicht angegeben, werden alle Features installiert, die für eine Standardinstallation vorgesehen sind. Beachten Sie bei der Auflistung der Features unter ADDLOCAL Folgendes:- Trennen Sie die Features nur mit einem Komma, nicht mit einem Leerzeichen. - Beachten Sie Groß- und Kleinschreibung. - Wenn Sie ein Feature auswählen, müssen Sie auch alle übergeordneten Features (Feature Parents) zur Kommandozeile hinzufügen!
ADDLOCAL=ALL	Installiert alle verfügbaren Features
REBOOT=Force   ReallySuppress	Erzwingt oder unterdrückt Neustart nach Installation. Ohne Angabe wird der Neustart erzwungen (Force).
/L* <path + filename>	Protokolliert alle Warnungen und Fehlermeldungen in die angegebene Protokolldatei. Der Parameter protokolliert ausschließlich Fehlermeldungen /Le <Pfad + Dateiname>.
Installdir= <directory>	Gibt das Verzeichnis an, in das Sophos SafeGuard Client installiert wird. Ohne Angabe wird als Standardinstallationsverzeichnis <SYSTEM>:\PROGRAM FILES\SOPHOS verwendet.

### 6.4.3.2 Sophos SafeGuard Features (ADDLOCAL)

Für eine zentrale Installation müssen Sie bereits im Vorfeld definieren, welche Sophos SafeGuard Features auf den Endpoint-Computern installiert werden sollen. Die Features werden der Option ADDLOCAL mitgegeben.

In den folgenden Tabellen sind alle Sophos SafeGuard Features aufgelistet, die auf den Endpoint-Computern installiert werden können.

#### Features für SafeGuard Device Encryption

**Hinweis:** SGNClient.msi, SDEClient.msi oder die jeweiligen 64 Bit-Varianten.

**Hinweis:** Die Features **Client** und **Authentication** müssen standardmäßig installiert werden. Wenn Sie ein Feature auswählen, müssen Sie auch alle übergeordneten Features (Feature Parents) zur Kommandozeile hinzufügen!

Feature Parents	Feature
<b>Client</b>	<b>Authentication</b> Das Feature <b>Authentication</b> und sein Feature Parent <b>Client</b> müssen standardmäßig installiert werden.
<b>Client, Authentication</b>	<b>CredentialProvider</b> Für Computer mit Windows Vista müssen Sie dieses Feature installieren. Es dient zur Anmeldung über den Credential Provider.
<b>Client, BaseEncryption</b>	<b>SectorBasedEncryption</b> Installiert die volume-basierende Verschlüsselung von Sophos SafeGuard mit den folgenden Funktionen: Alle Volumes, auch Wechselmedien, lassen sich mit der volumebasierenden Verschlüsselung von Sophos SafeGuard verschlüsseln. Sophos SafeGuard Power-on Authentication (POA), Sophos SafeGuard Recovery mit Challenge/Response
<b>Client</b>	<b>SecureDataExchange</b> <b>Hinweis:</b> Dieses Feature wird mit ESDP nicht unterstützt. SafeGuard Data Exchange mit dateibasierender Verschlüsselung wird immer auf lokaler Ebene und für Wechselmedien installiert. SafeGuard Data Exchange sorgt für die sichere Verschlüsselung von Wechselmedien. Daten können sicher und einfach mit anderen Benutzern ausgetauscht werden. Alle Ver- und Entschlüsselungsvorgänge laufen transparent und mit minimaler Benutzerinteraktion ab. Wenn Sie SafeGuard Data Exchange auf Ihrem Computer installiert haben, ist auch SafeGuard Portable installiert. SafeGuard Portable ermöglicht den sicheren Datenaustausch mit Computern, auf denen SafeGuard Data Exchange nicht installiert ist.

## Features für SafeGuard Data Exchange

SGNClient\_withoutDE.msi, SGNClient\_withoutDE\_x64.msi.

**Hinweis:** Diese Installationspakete werden mit ESDP nicht unterstützt.

**Hinweis:** Die Features **Client** und **Authentication** müssen standardmäßig installiert werden. Wenn Sie ein Feature auswählen, müssen Sie auch alle übergeordneten Features (Feature Parents) zur Kommandozeile hinzufügen!

Feature Parents	Feature
<b>Client</b>	<b>Authentication</b> Das Feature <b>Authentication</b> und sein Feature Parent <b>Client</b> müssen standardmäßig installiert werden.
<b>Client</b>	<b>SecureDataExchange</b> <b>Hinweis:</b> Dieses Feature wird mit ESDP nicht unterstützt. SafeGuard Data Exchange mit dateibasierender Verschlüsselung wird immer auf lokaler Ebene und für Wechselmedien installiert. SafeGuard Data Exchange sorgt für die sichere Verschlüsselung von Wechselmedien. Daten können sicher und einfach mit anderen Benutzern ausgetauscht werden. Alle Ver- und Entschlüsselungsvorgänge laufen transparent und mit minimaler Benutzerinteraktion ab. Wenn Sie SafeGuard Data Exchange auf Ihrem Computer installiert haben, ist auch SafeGuard Portable installiert. SafeGuard Portable ermöglicht den sicheren Datenaustausch mit Computern, auf denen SafeGuard Data Exchange nicht installiert ist.

## Beispielkommando für volume-basierende Verschlüsselung

Folgendes wird durch das unten aufgeführte Kommando ausgeführt:

- Die Endpoint-Computer werden mit den nötigen Voraussetzungen für eine erfolgreiche Installation der Verschlüsselungs-Software ausgestattet.
- Die Sophos SafeGuard Power-on Authentication wird installiert, über die sich die Benutzer an durch Sophos SafeGuard geschützten Computern anmelden.
- Die Sophos SafeGuard volume-basierende Verschlüsselung wird installiert.
- Es wird eine Protokolldatei angelegt.
- Das Standard-Konfigurationspaket wird ausgeführt.

**Beispiel:**

```
msiexec /i F:\Software\SGxClientPreinstall.msi /qn /log  
I:\Temp\SGxClientPreinstall.log  
  
msiexec /i F:\Software\SGNClient.msi /qn /log I:\Temp\SGNClient.log  
  
ADDLOCAL=Client,Authentication,BaseEncryption,SectorBasedEncryption  
  
InstallDir=C:\Programme\Sophos\Sophos SafeGuard  
  
msiexec /i F:\Software\StandardConfig.msi /qn /log  
I:\Temp\StandardConfig.log
```

#### **6.4.4 FIPS-konforme Installation**

Die FIPS-Zertifizierung beschreibt Sicherheitsanforderungen für Verschlüsselungsmodule. Beispielsweise verlangen Regierungsbehörden in den USA und in Kanada FIPS 140-2-zertifizierte Software für besonders sicherheitskritische Informationen.

Sophos SafeGuard verwendet FIPS-zertifizierte Algorithmen für die Verschlüsselung. Bei den AES Algorithmen wird standardmäßig eine neue, schnellere Implementierung installiert, die noch nicht FIPS-zertifiziert ist.

Wenn Sie die FIPS-zertifizierte Variant der AES Algorithmen nutzen wollen, setzen Sie für die Installation des Sophos SafeGuard Client die Property FIPS\_AES auf 1.

Dies können Sie auf zwei Arten durchführen:

- Fügen Sie die Property dem Kommandozeilen-Skript hinzu:

```
msiexec /i F:\Software\SGNClient.msi FIPS_AES=1
```

- Verwenden Sie eine sogenannte Transformation.

## 7 Sophos SafeGuard auf einem Computer mit mehreren Betriebssystemen installieren

**Hinweis:** Diese Funktion wird für ESDP (Endpoint Security and Data Protection) nicht unterstützt.

Der Sophos SafeGuard kann auch dann auf einem Computer zum Schutz der Daten installiert werden, wenn mehrere Betriebssysteme auf separaten Volumes der Festplatte installiert sind. Sophos SafeGuard bietet ein sogenanntes „Runtime“-System. Sophos SafeGuard Runtime stellt folgendes sicher, wenn es auf Volumes mit einer zusätzlichen Windows-Installation installiert wird:

- Die Windows-Installation, die sich auf diesen Volumes befindet, kann erfolgreich durch einen Boot Manager gestartet werden.
- Auf Partitionen dieser Volumes, die durch eine vollständige Sophos SafeGuard Client Installation mit dem definierten Computerschlüssel verschlüsselt worden sind, kann erfolgreich zugegriffen werden.

### 7.1 Voraussetzungen und Einschränkungen

Beachten Sie folgendes:

- Sophos SafeGuard Runtime bietet keine Sophos SafeGuard-spezifischen Features oder Funktionalitäten.
- Sophos SafeGuard Runtime unterstützt nur die Betriebssysteme, die auch für die Sophos SafeGuard Client Verschlüsselungssoftware unterstützt werden.
- USB-Tastaturen können unter Umständen nur eingeschränkt benutzt werden.
- Es werden nur Boot Manager unterstützt, die nach der Power-on Authentication aktiv werden.
- Die Unterstützung von Boot Managern von Drittanbietern wird nicht garantiert. Wir empfehlen den Einsatz von Microsoft Boot Managern.
- Sophos SafeGuard Runtime kann nicht auf einen Sophos SafeGuard Client in Vollversion aktualisiert werden.
- Das Runtime-Installationspaket muss vor der Vollversion des Sophos SafeGuard Client Installationspakets installiert werden.
- Es kann nur auf Volumes, die mit dem definierten Computerschlüssel in Sophos SafeGuard verschlüsselt wurden, zugegriffen werden.

## 7.2 Vorbereitung

Um Sophos SafeGuard Runtime einzurichten, führen Sie die folgenden vorbereitenden Schritte in der angegebenen Reihenfolge durch:

1. Stellen Sie sicher, dass die Volumes, auf denen Sophos SafeGuard Runtime laufen soll, zum Zeitpunkt der Installation sichtbar sind und mit ihrem Windows-Namen (z. B. C:) angesprochen werden können..
2. Legen Sie fest, auf welchem Volume/welchen Volumes der Festplatte Sophos SafeGuard Runtime installiert werden soll. In Zusammenhang mit Sophos SafeGuard sind diese Volumes als "sekundäre" Windows-Installationen definiert. Es können mehrere sekundäre Windows-Installationen vorhanden sein. Verwenden Sie folgendes Paket: SGNClientRuntime.msi (oder SGNClientRuntime\_x64.msi, wenn das Betriebssystem des Computers Windows 7 64 Bit oder Windows Vista 64 Bit ist).
3. Legen Sie fest, auf welchem Volume der Festplatte die Vollversion des Sophos SafeGuard Clients installiert werden soll. In Zusammenhang mit Sophos SafeGuard ist dieses Volume als "primäre" Windows-Installation definiert. Es kann jeweils nur eine primäre Windows-Installation geben.. Verwenden Sie folgendes Paket: SGNClient.msi (SGNClient\_x64.msi, wenn das Betriebssystem des Computers Windows 7 64 Bit oder Windows Vista 64 Bit ist).

## 7.3 Sophos SafeGuard Runtime einrichten

Gehen Sie wie folgt vor:

1. Wählen Sie das/die gewünschte(n) Volume(s) der Festplatte aus, auf dem/denen Sie Sophos SafeGuard Runtime installieren möchten.
2. Starten Sie die sekundäre Windows-Installation auf dem ausgewählten Volume.
3. Installieren Sie das Client Runtime-Installationspaket auf dem ausgewählten Volume.
4. Bestätigen Sie die Standardeinstellungen im nächsten Dialog des Installers. Hier ist keine spezielle Funktionsauswahl notwendig.
5. Wählen Sie einen Installationsordner für die Runtime-Installation.
6. Bestätigen Sie, dass die Runtime-Installation abgeschlossen werden soll.
7. Wählen Sie das primäre Volume der Festplatte, auf dem der Sophos SafeGuard Client installiert werden soll.
8. Starten Sie die primäre Windows-Installation auf dem ausgewählten Volume.

9. Starten Sie das vorbereitende Installationspaket SGxClientPreinstall.msi, um die Endpoint-Computer mit notwendigen Voraussetzungen für die erfolgreiche Installation der Verschlüsselungssoftware (z. B. relevante DLLs) auszustatten.
10. Installieren Sie das entsprechende Sophos SafeGuard Client Installationspaket auf dem ausgewählten Volume.
11. Erstellen Sie das Konfigurationspaket und verteilen Sie es an den Endpoint-Computer.
12. Verschlüsseln Sie beide Volumes mit dem definierten Computerschlüssel.

## **7.4 Von einem sekundären Volume über einen Boot Manager booten**

Gehen Sie wie folgt vor:

1. Starten Sie den Computer.
2. Melden Sie sich an der Power-on Authentication mit Ihren Anmeldeinformationen an.
3. Starten Sie den Boot Manager und wählen Sie das gewünschte sekundäre Volume als Boot-Laufwerk.
4. Starten Sie den Computer von diesem Volume aus neu.

Auf jedes Volume, das mit dem definierten Computerschlüssel verschlüsselt ist, kann zugegriffen werden.

## **8 Am SafeGuard Policy Editor anmelden**

So melden Sie sich am SafeGuard Policy Editor an:

1. Starten Sie den SafeGuard Policy Editor. Ein Anmeldebildschirm wird angezeigt.
2. Geben Sie das während der Konfiguration festgelegte Sicherheitsbeauftragten-Kennwort ein und bestätigen Sie es mit **OK**.

Der SafeGuard Policy Editor wird geöffnet.

## 9 Mit Richtlinien arbeiten

Die folgenden Abschnitte beschreiben richtlinienrelevanten Vorgänge, z. B. das Erstellen, Gruppieren und Sichern von Richtlinien.

Während der Erstkonfiguration im SafeGuard Policy Editor wird bereits ein vorkonfigurierter Satz mit Standardrichtlinien erstellt, siehe [Erstkonfiguration im SafeGuard Policy Editor Konfigurationsassistent durchführen](#), Seite 22. Für eine detaillierte Beschreibung der Standardrichtlinien, siehe [Standardrichtlinien](#), Seite 70.

Für eine Beschreibung aller Sophos SafeGuard verfügbaren Richtlinieneinstellungen, siehe [Richtlinieneinstellungen](#), Seite 80.

### 9.1 Richtlinien anlegen

So legen Sie eine neue Richtlinie an:

1. Melden Sie sich mit dem Kennwort, das Sie während der Erstkonfiguration festgelegt haben, am SafeGuard Policy Editor an.
2. Klicken Sie auf die Schaltfläche **Richtlinien** im Navigationsbereich.
3. Klicken Sie im Navigationsfenster mit der rechten Maustaste auf **Richtlinien** und wählen Sie im Kontextmenü den Befehl **Neu**.
4. Wählen Sie den Richtlinientyp aus. Es wird ein Dialog für die Benennung der Richtlinie des ausgewählten Richtlinientyps angezeigt.
5. Geben Sie einen Namen und optional eine Beschreibung für die neue Richtlinie ein.

Richtlinien für den Geräteschutz:

Wenn Sie eine Richtlinie für den Geräteschutz anlegen wollen, müssen Sie in diesem Dialog auch das Ziel des Geräteschutzes angeben. Mögliche Ziele sind:

- Massenspeicher (Boot-Laufwerke/Andere Volumes)
- Wechselmedien (Dieses Ziel wird nur für SafeGuard Easy Installationen unterstützt.)
- Optische Laufwerke (Dieses Ziel wird nur für SafeGuard Easy Installationen unterstützt.)


Für jedes Ziel muss eine eigene Richtlinie angelegt werden. Sie können die einzelnen Richtlinien später z. B. zu einer Richtliniengruppe mit der Bezeichnung *Verschlüsselung* zusammenfassen.

6. Klicken Sie auf **OK**.

Die neu angelegte Richtlinie wird im Navigationsfenster unter **Richtlinien** angezeigt. Im Aktionsbereich werden alle Einstellungen für den gewählten Richtlinientyp angezeigt und können je nach Anforderung geändert werden.






## 9.2 RichtlinienEinstellungen bearbeiten

Wenn Sie im Navigationsfenster eine Richtlinie auswählen, können Sie deren Einstellungen im Aktionsbereich bearbeiten.

	Das rote Symbol vor dem Text „nicht konfiguriert“ gibt an, dass für diese Einstellung ein Wert festgelegt werden muss. Sie können die Richtlinie erst speichern, wenn Sie eine andere Einstellung als „nicht konfiguriert“ ausgewählt haben.
---	--

### 9.2.1 Einstellungen auf Standardwerte setzen

In der Symbolleiste stehen folgende Symbole für RichtlinienEinstellungen zur Verfügung:

	Zeigt die Standardwerte für nicht konfigurierte RichtlinienEinstellungen.
	Setzt die markierte RichtlinienEinstellung auf „nicht konfiguriert“.
	Setzt alle RichtlinienEinstellungen eines Bereichs auf „nicht konfiguriert“.
	Setzt den Standardwert für die markierte RichtlinienEinstellung.
	Setzt alle RichtlinienEinstellungen eines Bereichs auf den Standardwert.

### 9.2.2 Maschinen- und benutzerspezifische Richtlinien unterscheiden

Richtlinienfarbe blau	Richtlinie wird nur für Maschinen angewandt, nicht für Benutzer.
Richtlinienfarbe schwarz	Richtlinie wird für Maschinen und Benutzer angewandt.

## 9.3 Richtliniengruppen

Sophos SafeGuard Richtlinien müssen in Richtliniengruppen zusammengefasst werden, damit sie in einem Konfigurationspaket übertragen werden können. Eine Richtliniengruppe kann verschiedene Richtlinientypen enthalten.

Wenn Sie Richtlinien vom selben Typ in einer Gruppe zusammenfassen, werden die Einstellungen automatisch vereinigt. Sie können dafür eine Auswertungsreihenfolge festlegen. Die Einstellungen einer höher gereihten Richtlinie überschreiben jene einer niedriger priorisierten. Ist eine Einstellung auf **nicht konfiguriert** gesetzt, wird die Einstellung in einer niedriger priorisierten Richtlinie **nicht überschrieben**.

### Ausnahme Geräteschutz:

Richtlinien für den Geräteschutz werden nur vereinigt, wenn sie für dasselbe Ziel (z. B. Boot-Volume) angelegt werden. Weisen sie auf verschiedene Ziele, werden sie addiert.

### 9.3.1 Richtlinien zu Gruppen zusammenfassen

#### Voraussetzungen:

Die einzelnen Richtlinien der verschiedenen Typen müssen angelegt sein.

Sophos SafeGuard Richtlinien müssen zu Richtliniengruppen zusammengefasst werden, damit sie in einem Konfigurationspaket an die Endpoint-Computer übertragen werden können. Eine Richtliniengruppe kann verschiedene Richtlinientypen enthalten.

So fassen Sie Richtlinien in Gruppen zusammen:

1. Klicken Sie auf die Schaltfläche **Richtlinien** im Navigationsbereich.
2. Klicken Sie im Navigationsfenster mit der rechten Maustaste auf **Richtlinien-Gruppen** und wählen Sie **Neu**.
3. Klicken Sie auf **Neue Richtlinien-Gruppe**. Es wird ein Dialog für die Benennung der Richtlinien-Gruppe angezeigt.
4. Geben Sie einen eindeutigen Namen und optional eine Beschreibung für die Richtlinien-Gruppe ein. Klicken Sie auf **OK**.
5. Die neu angelegte Richtlinie-Gruppe wird im **Navigationsfenster** unter **Richtlinie-Gruppen** angezeigt.
6. Wählen Sie die Richtlinien-Gruppe aus. Im Aktionsbereich werden alle für das Gruppieren der Richtlinien notwendigen Elemente angezeigt.

7. Zum Gruppieren der Richtlinien ziehen Sie sie aus der Liste der verfügbaren Richtlinien in den Richtlinienbereich.
8. Sie können für jede Richtlinie eine **Priorität** festlegen, indem Sie die Richtlinie über das Kontextmenü nach oben oder unten reihen.

Wenn Sie Richtlinien vom selben Typ in einer Gruppe zusammenfassen, werden die Einstellungen automatisch vereinigt. Sie können dafür eine Auswertungsreihenfolge festlegen. Die Einstellungen einer höher gereihten Richtlinie überschreiben jene einer niedriger priorisierten. Ist eine Einstellung auf **nicht konfiguriert** gesetzt, wird die Einstellung in einer niedriger priorisierten Richtlinie **nicht überschrieben**.

**Ausnahme Geräteschutz:**

Richtlinien für den Geräteschutz werden nur vereinigt, wenn sie für dasselbe Ziel (z. B. Boot-Volumen) angelegt werden. Weisen sie auf verschiedene Ziele werden sie addiert.

9. Speichern Sie die Richtlinienengruppe über **Datei > Speichern**.

Die Richtlinienengruppe enthält nun die Einstellungen aller einzelnen Richtlinien. Erstellen Sie nun ein Konfigurationspaket, das die Richtlinienengruppe enthält.

### **9.3.2 Ergebnis der Gruppierung**

Das Ergebnis der Zusammenfassung wird in einer eigenen Ansicht dargestellt.

Klicken Sie zum Anzeigen der Zusammenfassung auf die Registerkarte **Ergebnis**.

- Für jeden Richtlinien-Typ steht eine eigene Registerkarte zur Verfügung.

Die aus der Zusammenfassung der einzelnen Richtlinien resultierenden Einstellungen werden angezeigt.

- Für Richtlinien zum Geräteschutz werden Registerkarten für jedes Ziel der Richtlinie angezeigt (z. B. Boot-Volumen, Laufwerk X: usw.).

## 9.4 Richtlinien und Richtliniengruppen sichern

Sie können Sicherungskopien von Richtlinien und Richtliniengruppen in Form von XML-Dateien erstellen. Falls notwendig, lassen sich die betreffenden Richtlinien/Richtliniengruppen daraufhin aus diesen XML-Dateien wiederherstellen.

So erstellen Sie eine Sicherungskopie von einer Richtlinie/Richtliniengruppe:

1. Markieren Sie die Richtlinie/Richtliniengruppe im Navigationsfenster unter **Richtlinien** bzw. **Richtlinien-Gruppen**.
2. Klicken Sie mit der rechten Maustaste und wählen Sie im angezeigten Kontextmenü **Richtlinie sichern**.  
Der Befehl **Richtlinie sichern** steht auch im Menü **Aktionen** zur Verfügung.
3. Geben Sie im Dialog **Speichern unter** einen Dateinamen für die XML-Datei an und wählen Sie das Verzeichnis aus, in dem die Datei gespeichert werden soll. Klicken Sie auf **Speichern**.

Die Sicherungskopie der Richtlinie/Richtliniengruppe ist im angegebenen Verzeichnis als XML-Datei abgelegt.

## 9.5 Richtlinien und Richtliniengruppen wiederherstellen

So stellen Sie eine Richtlinie/Richtliniengruppe aus einer XML-Datei wieder her:

1. Markieren Sie im Navigationsbereich **Richtlinien/Richtlinien-Gruppen**.
2. Klicken Sie mit der rechten Maustaste und wählen Sie im angezeigten Kontextmenü **Richtlinie wiederherstellen**.  
Der Befehl **Richtlinie wiederherstellen** steht auch im Menü **Aktionen** zur Verfügung.
3. Wählen Sie die XML-Datei für die Wiederherstellung der Richtlinie/Richtliniengruppe aus und klicken Sie auf **Öffnen**.

Die Richtlinie/Richtliniengruppe ist wiederhergestellt.

## 10 Mit Konfigurationspaketen arbeiten

Durch Sophos SafeGuard geschützte Computer erhalten ihre Verschlüsselungsrichtlinien über im SafeGuard Policy Editor erstellte Konfigurationspakete. Für den erfolgreichen Betrieb von Sophos SafeGuard auf den Endpoint-Computern müssen Sie ein Konfigurationspaket mit den relevanten Richtliniengruppen erstellen und das Paket an die Endpoint-Computer verteilen.

Während der Erstkonfiguration im SafeGuard Policy Editor Konfigurationsassistenten kann bereits ein Standard-Konfigurationspaket mit Standardrichtlinien erstellt werden.

Wenn Sie Richtlinieneinstellungen ändern, müssen Sie jeweils neue Konfigurationspakete erstellen und an die Endpoint-Computer verteilen.

Die folgenden Abschnitte beschreiben die Erstellung von Konfigurationspaketen sowie die Verteilung an die Endpoint-Computer.

**Hinweis:** Überprüfen Sie Ihr Netzwerk und Ihre Computer in regelmäßigen Abständen auf veraltete oder nicht benutzte Konfigurationspakete und löschen Sie diese aus Sicherheitsgründen.

### 10.1 Sophos SafeGuard Konfigurationspaket erstellen

**Hinweis:** Richtlinien werden in einem Konfigurationspaket an die Endpoint-Computer übertragen. Wenn Sie eine neue Richtlinie erstellt oder eine bestehende Richtlinie bearbeitet haben, führen Sie die folgenden Schritte durch. Wenn Sie nur die Standardrichtlinien verwenden, wird während der Erstkonfiguration automatisch ein Konfigurationspaket erstellt. In diesem Fall müssen Sie die folgenden Schritte nicht ausführen.

So erstellen Sie ein Konfigurationspaket:

1. Wählen Sie im SafeGuard Policy Editor aus dem Menü **Extras** den Befehl **Konfigurationspakete**.
2. Klicken Sie auf **Konfigurationspaket hinzufügen**.
3. Geben Sie einen beliebigen Namen für das Konfigurationspaket ein.
4. Geben Sie eine zuvor im SafeGuard Policy Editor erstellte **Richtliniengruppe**, die für die Computer gelten soll, an.
5. Geben Sie unter **Speicherort für Schlüssel-Sicherungskopie** einen freigegebenen Netzwerkpfad für das Speichern der Schlüssel-Recovery-Datei an. Geben Sie den freigegebenen Pfad in folgender Form ein: \\networkcomputer\, z. B. "\\mycompany.edu\". Wenn Sie hier keinen Pfad angeben, wird der Benutzer beim ersten Anmelden am Endpoint-Computer nach der Installation gefragt, wo die Schlüsseldatei gespeichert werden soll.

Die Schlüssel-Recovery-Datei wird für die Durchführung von Recovery-Vorgängen bei durch Sophos SafeGuard geschützten Computern benötigt. Sie wird auf allen durch Sophos SafeGuard geschützten Computern generiert.

Stellen Sie sicher, dass diese Schlüssel-Recovery-Datei an einem Speicherort abgelegt wird, auf den die Mitarbeiter des Helpdesk Zugriff haben, z. B. auf einem freigegebenen Netzwerkpfad. Die Dateien können dem Helpdesk auch über andere Mechanismen zur Verfügung gestellt werden. Die Datei ist mit dem Unternehmenszertifikat verschlüsselt. Sie kann also auch auf externen Medien oder auf dem Netzwerk gespeichert werden, um sie dem Helpdesk für Recovery-Vorgänge zur Verfügung zu stellen. Sie kann auch per E-Mail verschickt werden.

6. Unter **POA-Gruppe** können Sie eine POA Access Account Gruppe auswählen, die dem Endpoint-Computer zugeordnet werden soll. POA Access Accounts bieten Zugang für administrative Aufgaben auf dem Endpoint-Computer, nachdem die Power-on Authentication aktiviert wurde. Um POA Access Accounts zuordnen zu können, muss die POA-Gruppe zuvor im Bereich **Benutzer** des SafeGuard Policy Editor angelegt werden.
7. Legen Sie den Ausgabepfad für das Konfigurationspaket (MSI) fest.
8. Klicken Sie auf **Konfigurationspaket erstellen**.

Das Konfigurationspaket (MSI) wird im angegebenen Verzeichnis angelegt. Im nächsten Schritt verteilen Sie das Paket an die Sophos SafeGuard Endpoint-Computern zur Installation.

## 10.2 Konfigurationspakete verteilen

Konfigurationspakete müssen nach der Installation der Sophos SafeGuard Verschlüsselungssoftware sowie nach jeder Änderung in den Konfigurationseinstellungen auf den Endpoint-Computern installiert werden.

Verteilen Sie die Konfigurationspakete über Ihre unternehmenseigenen Software-Verteilungsmechanismen, oder installieren Sie die Pakete manuell auf den Endpoint-Computern.

**Hinweis:** Um die Richtlinieneinstellungen für einen durch Sophos SafeGuard geschützten Computer zu ändern, erstellen Sie ein neues Konfigurationspaket mit den geänderten Richtlinien und übertragen Sie es an den Computer.

**Hinweis:** Wenn Sie versuchen, ein älteres Konfigurationspaket über ein neues zu installieren, wird die Installation mit einer Fehlermeldung abgebrochen.

## 11 Unternehmenszertifikat und Master Security Officer Zertifikat exportieren

In einer Sophos SafeGuard Installation sind die beiden folgenden Elemente von entscheidender Bedeutung und erfordern daher die Erstellung von Sicherungskopien an einem sicheren Speicherort:

- das in der SafeGuard-Datenbank gespeicherte Unternehmenszertifikat
- das Zertifikat des Haupt-Sicherheitsbeauftragten (MSO) im Zertifikatsspeicher des Computers, auf dem der SafeGuard Policy Editor installiert ist.

**Hinweis:** Im SafeGuard Policy Editor ist der MSO der Sicherheitsbeauftragte, der während der Erstkonfiguration definiert wird. Im Produkt-Bundle mit ESDP hat dieser Sicherheitsbeauftragte immer den Namen "Administrator".

Beide Zertifikate lassen sich als .p12 Dateien zur Erstellung von Sicherungskopien exportieren. Beschädigte Installationen des SafeGuard Policy Editor oder eine beschädigte Datenbank lassen sich damit durch den Import des entsprechenden Zertifikats (.p12-Datei) wiederherstellen.

**Hinweis:** Wir empfehlen, diesen Vorgang direkt nach der Erstkonfiguration im SafeGuard Policy Editor auszuführen.

### 11.1 Unternehmenszertifikate exportieren

1. Wählen Sie **Extras > Optionen** in der SafeGuard Policy Editor Menüleiste.
2. Wechseln Sie in die Registerkarte **Zertifikate** und klicken Sie im Bereich **Unternehmenszertifikat** auf **Exportieren**.
3. Sie werden aufgefordert, ein Kennwort für die Sicherung der exportierten Datei einzugeben. Geben Sie ein Kennwort ein, bestätigen Sie es und klicken Sie auf **OK**.
4. Geben Sie einen Dateinamen und einen Speicherort für die zu exportierende Datei ein und klicken Sie auf **OK**.

Das Unternehmenszertifikat wird als P12-Datei an den definierten Speicherort exportiert und kann für Recovery-Vorgänge benutzt werden.

## 11.2 Zertifikat des Haupt-Sicherheitsbeauftragten exportieren

So exportieren Sie das Zertifikat des Haupt-Sicherheitsbeauftragten (MSO), der am SafeGuard Policy Editor angemeldet ist.

1. Wählen Sie **Extras > Optionen** in der SafeGuard Policy Editor Menüleiste.
2. Wechseln Sie in die Registerkarte **Zertifikate** und klicken Sie im Bereich **<Administrator> Zertifikat** auf **Exportieren**.
3. Sie werden dazu aufgefordert, ein Kennwort für die Sicherung der exportierten Datei einzugeben. Geben Sie ein Kennwort ein, bestätigen Sie es und klicken Sie auf **OK**.
4. Geben Sie einen Dateinamen und einen Speicherort für die zu exportierende Datei ein und klicken Sie auf **OK**.

Das Zertifikat des derzeit angemeldeten Hauptsicherheitsbeauftragten wird als P12-Datei an den definierten Speicherort exportiert und kann für Recovery-Vorgänge benutzt werden.

## 12 Korrupte SafeGuard Policy Editor Installation wiederherstellen

Eine korrupte SafeGuard Policy Editor Installation kann auf einfache Art und Weise wiederhergestellt werden, wenn die Datenbank noch intakt ist. In diesem Fall müssen Sie nur den SafeGuard Policy Editor neu installieren und die vorhandene Datenbank sowie das gesicherte Sicherheitsbeauftragten-Zertifikat verwenden.

Gehen Sie wie folgt vor:

1. Installieren Sie das Policy Editor Installationspaket neu. Öffnen Sie den SafeGuard Policy Editor. Der Konfigurationsassistent wird automatisch geöffnet.
2. Aktivieren Sie unter **Datenbank-Verbindung**, die Option **Vorhandene Datenbank verwenden**. Wählen Sie unter **Datenbankname** den Namen der Datenbank aus der Liste aus. Falls erforderlich, konfigurieren Sie unter **Datenbankeinstellungen** die Verbindung zur Datenbank. Klicken Sie auf **Weiter**.
3. Führen Sie unter **Sicherheitsbeauftragter** einen der beiden folgenden Schritte aus:
  - Wenn die gesicherte Zertifikatdatei auf dem Computer gefunden wird, wird sie angezeigt. Geben Sie das Kennwort ein, das Sie zur Anmeldung an den Sophos SafeGuard Policy Editor benutzen.
  - Wird die gesicherte Zertifikatdatei nicht auf dem Computer gefunden, klicken Sie auf **Importieren**. Suchen Sie nach der gesicherten Zertifikatdatei und bestätigen Sie Ihre Auswahl mit **Öffnen**. Geben Sie das Kennwort für die ausgewählte Zertifikatdatei ein. Bestätigen Sie das Kennwort mit **Ja**. Geben Sie ein Kennwort für die Anmeldung am SafeGuard Policy Editor ein und bestätigen Sie es.
4. Klicken Sie auf **Weiter** und dann auf **Fertig stellen**, um die Konfiguration des SafeGuard Policy Editor abzuschließen.

Die beschädigte SafeGuard Policy Editor Installation ist wiederhergestellt.

## 13 Korrupte Datenbankkonfiguration wiederherstellen

Sie können eine korrupte Datenbankkonfiguration wiederherstellen, indem Sie den SafeGuard Policy Editor neu installieren und basierend auf den gesicherten Zertifikatsdateien eine neue Instanz der Datenbank erstellen. Dadurch wird sichergestellt, dass alle vorhandenen Sophos SafeGuard Endpoint-Computer Richtlinien von der neuen Installation annehmen. Somit müssen Sie nicht die gesamte Datenbank neu einrichten und wiederherstellen.

- Das Unternehmenszertifikat und das Haupt-Sicherheitsbeauftragten-Zertifikat der betreffenden Datenbankkonfiguration müssen als .p12 Dateien exportiert worden sein. Die Dateien müssen vorhanden und gültig sein.
- Die Kennwörter für die beiden .p12 Dateien sowie für den Zertifikatsspeicher müssen Ihnen bekannt sein.

Gehen Sie wie folgt vor:

1. Installieren Sie das Policy Editor Installationspaket neu. Öffnen Sie den SafeGuard Policy Editor. Der Konfigurationsassistent wird automatisch geöffnet.
2. Wählen Sie unter **Datenbank-Verbindung** die Option **Neue Datenbank erstellen**. Konfigurieren Sie unter **Datenbankeinstellungen** die Verbindung zur Datenbank. Klicken Sie auf **Weiter**.
3. Wählen Sie unter **Sicherheitsbeauftragter** den relevanten Sicherheitsbeauftragten. Deaktivieren Sie die Option **Zertifikat automatisch erzeugen**. Klicken Sie auf **Importieren**, um nach der gesicherten Zertifikatsdatei zu suchen. Geben Sie das relevante Sicherheitsbeauftragten-Kennwort für den Zertifikatsspeicher ein. Das Zertifikat wird importiert. Klicken Sie auf **Weiter**.
4. Deaktivieren Sie unter **Unternehmensinformationen** die Option **Zertifikat automatisch erzeugen**. Klicken Sie auf **Importieren**, um nach der gesicherten Zertifikatsdatei zu suchen, die das gültige Unternehmenszertifikat enthält. Sie werden aufgefordert, das für den Zertifikatsspeicher definierte Kennwort einzugeben. Geben Sie das Kennwort ein und bestätigen Sie es mit **OK**. Bestätigen Sie die Meldung mit **Ja**. Das Unternehmenszertifikat wird importiert.
5. Geben Sie unter **Zertifikat-Sicherungskopie** einen Speicherort für die Zertifikat-Sicherungskopien an. Bestätigen Sie den Speicherort mit **Weiter**.

6. Deaktivieren Sie unter **Standardrichtlinie** die Option **Standardrichtlinie erzeugen** und bestätigen Sie mit **Weiter**.
7. Deaktivieren Sie unter **Recovery-Schlüssel** die Option **Einstellungen für die Netzwerkfreigabe**, klicken Sie auf **Weiter** und dann auf **Beenden**.

Die Datenbankkonfiguration ist wiederhergestellt.

## 14 Administrative Zugangsoptionen für Endpoint-Computer

Für den Fall, dass nach der Installation von Sophos SafeGuard der Zugang zur Durchführung von administrativen Vorgängen auf Endpoint-Computern erforderlich ist, bietet Sophos SafeGuard folgende administrative Zugangsoptionen:

### ■ Service Accounts für die Windows-Anmeldung

Mit Service Accounts können sich Benutzer (z. B. Rollout-Beauftragte, Mitglieder des IT-Teams) nach der Installation von Sophos SafeGuard an Endpoint-Computern anmelden (Windows-Anmeldung), ohne die Power-on Authentication zu aktivieren. Die Benutzer werden auch nicht als Sophos SafeGuard Benutzer zum Computer hinzugefügt. Service Account Listen werden im Bereich **Richtlinien** des SafeGuard Policy Editor angelegt und über in Sophos SafeGuard Konfigurationspaketen enthaltenen Richtlinien den Endpoint-Computern zugewiesen. Benutzer, die in eine Service Account Liste aufgenommen wurden, werden bei der Anmeldung am Endpoint-Computer als Gastbenutzer behandelt.

**Hinweis:** Service Account Listen werden den Endpoint-Computern über Richtlinien zugewiesen. Sie sollten bereits im ersten Sophos SafeGuard Konfigurationspaket, das Sie für die Konfiguration der Endpoint-Computer erstellen, enthalten sein. Sie können Service Account Listen aktualisieren, indem Sie ein neues Konfigurationspaket erstellen und an die Endpoint-Computer verteilen.

### ■ POA Access Accounts für die POA-Anmeldung

POA Access Accounts sind vordefinierte lokale Benutzerkonten, die es Benutzern (z. B. Mitgliedern des IT-Teams) ermöglichen, sich nach der Aktivierung der POA an Endpoint-Computern zur Ausführung administrativer Aufgaben anzumelden. POA Access Accounts ermöglichen die Anmeldung an der POA, eine automatische Anmeldung an Windows erfolgt nicht. Diese Benutzerkonten werden im Bereich **Benutzer** des Sophos SafeGuard Policy Editor definiert (Benutzer-ID und Kennwort) und werden den Endpoint-Computer über POA-Gruppen in Sophos SafeGuard Konfigurationspaketen zugewiesen.

## 14.1 Service Account Listen für die Windows-Anmeldung

Bei den meisten Implementationen von Sophos SafeGuard installiert zunächst ein Rollout-Team neue PCs in einer Umgebung. Danach folgt die Installation von Sophos SafeGuard. Zu Installations- und Prüfungszwecken meldet sich der Rollout-Beauftragte dann am jeweiligen Computer an, bevor der Endbenutzer diesen erhält und die Möglichkeit hat, die Power-on Authentication zu aktivieren.

So ergibt sich folgendes Szenario:

1. Sophos SafeGuard wird auf einem Endpoint-Computer installiert.
2. Nach dem Neustart des Computers meldet sich der Rollout-Beauftragte an.
3. Der Rollout-Beauftragte wird zur POA hinzugefügt und die POA wird aktiv.

Wenn der Endbenutzer den Computer erhält, kann er sich nicht an der POA anmelden und muss ein Challenge/Response-Verfahren durchführen.

Um zu verhindern, dass administrative Vorgänge auf einem durch Sophos SafeGuard geschützten Computer bewirken, dass die Power-on Authentication aktiviert wird und Rollout-Beauftragte als Benutzer zum Computer hinzugefügt werden, ermöglicht Sophos SafeGuard das Anlegen von Listen mit Service Accounts für Endpoint-Computer. Die in den Listen enthaltenen Benutzer werden dadurch als Sophos SafeGuard Gastbenutzer behandelt.

Mit Service Accounts ergibt sich folgendes Szenario:

1. Sophos SafeGuard wird auf einem Endpoint-Computer installiert.
2. Der Computer wird neu gestartet und ein Rollout-Beauftragter, der in einer Service Account Liste aufgeführt ist, meldet sich an (Windows-Anmeldung).
3. Gemäß der auf den Computer angewendeten Service Account Liste wird der Benutzer als Service Account erkannt und als Gastbenutzer behandelt.

Der Rollout-Beauftragte wird nicht zur POA hinzugefügt und die POA wird nicht aktiviert. Der Endbenutzer kann sich anmelden und die POA aktivieren.

**Hinweis:** Service Account Listen sollten bereits im ersten Sophos SafeGuard Konfigurationspaket, das Sie für die Konfiguration der Endpoint-Computer erstellen, enthalten sein. Sie können Service Account Listen aktualisieren, indem Sie ein neues Konfigurationspaket erstellen und an die Endpoint-Computer verteilen.

### 14.1.1 Service Account Listen anlegen und Benutzer hinzufügen

So legen Sie Service Account Listen an und fügen Benutzer hinzu:

1. Klicken Sie auf **Richtlinien** im Navigationsbereich.
2. Markieren Sie **Service Account Listen** Richtlinien-Navigationsfenster.
3. Klicken Sie im Kontextmenü von **Service Account Listen** auf **Neu > Service Account Liste**.
4. Geben Sie einen Namen für die Service Account Liste ein und klicken Sie auf **OK**.
5. Markieren Sie die neue Liste unter **Service Account Listen** im Richtlinien-Navigationsfenster.
6. Klicken Sie im Arbeitsbereich mit der rechten Maustaste. Das Kontextmenü für die Service Account Liste wird geöffnet. Wählen Sie **Hinzufügen**.
7. Eine neue Benutzerzeile wird hinzugefügt. Geben Sie den **Benutzernamen** und den **Domänennamen** in den entsprechenden Spalten ein und drücken Sie Enter. Um weitere Benutzer hinzuzufügen, wiederholen Sie diesen Schritt.
8. Speichern Sie Ihre Änderungen, indem Sie auf das **Speichern**-Symbol in der Symbolleiste klicken.

Die Service Account Liste ist registriert und kann beim Anlegen einer Richtlinie ausgewählt werden.

#### 14.1.1.1 Zusätzliche Informationen zur Eingabe von Benutzer- und Domänennamen

Für die Definition von Benutzern in Service Account Listen in den beiden Feldern **Benutzername** und **Domänenname** gibt es unterschiedliche Vorgehensweisen (siehe [Verschiedene Anmeldekombinationen abdecken](#), Seite 59). Darüber hinaus gelten für die Eingabewerte in diesen Feldern bestimmte Einschränkungen (siehe [Einschränkungen](#), Seite 61).

##### Verschiedene Anmeldekombinationen abdecken

Durch die beiden separaten Felder **Benutzername** und **Domänenname** pro Listeneintrag bieten die Service Account Listen die zum Abdecken aller möglichen Anmeldekombinationen (z. B. „Benutzer@Domäne oder „Domäne\Benutzer“) erforderliche Flexibilität.

Um mehrere Kombinationen aus Benutzername und Domänenname anzugeben, können Sie Asterisken (\*) als Platzhalter verwenden. Ein \* ist als erstes Zeichen, als letztes Zeichen und als einziges Zeichen zulässig.

Zum Beispiel:

- **Benutzername:** Administrator
- **Domänenname:** \*

Mit dieser Kombination geben Sie alle Benutzer mit dem Benutzernamen „Administrator“ an, die sich an einem Netzwerk oder an einer beliebigen lokalen Maschine anmelden.

Der vordefinierte Domänenname [LOCALHOST], der in der Dropdownliste des Felds **Domänenname** zur Verfügung steht, steht für die Anmeldung an einer beliebigen lokalen Maschine.

Zum Beispiel:

- **Benutzername:** "Admin\*"
- **Domänname:** [LOCALHOST]

Mit dieser Kombination geben Sie alle Benutzer an, deren Benutzernamen mit Admin beginnen und die sich an einer beliebigen lokalen Maschine anmelden.

Darüber hinaus können sich Benutzer auf verschiedene Art und Weise anmelden, z. B.:

- Benutzer: test, Domäne: mycompany
- Benutzer: test, Domäne: mycompany.com.

Da Domänenangaben in Service Account Listen nicht automatisch aufgelöst werden, gibt es drei mögliche Methoden für das korrekte Angeben der Domäne:

- Sie wissen genau, wie der Benutzer sich anmelden wird, und geben die Domäne entsprechend exakt ein.
- Sie erstellen mehrere Einträge in der Service Account Liste.
- Sie verwenden Platzhalter, um alle unterschiedlichen Fälle abzudecken (Benutzer: test, Domäne: mycompany\*).

**Hinweis:** Windows verwendet möglicherweise nicht dieselbe Zeichenfolge und kürzt Namen ab. Um dadurch entstehende Probleme zu vermeiden, empfehlen wir, den FullQualifiedName und den Netbios-Namen einzugeben oder Platzhalter zu verwenden.

## Einschränkungen

Asterisken sind nur als erstes, letztes und einziges Zeichen zulässig. Beispiele für gültige und ungültige Zeichenfolgen:

- Gültige Zeichenfolgen sind z. B.: admin\*, \*, \*strator, \*minis\*.
- Ungültige Zeichenfolgen sind z. B.: \*\*, Admin\*trator, Ad\*minst\*.

Darüber hinaus gelten folgende Einschränkungen:

- Das Zeichen ? ist in Benutzernamen nicht zulässig.
- Die Zeichen / \ [ ] : ; | = , + \* ? < > " sind in Domännennamen nicht zulässig.

### 14.1.2 Service Account Listen bearbeiten und löschen

Als Sicherheitsbeauftragter mit der Berechtigung **Service Account Listen ändern** können Sie Service Account Listen jederzeit bearbeiten oder löschen:

- Um eine Service Account Liste zu bearbeiten, doppelklicken Sie auf der Liste im Richtlinien-Navigationsfenster. Die Service Account Liste wird geöffnet und Sie können Benutzernamen hinzufügen, löschen oder ändern.
- Um eine Service Account Liste zu löschen, wählen Sie die Liste im Richtlinien-Navigationsfenster aus, öffnen Sie das Kontextmenü und wählen Sie **Löschen**.

### 14.1.3 Service Account Liste über Richtlinie zuweisen

So weisen Sie eine Service Account Liste zu:

1. Legen Sie eine Richtlinie vom Typ **Authentisierung** an oder wählen Sie eine bereits vorhandene aus.
2. Wählen Sie unter **Anmeldeoptionen** die gewünschte Service Account Liste aus der Dropdownliste des Felds **Service Account Liste**.

**Hinweis:** Die Standardeinstellung dieses Felds ist [**Keine Liste**], d. h. es gilt keine Service Account Liste. Rollout-Beauftragte, die sich nach der Installation von Sophos SafeGuard an dem Computer anmelden, werden somit nicht als Gastbenutzer behandelt und können die Power-on Authentication aktivieren sowie zum Computer hinzugefügt werden.

Um die Zuweisung einer Service Account Liste rückgängig zu machen, wählen Sie die Option **[Keine Liste]**.

3. Speichern Sie Ihre Änderungen, indem Sie auf das Speichern-Symbol in der Symbolleiste klicken.

Sie können die Richtlinie nun an den Benutzercomputer übertragen, um die Service Accounts auf dem Computer zur Verfügung zu stellen.

**Hinweis:** Wenn Sie unterschiedliche Service Account Listen in verschiedenen Richtlinien auswählen, die alle nach dem RSOP (Resulting Set of Policies, die für einen bestimmten Computer/eine bestimmte Gruppe geltenden Einstellungen) relevant sind, setzt die Service Account Liste in der zuletzt angewandten Richtlinie alle zuvor zugewiesenen Service Account Listen außer Kraft. Service Account Listen werden nicht zusammengeführt.

#### **14.1.4 Richtlinie an den Endpoint-Computer übertragen**

Durch Sophos SafeGuard geschützte Computer erhalten Richtlinien über Konfigurationspakete, die im SafeGuard Policy Editor über **Extras > Konfigurationspakete** erstellt werden.

Die Konfigurationsdatei kann über unternehmenseigene Software-Verteilungsmechanismen verteilt werden. Das Konfigurationspaket kann jedoch auch manuell auf den Endpoint-Computern installiert werden.

**Hinweis:** Da Service Account Listen besonders während der initialen Installation in der Rollout-Phase einer Implementation nützlich sind, empfehlen wir, eine Richtlinie vom Typ **Authentisierung** mit den erforderlichen Einstellungen bereits in die Richtliniengruppe aufzunehmen, die Sie mit dem ersten Sophos SafeGuard Konfigurationspaket nach der Installation an die Endpoint-Computer zu übertragen.

**Hinweis:** Um die Richtlinieneinstellungen für einen durch Sophos SafeGuard geschützten Computer zu ändern, erstellen Sie ein neues Konfigurationspaket mit den geänderten Richtlinien und verteilen Sie dieses an den Computer.

### **14.1.5 Auf einem Endpoint-Computer mit einem Service Account anmelden**

Bei der ersten Windows-Anmeldung nach dem Neustart des Computers meldet sich ein Benutzer, der auf einer Service Account Liste aufgeführt ist, am Computer als Sophos SafeGuard Gastbenutzer an. Diese erste Windows-Anmeldung an dieser Maschine löst weder eine ausstehende Aktivierung der Power-on Authentication aus, noch wird durch die Anmeldung der Benutzer zum Computer hinzugefügt. Das Sophos SafeGuard System Tray Icon zeigt in diesem Fall auch nicht den Balloon Tooltip „Initialer Benutzerabgleich abgeschlossen“ an.

#### **14.1.5.1 Anzeige des Service Account Status auf dem Endpoint-Computer**

Der Gastbenutzer-Anmeldestatus wird auch über das System Tray Icon angezeigt. Weitere Informationen zum System Tray Icon finden Sie in der Sophos SafeGuard Benutzerhilfe, Kapitel *System Tray Icon und Balloon-Ausgabe* (Beschreibung des Benutzerstatus-Felds).

### **14.1.6 Protokollierte Ereignisse**

Die in Zusammenhang mit Service Account Listen durchgeführten Aktionen werden über die folgenden Ereignisse protokolliert:

#### **SafeGuard Policy Editor**

- Service Account Liste <Name> angelegt.
- Service Account Liste <Name> geändert.
- Service Account Liste <Name> gelöscht.

#### **Sophos SafeGuard Endpoint-Computer**

- Windows-Benutzer <Domäne/Benutzer> hat sich um <Zeit> an Maschine <Domäne/Computer> als SGN Service Account angemeldet.
- Neue Service Account Liste importiert.
- Service Account Liste <Name> gelöscht.

## 14.2 POA Access Accounts für die POA-Anmeldung

Nach der Installation von Sophos SafeGuard und der Aktivierung der Power-on Authentication (POA), kann der Zugang zu Endpoint-Computern für administrative Aufgaben notwendig sein. Mit POA Access Accounts können sich Benutzer (z. B. Mitglieder des IT-Teams) zur Durchführung von administrativen Aufgaben an der Power-on Authentication anmelden, ohne ein Challenge/Response-Verfahren durchführen zu müssen. Eine automatische Anmeldung an Windows erfolgt nicht. Die Benutzer müssen sich an Windows mit ihren vorhandenen Windows-Benutzerkonten anmelden.

Sie können POA Access Accounts im SafeGuard Policy Editor anlegen, diese in POA Access Account-Gruppen gruppieren und die Gruppen über Konfigurationspakete den Endpoint-Computern zuweisen. Die Benutzer, d. h. die POA Access Accounts, die in der zugewiesenen POA Access Account-Gruppe enthalten sind, werden zur POA hinzugefügt und können sich mit Ihrem vordefinierten Benutzernamen und Kennwort an der POA anmelden.

### 14.2.1 POA Access Accounts erstellen

So erstellen Sie POA Access Accounts:

1. Klicken Sie im Navigationsbereich des SafeGuard Policy Editor auf **Benutzer**.
2. Wählen Sie im **Benutzer** Navigationsfenster unter **POA** den Knoten **POA-Benutzer**.
3. Klicken Sie im **POA-Benutzer** Kontextmenü auf **Neu > Neuen Benutzer erstellen**.

Der Dialog **Neuen Benutzer erstellen** wird angezeigt.

4. Geben Sie im Feld **Vollständiger Name** einen Namen, d. h. den Anmeldenamen für den neuen POA-Benutzer ein.

5. Optional können Sie eine Beschreibung für den neuen POA-Benutzer eingeben.

6. Geben Sie ein Kennwort für das neue POA Access Account ein und bestätigen Sie es.

Aus Sicherheitsgründen sollte das Kennwort bestimmten Mindest-Komplexitätsanforderungen entsprechen. Zum Beispiel sollte es eine Mindestlänge von 8 Zeichen haben und sowohl aus numerischen als auch alphanumerischen Zeichen bestehen. Ist das hier eingegebene Kennwort zu kurz, so wird eine entsprechende Warnungsmeldung angezeigt.

7. Klicken Sie auf **OK**.

Das neue POA Access Account wird angelegt und der POA-Benutzer (d. h. das POA Access Account) wird unter **POA-Benutzer** im **Benutzer** Navigationsbereich angezeigt.

## 14.2.2 Kennwort für ein POA Access Account ändern

So ändern Sie das Kennwort für ein POA Access Account:

1. Klicken Sie auf **Benutzer** im Navigationsbereich des SafeGuard Policy Editor.
2. Wählen Sie im **Benutzer** Navigationsfenster unter **POA, POA-Benutzer** den relevanten POA-Benutzer.
3. Wählen Sie im Kontextmenü des POA-Benutzers den Befehl **Eigenschaften**.

Der Eigenschaftendialog für den POA-Benutzer wird angezeigt.

4. Geben Sie in der Registerkarte **Allgemein** unter **Benutzerkennwort** das neue Kennwort ein und bestätigen Sie es.
5. Klicken Sie auf **OK**.

Für das relevante POA Access Account gilt das neue Kennwort.

## 14.2.3 POA Access Accounts löschen

So löschen Sie POA Access Accounts:

1. Klicken Sie im Navigationsbereich des SafeGuard Policy Editor auf **Benutzer**.
2. Wählen Sie im **Benutzer** Navigationsfenster unter **POA, POA-Benutzer** das relevante POA Access Account.
3. Klicken Sie mit der rechten Maustaste auf das POA Access Account und wählen Sie **Löschen** aus dem Kontextmenü.

Das POA Access Account, d. h. der POA-Benutzer, wird gelöscht und nicht mehr im **Benutzer** Navigationsfenster angezeigt.

**Hinweis:** Wenn der Benutzer einer oder mehreren POA-Gruppen angehört, wird er auch aus allen Gruppen entfernt. Das POA Access Account steht jedoch noch so lange auf dem Endpoint-Computer zur Verfügung, bis ein neues Konfigurationspaket erstellt und zugewiesen wird. Für weitere Details zu POA-Gruppen, siehe [POA Access Account Gruppen erstellen](#), Seite 66. Für weitere Details zum Ändern der POA Access Account Zuweisung, siehe [POA Access Account Zuweisungen auf Endpoint-Computern ändern](#), Seite 68

#### 14.2.4 POA Access Account Gruppen erstellen

Damit die POA Access Accounts Endpoint-Computern über Konfigurationspakete zugewiesen werden können, müssen sie in Gruppen zusammengefasst werden. Beim Erstellen von Konfigurationspaketen können Sie dann eine POA Access Account Gruppe für die Zuweisung auswählen.

So erstellen Sie POA Access Account Gruppen:

1. Klicken Sie im Navigationsbereich des SafeGuard Policy Editor auf **Benutzer**.
2. Wählen Sie im **Benutzer** Navigationsbereich unter **POA** den Knoten **POA-Gruppen**.
3. Klicken Sie im **POA-Gruppen** Kontextmenü auf **Neu > Neue Gruppe erstellen**.

Der **Neue Gruppe erstellen** Dialog wird angezeigt.

4. Geben Sie im Feld **Vollständiger Name** einen Namen für die neue POA-Gruppe ein.
5. Optional können Sie eine Beschreibung für die neue POA-Gruppe eingeben.
6. Klicken Sie auf **OK**.

Die neue POA Access Account Gruppe wird angelegt und unter **POA-Gruppen** im **Benutzer** Navigationsbereich angezeigt. Sie können nun Benutzer, d. h. POA Access Accounts, zur Gruppe hinzufügen.

#### 14.2.5 POA Access Accounts zu Gruppen hinzufügen

So fügen Sie Benutzer, d. h. POA Access Accounts, zu POA Access Account Gruppen hinzu:

1. Klicken Sie im Navigationsbereich des SafeGuard Policy Editor auf **Benutzer**.
2. Wählen Sie im **Benutzer** Navigationsfenster unter **POA**, **POA-Gruppe** die relevante POA-Gruppe.

Im Aktionsbereich des SafeGuard Policy Editor auf der rechten Seite wird die **Mitglieder** Registerkarte angezeigt.

3. Klicken Sie in der SafeGuard Policy Editor Symbolleiste auf das **Hinzufügen** Symbol (grünes Pluszeichen).

Der Dialog **Mitgliedobjekt auswählen** wird angezeigt.

4. Wählen Sie den Benutzer (d. h. das POA Access Account) den Sie zur Gruppe hinzufügen möchten.
5. Klicken Sie auf **OK**.

Das POA Access Account wird zur Gruppe hinzugefügt und in der Registerkarte **Mitglieder** angezeigt.

**Hinweis:** Sie können POA Access Accounts auch zu einer Gruppe hinzufügen, indem Sie den POA-Benutzer im Navigationsfenster auswählen und die beschriebenen Schritte ausführen. Der einzige Unterschied bei dieser Vorgehensweise besteht darin, dass nach Auswahl des Benutzers die **Mitglied von** Registerkarte im Aktionsbereich angezeigt wird. Diese Registerkarte zeigt die Gruppen, denen der Benutzer zugewiesen wurde. Der grundlegende Workflow ist identisch.

#### **14.2.5.1 Mitglieder aus POA Access Account Gruppen entfernen**

So entfernen Sie Mitglieder, d. h. POA Access Account, aus Gruppen:

1. Klicken Sie im Navigationsbereich des SafeGuard Policy Editor auf **Benutzer**.
2. Wählen Sie im **Benutzer** Navigationsfenster unter **POA, POA-Gruppe** die relevante POA-Gruppe.

Im Aktionsbereich des SafeGuard Policy Editor auf der rechten Seite wird die **Mitglieder** Registerkarte angezeigt.

3. Wählen Sie den Benutzer, den Sie aus der Gruppe entfernen möchten.
4. Klicken Sie in der SafeGuard Policy Editor Symbolleiste auf das **Löschen** Symbol (rotes Kreuzzeichen).

Der Benutzer wird aus der Gruppe entfernt.

**Hinweis:** Sie können POA Access Accounts aus einer Gruppe entfernen, indem Sie den POA-Benutzer im Navigationsfenster auswählen und die beschriebenen Schritte ausführen. Der einzige Unterschied bei dieser Vorgehensweise besteht darin, dass nach Auswahl des Benutzers die **Mitglied von** Registerkarte im Aktionsbereich angezeigt wird. Diese Registerkarte zeigt die Gruppen, denen der Benutzer zugewiesen wurde. Der grundlegende Workflow ist identisch.

## 14.2.6 POA Access Accounts zu Endpoint-Computern zuweisen

So weisen Sie POA Access Accounts Endpoint-Computern über Konfigurationspakete zu:

1. Wählen Sie im SafeGuard Policy Editor aus dem Menü **Extras** den Befehl **Konfigurationspakete**.
2. Wählen Sie ein vorhandenes Konfigurationspaket aus oder erstellen Sie ein neues.  
Für Details zum Erstellen eines neuen Konfigurationspakets, siehe [Sophos SafeGuard Konfigurationspaket erstellen](#), Seite 50.
3. Wählen Sie eine **POA-Gruppe**, die Sie zuvor im Bereich **Benutzer** des SafeGuard Policy Editor erstellt haben, aus.

Die Standardeinstellung für die POA-Gruppe ist **Keine Gruppe**.

Darüber hinaus steht standardmäßig eine leere Gruppe zur Auswahl zur Verfügung. Diese Gruppe kann dazu verwendet werden, die Zuweisung einer POA Access Account Gruppe auf Endpoint-Computern zu löschen. Für weitere Details, siehe [POA Access Accounts auf Endpoint-Computern löschen](#), Seite 69.

4. Geben Sie einen Ausgabepfad für das Konfigurationspaket (MSI) an.
5. Klicken Sie auf **Konfigurationspaket erstellen**.
6. Verteilen Sie das Konfigurationspaket (MSI) an die Endpoint-Computer.

Durch Installation des Konfigurationspakets werden die Benutzer, d. h. die POA Access Accounts, aus der Gruppe zur POA auf den Endpoint-Computern hinzugefügt. Die POA Access Accounts stehen für die POA-Anmeldung zur Verfügung.

## 14.2.7 POA Access Account Zuweisungen auf Endpoint-Computern ändern

So ändern Sie die Zuweisung von POA Access Accounts auf Endpoint-Computern:

1. Legen Sie eine neue POA Access Account-Gruppe an oder ändern Sie eine bestehende Gruppe.
2. Erstellen Sie ein neues Konfigurationspaket und wählen Sie die neue oder modifizierte POA Access Account Gruppe aus.

Die neue POA Access Account Gruppe steht auf dem Endpoint-Computer zur Verfügung. Alle enthaltenen Benutzer werden zur POA hinzugefügt. Die neue Gruppe überschreibt die alte. POA Access Account Gruppen werden nicht miteinander kombiniert.

### 14.2.8 POA Access Accounts auf Endpoint-Computern löschen

Sie können POA Access Accounts auf Endpoint-Computern löschen, indem Sie den Computern eine leere POA Access Account Gruppe zuweisen:

1. Wählen Sie im Menü **Extras** des SafeGuard Policy Editor den Befehl **Konfigurationspakete**.
2. Wählen Sie ein vorhandenes Konfigurationspaket aus oder erstellen Sie ein neues.  
Für Details zum Erstellen eines neuen Konfigurationspakets, siehe [Sophos SafeGuard Konfigurationspaket erstellen](#), Seite 50.
3. Wählen Sie eine leere **POA-Gruppe**, die sie zuvor im Bereich **Benutzer** des SafeGuard Policy Editor angelegt haben, oder die leere POA-Gruppe, die standardmäßig unter **Konfigurationspakete** zur Verfügung steht.
4. Geben Sie einen Ausgabepfad für das Konfigurationspaket (MSI) an.
5. Klicken Sie auf **Konfigurationspaket erstellen**.
6. Verteilen Sie das Konfigurationspaket an die Endpoint-Computer.

Durch Installation des Konfigurationspakets werden alle POA Access Accounts von den Endpoint-Computern entfernt. Somit werden alle relevanten Benutzer aus der POA entfernt.

### 14.2.9 Mit POA Access Account am Endpoint-Computer anmelden

So melden Sie sich mit einem POA Access Account an:

1. Schalten Sie den Computer ein.

Der Power-on Authentication Anmeldedialog wird angezeigt.

2. Geben Sie den **Benutzernamen** und das **Kennwort** des vordefinierten POA Access Account ein.

Sie werden nicht automatisch an Windows angemeldet. Der Windows-Anmeldedialog wird angezeigt.

3. Wählen Sie im **Domäne** Feld die Domäne **<POA>**.
4. Melden Sie sich mit Ihrem vorhandenen Windows-Benutzerkonto an Windows an.

## 15 Standardrichtlinien

Während der Erstkonfiguration im SafeGuard Policy Editor wird standardmäßig eine Richtliniengruppe mit vordefinierten Einstellungen für die Verschlüsselung und die Authentisierung erzeugt. Darüber hinaus wird automatisch ein Konfigurationspaket (MSI) erzeugt, das diese Standardrichtlinien enthält.

Nach der Installation werden die Richtlinien und die Richtliniengruppe im **Richtlinien** Navigationsbereich des SafeGuard Policy Editor angezeigt. Das automatisch erstellte Konfigurationspaket wird zur Auswahl unter **Konfigurationspakete** im SafeGuard Policy Editor angezeigt.

**Hinweis:** Die Standardrichtlinien lassen sich nur während der Erstkonfiguration im SafeGuard Policy Editor Konfigurationsassistenten erstellen.

In den folgenden beiden Abschnitten finden Sie jeweils eine Auflistung der mit SGE (SafeGuard Easy) und ESDP (Endpoint Security and Data Protection) verfügbaren Standardrichtlinien.

Für eine detaillierte Beschreibung aller Richtlinieneinstellungen, siehe [Richtlinieneinstellungen](#), Seite 80.

## 15.1 Mit SGE verfügbare Standardrichtlinien

Für Optionen, bei denen in der folgenden Tabelle die Einstellung nicht konfiguriert angegeben ist, gelten automatisch Standardwerte. Die relevanten Standardwerte sind in Klammern angegeben.

**Hinweis:** Für eine detaillierte Beschreibung aller Richtlinieneinstellungen, siehe [Richtlinieneinstellungen](#), Seite 80.

Richtlinie	Einstellungen
<p><b>Standardrichtlinie für allgemeine Einstellungen</b>                      Richtlinientyp: <b>Allgemeine Einstellungen</b></p>	<p><b>Anpassung:</b></p> <ul style="list-style-type: none"> <li>■ <b>Sprache am Client: Spracheinstellungen des Betriebssystems verwenden</b></li> </ul> <p><b>Recovery für die Anmeldung:</b></p> <ul style="list-style-type: none"> <li>■ <b>Recovery für die Anmeldung nach Beschädigung des Windows Local Cache aktivieren: Nein</b></li> </ul> <p><b>Local Self Help:</b></p> <ul style="list-style-type: none"> <li>■ <b>Local Self Help aktivieren: Ja</b></li> <li>■ <b>Minimale Länge der Antwort: 3</b></li> <li>■ <b>Benutzer dürfen eigene Fragen festlegen: Ja</b></li> </ul> <p><b>Challenge/Response (C/R):</b></p> <ul style="list-style-type: none"> <li>■ <b>Recovery für die Anmeldung über C/R aktivieren: Ja</b></li> <li>■ <b>Automatische Anmeldung an Windows erlauben: Ja</b></li> </ul>

Richtlinie	Einstellungen
<p><b>Standardrichtlinie für die Authentisierung</b>                      Richtlinientyp: Authentisierung</p>	<p><b>Zugriff:</b></p> <ul style="list-style-type: none"> <li>■ <b>Benutzer kann nur von der Festplatte booten: Ja</b></li> </ul> <p><b>Anmeldeoptionen:</b></p> <ul style="list-style-type: none"> <li>■ <b>Anmeldemodus: Benutzer-ID/Kennwort</b></li> <li>■ <b>Erfolgreiche Anmeldeversuche dieses Benutzers anzeigen: Nein</b></li> <li>■ <b>Letzte Benutzeranmeldung anzeigen: Nein</b></li> <li>■ <b>'Erzwungene Abmeldung' bei Sperre der Arbeitsstation deaktivieren: Nein</b></li> <li>■ <b>Letzte Benutzer/Domänen-Auswahl aktivieren: Ja</b></li> <li>■ <b>Durchgehende Anmeldung an Windows: Benutzer wählen lassen</b></li> </ul> <p><b>Erfolgreiche Anmeldungen:</b></p> <ul style="list-style-type: none"> <li>■ <b>Maximalanzahl von erfolgreichen Anmeldeversuchen: 16</b></li> <li>■ <b>Meldungen zur fehlgeschlagenen Anmeldung in der POA anzeigen: Standard</b></li> </ul> <p><b>Reaktion auf erfolgreiche Anmeldeversuche:</b></p> <ul style="list-style-type: none"> <li>■ <b>Computer sperren: Ja</b></li> </ul>

Richtlinie	Einstellungen
<p><b>Standardrichtlinie für Kennwörter</b>                      Richtlinientyp: <b>Kennwort</b></p>	<p><b>Kennwort:</b></p> <ul style="list-style-type: none"> <li>■ <b>Mindestlänge des Kennworts: 4</b></li> <li>■ <b>Maximallänge des Kennworts: 128</b></li> <li>■ <b>Mindestanzahl an Buchstaben: 0</b></li> <li>■ <b>Mindestanzahl an Ziffern: 0</b></li> <li>■ <b>Mindestanzahl an Symbolen: 0</b></li> <li>■ <b>Groß-/Kleinschreibung beachten: Nein</b></li> <li>■ <b>Tastaturzeile verboten: Nein</b></li> <li>■ <b>Tastaturspalte verboten: Nein</b></li> <li>■ <b>Drei oder mehr aufeinanderfolgende Zeichen verboten: Nein</b></li> <li>■ <b>Benutzername als Kennwort verboten: Nein</b></li> <li>■ <b>Liste nicht erlaubter Kennwörter verwenden: Nein</b></li> </ul> <p><b>Änderungen:</b></p> <ul style="list-style-type: none"> <li>■ <b>Kennwortänderung erlaubt nach mindestens (Tage): nicht konfiguriert (Standardwert 0 gilt)</b></li> <li>■ <b>Kennwort läuft ab nach (Tage): nicht konfiguriert (Standardwert 999 gilt)</b></li> <li>■ <b>Warnung vor Ablauf (Tage): nicht konfiguriert (Standardwert 10 gilt)</b></li> </ul> <p><b>Allgemein:</b></p> <ul style="list-style-type: none"> <li>■ <b>Kennwortgenerationen: 0</b></li> </ul>

Richtlinie	Einstellungen
<p><b>Standardrichtlinie für Device Encryption</b> Richtlinientyp: Geräteschutz</p>	<p>Verschlüsselung aller internen Festplatten.</p> <ul style="list-style-type: none"> <li>■ <b>Verschlüsselungsmodus für Medien: Volume-basierend</b></li> </ul> <p>Allgemeine Einstellungen:</p> <ul style="list-style-type: none"> <li>■ <b>Algorithmus für die Verschlüsselung: AES256</b></li> <li>■ <b>Schlüssel für die Verschlüsselung: Definierter Computerschlüssel</b></li> <li>■ <b>Benutzer darf einen lokalen Schlüssel erzeugen: nicht konfiguriert (Standardwert Ja gilt)</b></li> </ul> <p>Volume-basierende Einstellungen:</p> <ul style="list-style-type: none"> <li>■ <b>Benutzer darf dem verschlüsselten Volume Schlüssel hinzufügen oder diese entfernen: nicht konfiguriert (Standardwert Nein gilt)</b></li> <li>■ <b>Reaktion auf unverschlüsselte Volumes: Alle Medien akzeptieren und verschlüsseln</b></li> <li>■ <b>Benutzer darf Volume entschlüsseln: Nein</b></li> <li>■ <b>Bei defekten Sektoren fortfahren: Ja</b></li> </ul>
<p><b>Standardrichtlinie für Data Exchange</b> Richtlinientyp: Geräteschutz</p>	<p>Verschlüsselung von Wechselmedien</p> <ul style="list-style-type: none"> <li>■ <b>Verschlüsselungsmodus für Medien: Dateibasierend</b></li> </ul> <p>Allgemeine Einstellungen:</p> <ul style="list-style-type: none"> <li>■ <b>Algorithmus für die Verschlüsselung: AES256</b></li> <li>■ <b>Schlüssel für die Verschlüsselung: Beliebiger Schlüssel im Schlüsselring des Benutzers</b></li> </ul> <p>Dateibasierende Einstellungen:</p> <ul style="list-style-type: none"> <li>■ <b>SafeGuard Portable auf Wechselmedien kopieren: Ja</b></li> <li>■ <b>Benutzer darf eine Medien-Passphrase für Wechselmedien erzeugen: Ja</b></li> </ul>

Richtlinie	Einstellungen
<p><b>Standardrichtlinie für Computereinstellungen</b>                      Richtlinientyp: <b>Spezifische Computereinstellungen</b></p>	<p><b>Power-on Authentication (POA):</b></p> <ul style="list-style-type: none"> <li>■ <b>Power-on Authentication aktivieren: Ja</b></li> </ul> <p><b>Sicheres Wake On LAN (WOL):</b></p> <ul style="list-style-type: none"> <li>■ <b>Anzahl der automatischen Anmeldungen: 0</b></li> <li>■ <b>Anmeldung an Windows während WOL erlaubt: Nein</b></li> </ul> <p><b>Anzeigeoptionen:</b></p> <ul style="list-style-type: none"> <li>■ <b>Computer-Identifikation anzeigen: Name der Arbeitsstation</b></li> <li>■ <b>Rechtliche Hinweise anzeigen: Nein</b></li> <li>■ <b>Zusätzliche Informationen anzeigen: Nie</b></li> <li>■ <b>System Tray Icon aktivieren und anzeigen: Ja</b></li> <li>■ <b>Overlay-Symbole im Explorer anzeigen: Ja</b></li> <li>■ <b>Virtuelle Tastatur in der POA: Ja</b></li> </ul> <p><b>Installationsoptionen:</b></p> <ul style="list-style-type: none"> <li>■ <b>Deinstallation erlaubt: Ja</b></li> <li>■ <b>Sophos Manipulationsschutz aktivieren: Ja</b></li> </ul> <p><b>Hinweis:</b> Diese Einstellungen bezieht sich nur auf Endpoint-Computer, auf denen Version 9.5 von Sophos Endpoint Security and Control oder eine neuere Version installiert ist.</p>
<p><b>Standardrichtlinie für die Protokollierung</b>                      Richtlinientyp: <b>Protokollierung</b></p>	<p>Fehler nur in der Ereignisanzeige protokollieren. Andere Fehler werden nicht protokolliert.</p>

## 15.2 Mit ESDP verfügbare Standardrichtlinien

Für Optionen, bei denen in der folgenden Tabelle die Einstellung nicht konfiguriert angegeben ist, gelten automatisch Standardwerte. Die relevanten Standardwerte sind in Klammern angegeben.

**Hinweis:** Für eine detaillierte Beschreibung aller Richtlinieneinstellungen siehe [Richtlinieneinstellungen](#), Seite 80.

Richtlinie	Einstellungen
<b>Standardrichtlinie für allgemeine Einstellungen</b> Richtlinientyp: <b>Allgemeine Einstellungen</b>	<b>Anpassung:</b> <ul style="list-style-type: none"> <li>■ <b>Sprache am Client: Spracheinstellungen des Betriebssystems verwenden</b></li> </ul> <b>Recovery für die Anmeldung:</b> <ul style="list-style-type: none"> <li>■ <b>Recovery für die Anmeldung nach Beschädigung des Windows Local Cache aktivieren: Nein</b></li> </ul> <b>Local Self Help:</b> <ul style="list-style-type: none"> <li>■ <b>Local Self Help aktivieren: Ja</b></li> <li>■ <b>Minimale Länge der Antwort: 3</b></li> <li>■ <b>Benutzer dürfen eigene Fragen festlegen: Ja</b></li> </ul> <b>Challenge/Response (C/R):</b> <ul style="list-style-type: none"> <li>■ <b>Recovery für die Anmeldung über C/R aktivieren: Ja</b></li> <li>■ <b>Automatische Anmeldung an Windows erlauben: Ja</b></li> </ul>

Richtlinie	Einstellungen
<p><b>Standardrichtlinie für die Authentisierung</b>                      Richtlinientyp: Authentisierung</p>	<p><b>Zugriff:</b></p> <ul style="list-style-type: none"> <li>■ <b>Benutzer kann nur von der Festplatte booten: Ja</b></li> </ul> <p><b>Anmeldeoptionen:</b></p> <ul style="list-style-type: none"> <li>■ <b>Anmeldemodus: Benutzer-ID/Kennwort</b></li> <li>■ <b>Erfolgreiche Anmeldeversuche dieses Benutzers anzeigen: Nein</b></li> <li>■ <b>Letzte Benutzeranmeldung anzeigen: Nein</b></li> <li>■ <b>'Erzwungene Abmeldung' bei Sperre der Arbeitsstation deaktivieren: Nein</b></li> <li>■ <b>Letzte Benutzer/Domänen-Auswahl aktivieren: Ja</b></li> <li>■ <b>Durchgehende Anmeldung an Windows: Benutzer wählen lassen</b></li> </ul> <p><b>Erfolgreiche Anmeldungen:</b></p> <ul style="list-style-type: none"> <li>■ <b>Maximalanzahl von erfolgreichen Anmeldeversuchen: 16</b></li> <li>■ <b>Meldungen zur fehlgeschlagenen Anmeldung in der POA anzeigen: Standard</b></li> </ul> <p><b>Reaktion auf erfolgreiche Anmeldeversuche:</b></p> <ul style="list-style-type: none"> <li>■ <b>Computer sperren: Ja</b></li> </ul>

Richtlinie	Einstellungen
<p><b>Standardrichtlinie für Kennwörter</b> Richtlinientyp: <b>Kennwort</b></p>	<p><b>Kennwort:</b></p> <ul style="list-style-type: none"> <li>■ <b>Mindestlänge des Kennworts: 4</b></li> <li>■ <b>Maximallänge des Kennworts: 128</b></li> <li>■ <b>Mindestanzahl an Buchstaben: 0</b></li> <li>■ <b>Mindestanzahl an Ziffern: 0</b></li> <li>■ <b>Mindestanzahl an Symbolen: 0</b></li> <li>■ <b>Groß-/Kleinschreibung beachten: Nein</b></li> <li>■ <b>Tastaturzeile verboten: Nein</b></li> <li>■ <b>Tastaturspalte verboten: Nein</b></li> <li>■ <b>Drei oder mehr aufeinanderfolgende Zeichen verboten: Nein</b></li> <li>■ <b>Benutzername als Kennwort verboten: Nein</b></li> <li>■ <b>Liste nicht erlaubter Kennwörter verwenden: Nein</b></li> </ul> <p><b>Änderungen:</b></p> <ul style="list-style-type: none"> <li>■ <b>Kennwortänderung erlaubt nach mindestens (Tage): nicht konfiguriert (Standardwert 0 gilt)</b></li> <li>■ <b>Kennwort läuft ab nach (Tage): nicht konfiguriert (Standardwert 999 gilt)</b></li> <li>■ <b>Warnung vor Ablauf (Tage): nicht konfiguriert (Standardwert 10 gilt)</b></li> </ul> <p><b>Allgemein:</b></p> <ul style="list-style-type: none"> <li>■ <b>Kennwortgenerationen: 0</b></li> </ul>
<p><b>Standardrichtlinie für Device Encryption</b> Richtlinientyp: <b>Geräteschutz</b></p>	<p>Verschlüsselung aller internen Festplatten.</p> <ul style="list-style-type: none"> <li>■ <b>Verschlüsselungsmodus für Medien: Volume-basierend</b></li> </ul> <p><b>Allgemeine Einstellungen:</b></p> <ul style="list-style-type: none"> <li>■ <b>Algorithmus für die Verschlüsselung: AES256</b></li> <li>■ <b>Schlüssel für die Verschlüsselung: Definierter Computerschlüssel</b></li> </ul> <p><b>Volume-basierende Einstellungen:</b></p> <ul style="list-style-type: none"> <li>■ <b>Reaktion auf unverschlüsselte Volumes: Alle Medien akzeptieren und verschlüsseln</b></li> <li>■ <b>Benutzer darf Volume entschlüsseln: Nein</b></li> <li>■ <b>Bei defekten Sektoren fortfahren: Ja</b></li> </ul>

Richtlinie	Einstellungen
<p><b>Standardrichtlinie für Computereinstellungen</b>                      Richtlinientyp: <b>Spezifische Computereinstellungen</b></p>	<p><b>Power-on Authentication (POA):</b></p> <ul style="list-style-type: none"> <li>■ <b>Power-on Authentication aktivieren: Ja</b></li> </ul> <p><b>Sicheres Wake on LAN (WOL):</b></p> <ul style="list-style-type: none"> <li>■ <b>Anzahl der automatischen Anmeldungen: 0</b></li> <li>■ <b>Anmeldung an Windows während WOL erlaubt: Nein</b></li> </ul> <p><b>Anzeigeoptionen:</b></p> <ul style="list-style-type: none"> <li>■ <b>Computer-Identifikation anzeigen: Name der Arbeitsstation</b></li> <li>■ <b>Rechtliche Hinweise anzeigen: Nein</b></li> <li>■ <b>Zusätzliche Informationen anzeigen: Nie</b></li> <li>■ <b>System Tray Icon aktivieren und anzeigen: Ja</b></li> <li>■ <b>Overlay-Symbole im Explorer anzeigen: Ja</b></li> <li>■ <b>Virtuelle Tastatur in der POA: Ja</b></li> </ul> <p><b>Installationsoptionen:</b></p> <ul style="list-style-type: none"> <li>■ <b>Deinstallation erlaubt: Ja</b></li> <li>■ <b>Sophos Manipulationsschutz aktivieren: Ja</b></li> </ul> <p><b>Hinweis:</b> Diese Einstellung gilt nur für Endpoint-Computer, auf denen Sophos Endpoint Security and Control in der Version 9.5 oder in einer neueren Version installiert ist.</p>
<p><b>Standardrichtlinie für die Protokollierung</b>                      Richtlinientyp: <b>Protokollierung</b></p>	<p>Nur Fehler in der Ereignisanzeige protokollieren, andere Ereignisse ignorieren.</p>

## 16 Richtlinienereinstellungen

Die Sophos SafeGuard Richtlinien enthalten alle Einstellungen, die zur Abbildung einer unternehmensweiten Sicherheitsrichtlinie auf den Endpoint-Computern wirksam werden sollen.

In den Sophos SafeGuard Richtlinien können Sie Einstellungen für die folgenden Bereiche (Richtlinientypen) festlegen:

### ■ **Allgemeine Einstellungen**

Enthält Einstellungen für z. B. Transferrate, Hintergrundbilder usw.

### ■ **Authentisierung**

Enthält Einstellungen zum Anmeldemodus, zur Gerätesperre usw.

### ■ **Kennwörter**

Legt Anforderungen an die verwendeten Kennwörter fest.

### ■ **Passphrasen für SafeGuard Data Exchange**

**Hinweis:** Diese Einstellungen werden mit ESDP (Endpoint Security and Data Protection) nicht unterstützt.

Legt Anforderungen für die verwendeten Passphrasen fest. Passphrasen werden bei der Schlüsselerzeugung für den sicheren Datenaustausch mit SafeGuard Data Exchange verwendet.

### ■ **Geräteschutz**

Enthält Einstellungen für die volume- oder dateibasierende Verschlüsselung (auch Einstellungen für SafeGuard Data Exchange und SafeGuard Portable): Algorithmen, Schlüssel, Daten auf welchen Laufwerken sollen verschlüsselt werden, usw.

### ■ **Spezifische Computereinstellungen**

Enthält Einstellungen zur Power-on Authentication (aktivieren/deaktivieren), zum sicheren Wake On LAN, Anzeigeoptionen, usw.

### ■ **Protokollierung**







Legt fest, welche Ereignisse protokolliert werden.

In den folgenden Abschnitten finden Sie eine detaillierte Beschreibung der Richtlinienereinstellungen, die im SafeGuard Policy Editor zur Verfügung stehen.





Für Sophos SafeGuard stehen in den beiden Produkt-Bundles mit SGE (SafeGuard Easy) und ESDP (Endpoint Security and Data Protection) unterschiedliche Einstellungen zur Verfügung. Für ESDP sind keine Einstellungen verfügbar, die sich auf dateibasierende Verschlüsselung und SafeGuard Data Exchange beziehen. In der folgenden Beschreibung sind die für SGE und ESDP verfügbaren Einstellungen jeweils durch einen Haken in der entsprechenden Spalte gekennzeichnet.

## 16.1 Allgemeine Einstellungen

Richtlinieneinstellung	SGE	ESDP	Erklärung
<b>ANPASSUNG</b>			
<b>Sprache am Client</b>	✓	✓	Legt fest, in welcher Sprache die Einstellungen für Sophos SafeGuard am Endpoint-Computer angezeigt werden. Neben den unterstützten Sprachen kann auch die Betriebssystem-Spracheinstellung des Endpoint-Computers ausgewählt werden.
<b>RECOVERY FÜR DIE ANMELDUNG</b>			
<b>Recovery für die Anmeldung nach Beschädigung des Windows Local Cache aktivieren</b>	✓	✓	Im Windows Local Cache werden alle Schlüssel, Richtlinien, Benutzertifikate und Audit-Dateien gespeichert. Alle im Local Cache gespeicherten Daten haben eine Signatur und können nicht manuell geändert werden. Für einen korrupten Windows Local Cache ist der Recovery-Vorgang für die Anmeldung standardmäßig deaktiviert. Das heißt, in diesem Fall wird der Windows Local Cache automatisch aus seiner Sicherungskopie wiederhergestellt. Für die Reparatur des Windows Local Cache ist also in diesem Fall kein Challenge/Response-Verfahren notwendig. Wenn der Windows Local Cache explizit über ein Challenge/Response-Verfahren repariert werden soll, wählen Sie in diesem Feld die Einstellung "JA".

Richtlinieneinstellung	SGE	ESDP	Erklärung
<b>Local Self Help aktivieren</b>			
<b>Local Self Help aktivieren</b>			Legt fest, ob sich ein Sophos SafeGuard Benutzer über Local Self Help an seinem Computer anmelden darf, wenn er sein Kennwort vergessen hat. Local Self Help ermöglicht dem Benutzer die Anmeldung durch die Beantwortung einer definierten Anzahl an zuvor festgelegten Fragen in der Power-on Authentication. Somit kann sich der Benutzer im Notfall auch in Situationen, in denen weder eine Telefon- noch eine Internetverbindung zur Verfügung stehen, ohne die Durchführung eines Challenge/Response-Verfahrens wieder Zugang zu seinem Computer verschaffen. Mit Local Self Help lassen sich Helpdesk-Aufwände und Kosten reduzieren. Für die Benutzung von Local Self Help ist es notwendig, dass die automatische Anmeldung an Windows aktiviert ist. Andernfalls funktioniert die Anmeldung über Local Self Help nicht.
<b>Mindestlänge der Antwort</b>			Legen Sie hier die Mindestlänge (in Zeichen) für die Antworten fest, die für Local Self Help auf dem Endpoint-Computer hinterlegt werden.
<b>Willkommenstext unter Windows</b>			Hier können Sie einen individuellen Informationstext angeben, der beim Starten des Local Self Help Assistenten im ersten Dialog angezeigt werden soll. Dieser Text muss zuvor erstellt und registriert werden.

Richtlinieneinstellung	SGE	ESDP	Erklärung
<b>Benutzer dürfen eigene Fragen festlegen</b>	✔	✔	Die für Local Self Help zu beantwortenden Fragen können Sie als zuständiger Sicherheitsbeauftragter zentral vordefinieren und per Richtlinie an den Endpoint-Computer verteilen. Sie können die Benutzer jedoch auch per Richtlinie berechtigen, selbst Fragen zu definieren. Um die Benutzer zur Definition eigener Fragen zu berechtigen, wählen Sie in diesem Feld die Einstellung <b>Ja</b> .
<b>Challenge/Response (CR)</b>			
<b>Recovery für die Anmeldung über C/R aktivieren</b>	✔	✔	<p>Legt fest, ob ein Benutzer in der Power-on Authentication (POA) für Recovery-Zwecke eine Challenge erzeugen darf, um über ein Challenge/Response-Verfahren wieder Zugang zu seinem Computer zu erhalten.</p> <ul style="list-style-type: none"> <li>■ <b>Ja:</b> Der Benutzer darf eine Challenge erzeugen und die <b>Challenge</b> Schaltfläche in der POA ist aktiv. In diesem Fall kann der Benutzer über ein Challenge/Response-Verfahren wieder Zugang zu seinem Computer erhalten.</li> <li>■ <b>Nein:</b> Der Benutzer darf keine Challenge erzeugen und die <b>Challenge</b> Schaltfläche in der POA ist nicht aktiv. In diesem Fall kann der Benutzer kein C/R-Verfahren starten, um wieder Zugang zu seinem Computer zu erhalten.</li> </ul> <p>Sophos SafeGuard bietet darüber hinaus die Recovery-Methode Local Self Help. Diese Methode kann über die Richtlinieneinstellung <b>Local Self Help aktivieren</b> aktiviert werden.</p>

Richtlinieneinstellung	SGE	ESDP	Erklärung
<b>Informationstext</b>			<p>Zeigt nach dem Starten eines Challenge/Response-Vorgangs in der POA einen Informationstext. Als Informationstext kann hier beispielsweise stehen "Bitte rufen Sie Ihren Support unter der Telefonnummer 01234- 56789.an". Bevor Sie einen Text angeben können, muss dieser als Textdatei im <b>Richtlinien</b> Navigationsbereich unter <b>Informationstext</b> erstellt werden.</p>
<b>Automatische Anmeldung anWindows erlauben</b>			<p>Erlaubt dem Benutzer nach einer Authentisierung per Challenge/Response die automatische Anmeldung an Windows.</p> <ul style="list-style-type: none"> <li>■ <b>Ja:</b> Benutzer wird automatisch an Windows angemeldet.</li> <li>■ <b>Nein:</b> Windows-Anmeldebildschirm erscheint.</li> </ul> <p><b>Anwendungsfall:</b> Ein Benutzer hat sein Kennwort vergessen. Sophos SafeGuard meldet ihn nach Austausch von Challenge und Response ohne Sophos SafeGuard Kennwort am Computer an. In diesem Fall wird die automatische Anmeldung an Windows ausgeschaltet und der Windows-Anmeldebildschirm erscheint. Da der Benutzer sein Sophos SafeGuard Kennwort (= Windows-Kennwort) nicht weiß, kann er sich nicht anmelden. Mit <b>Ja</b> wird eine automatische Anmeldung erlaubt und der Benutzer bleibt nicht im Windows-Anmeldebildschirm stecken.</p>
<b>BILDER</b>			<p>Voraussetzung: Neue Bilder müssen im <b>Richtlinien-Navigationsbereich</b> des SafeGuard Policy Editor unter <b>Bilder</b> registriert werden. Erst nach der Registrierung sind die Bilder verfügbar. Unterstützte Formate: .BMP, PNG, JPEG.</p>





Richtliniensestellung	SGE	ESDP	Erklärung
<p><b>Hintergrundbild in der POA</b></p> <p><b>Hintergrund-Bild in der POA (niedrige Auflösung)</b></p>	✓	✓	<p>Tauscht das blaue Hintergrund-Bitmap mit SafeGuard-Design gegen ein selbstgewähltes aus. Kunden können hier z. B. das Unternehmens-Logo in der POA verwenden. Maximale Dateigröße für alle Hintergrundbilder: 500 KB</p> <p>Normal:</p> <ul style="list-style-type: none"> <li>■ Auflösung: 1024 x 768 (VESA-Modus)</li> <li>■ Farben: keine Einschränkung</li> </ul> <p>Niedrig:</p> <ul style="list-style-type: none"> <li>■ Auflösung: 640 x 480 (VGA-Modus)</li> <li>■ Farben: 16 Farben</li> </ul>
<p><b>Anmeldebild in der POA</b></p> <p><b>Anmeldebild in der POA (niedrige Auflösung)</b></p>	✓	✓	<p>Tauscht das Sophos SafeGuard Bitmap aus, das im Anmeldedialog der POA angezeigt wird. Hier kann zum Beispiel das Firmenlogo angezeigt werden.</p> <p>Normal:</p> <ul style="list-style-type: none"> <li>■ Auflösung: 413 x 140 Pixel</li> <li>■ Farben: keine Einschränkung</li> </ul> <p>Niedrig:</p> <ul style="list-style-type: none"> <li>■ Auflösung: 413 x 140 Pixel</li> <li>■ Farben: 16 Farben</li> </ul>



## 16.2 Authentisierung







Wie sich Benutzer an ihrem Computer anmelden, wird in einer Richtlinie vom Typ **Authentisierung** festgelegt.

Richtlinieneinstellung	SGE	ESDP	Erklärung
<b>ZUGRIFF</b>			
<b>Benutzer kann nur von der Festplatte booten</b>	✔	✔	Legt fest, ob Benutzer den Computer von Festplatte und/oder anderem Medium starten dürfen. <b>Ja:</b> Benutzer darf ausschließlich von der Festplatte booten. Die Möglichkeit, den Computer mit Diskette oder einem weiteren externen Medium zu starten, wird nicht in der POA angeboten. <b>Nein:</b> Benutzer darf den Computer von Festplatte, Diskette oder einem externen Medium (USB, CD etc.) starten.
<b>ANMELDEOPTIONEN</b>			
<b>Anmeldemodus</b>	✔	Verfügbare ✔ Option für diese Einstellung: <b>Benutzername/Kennwort</b> <b>Hinweis:</b> Die Anmeldung mit Fingerabdruck ist mit ESDP nicht verfügbar.	Legt fest, wie sich ein Benutzer in der POA authentisieren muss. <ul style="list-style-type: none"> <li>■ <b>Benutzername/Kennwort:</b> Der Benutzer muss sich mit Benutzername und Kennwort in der POA anmelden.</li> <li>■ <b>Fingerabdruck:</b> Wählen Sie diese Option, um die Anmeldung mit Lenovo-Fingerabdruck-Leser zu aktivieren. Benutzer, für die diese Richtlinie wirksam ist, können sich mit Fingerabdruck oder Benutzername/Kennwort anmelden. Dieser Vorgang bietet das höchste Maß an Sicherheit.</li> </ul>

Richtlinieneinstellung	SGE	ESDP	Erklärung
			<p>Bei der Anmeldung führt der Benutzer den Finger über den Fingerabdruck-Leser. Wenn der Fingerabdruck erfolgreich erkannt wurde, liest die Power-on Authentication die Anmeldeinformationen des Benutzers und meldet den Benutzer an der Power-on Authentication an. Die Anmeldeinformationen werden dann an Windows übertragen und der Benutzer wird an seinem Computer angemeldet.</p> <p><b>Hinweis:</b> Nach Auswahl dieses Anmeldevorgangs kann sich der Benutzer nur mit einem vorher registrierten Fingerabdruck oder mit Benutzername und Kennwort anmelden.</p>
<b>Erfolgreiche Anmeldeversuche dieses Benutzers anzeigen</b>	✔	✔	<p>Zeigt (Einstellung: <b>Ja</b>) nach der Anmeldung in der POA und Windows einen Dialog mit Informationen über die letzte fehlgeschlagene Anmeldung (Benutzername/Datum/Zeit) an.</p>
<b>Letzte Benutzeranmeldung anzeigen</b>	✔	✔	<p>Zeigt (Einstellung: <b>Ja</b>) nach der Anmeldung in der POA und Windows einen Dialog mit Informationen über die</p> <ul style="list-style-type: none"> <li>■ Letzte erfolgreiche Anmeldung (Benutzername/Datum/Zeit)</li> <li>■ Letzte Anmeldeinformationen des angemeldeten Benutzers an.</li> </ul>

Richtlinieneinstellung	SGE	ESDP	Erklärung
<b>'Erzwungene Abmeldung' bei Sperre der Arbeitsstation deaktivieren</b>			<p>Wenn Benutzer den Computer nur für kurze Zeit verlassen wollen, können Sie den Rechner mittels Klick auf die Schaltfläche <b>Arbeitsstation sperren</b> für andere Benutzer sperren und danach mit ihrem Kennwort wieder entsperren. Steht diese Einstellung auf NEIN, dann kann sowohl jener Benutzer, der die Arbeitsstation gesperrt hat, als auch ein Administrator diese Sperre aufheben. Hebt ein Administrator die Sperre auf, so wird der aktuell angemeldete Benutzer zwangsweise abgemeldet. Die Einstellung JA ändert dieses Verhalten. In diesem Fall kann nur der Benutzer die Sperre der Arbeitsstation aufheben. Ein Aufheben der Sperre durch den Administrator und das damit verbundene erzwungene Abmelden des Benutzers ist nicht mehr möglich.</p> <p><b>Hinweis:</b> Diese Einstellung wird nur unter Windows XP wirksam.</p>
<b>Letzte Benutzer/Domänen Auswahl aktivieren</b>			<p><b>Ja:</b> Die POA speichert den Benutzernamen und die Domäne des letzten angemeldeten Benutzers. Benutzer müssen den Benutzernamen also nicht jedesmal eingeben, wenn sie sich anmelden.</p> <p><b>Nein:</b> Die POA speichert den Benutzernamen und die Domäne des letzten angemeldeten Benutzers <u>nicht</u>.</p>

Richtlinieneinstellung	SGE	ESDP	Erklärung
<b>Durchgehende Anmeldung an Windows</b>			<p><b>Hinweis:</b> Soll der Benutzer in der Lage sein, anderen Benutzern Zugriff auf "seinen" Computer zu gewähren, muss er in der Lage sein, die durchgehende Anmeldung an Windows zu deaktivieren.</p> <ul style="list-style-type: none"> <li>■ <b>Benutzer wählen lassen</b> Im POA Anmeldedialog kann der Benutzer durch aktivieren/deaktivieren dieser Option entscheiden, ob er automatisch an Windows angemeldet werden will oder nicht.</li> <li>■ <b>Durchgehende Anmeldung erzwingen</b> Der Benutzer wird immer automatisch an Windows angemeldet.</li> <li>■ <b>Durchgehende Anmeldung deaktivieren</b> Der Windows Anmeldedialog wird nach der POA-Anmeldung angezeigt und der Benutzer muss sich manuell an Windows anmelden.</li> </ul>

Richtlinieneinstellung	SGE	ESDP	Erklärung
<b>Service Account Liste</b>			<p>Um zu verhindern, dass administrative Vorgänge auf einem durch Sophos SafeGuardgeschützten Computer bewirken, dass die Power-on Authentication aktiviert wird und Rollout-Beauftragte als Benutzer zum Computer hinzugefügt werden, bietet Sophos SafeGuardService Account Listen für Sophos SafeGuard Endpoint-Computer. Die Benutzer, die in diese Listen aufgenommen werden, werden als Sophos SafeGuardGastbenutzer behandelt.</p> <p>Damit Sie in diesem Feld eine Liste auswählen können, müssen Sie zunächst im <b>Richtlinien</b> Navigationsbereich unter <b>Service Account Listen</b> Listen anlegen.</p>
<b>ERFOLGLOSE ANMELDUNGEN</b>			
<b>Maximalanzahl von erfolglosen Anmeldeversuchen</b>			<p>Bestimmt, wie oft ein Benutzer ohne Folgen bei der Anmeldung einen ungültigen Benutzernamen bzw. ein ungültiges Kennwort eingeben darf. Mit "3" darf der Benutzer beispielsweise dreimal hintereinander seinen Benutzernamen oder sein Kennwort falsch eingeben, beim vierten Mal greift die Einstellung unter "Reaktion auf erfolglose Anmeldungen".</p>
<b>Reaktion auf erfolglose Anmeldeversuche</b>			
<b>Computer sperren</b>			<p>Legt fest, ob der Computer nach fehlgeschlagenen Anmeldeversuchen gesperrt wird. Die Computersperre kann durch Neustart des Computers und durchAnmeldung eines lokalen Administrators aufgehoben werden. Beachten Sie in diesem Zusammenhang auch die Benutzersperre von Windows.</p>

Richtlinieneinstellung	SGE	ESDP	Erklärung
<b>OPTIONEN FÜR SPERRE DES GERÄTS</b>			
<b>Bildschirm nach X Minuten Leerlauf sperren</b>	✔	✔	Bestimmt die Zeit, nach deren Überschreitung ein nicht mehr benutzter Desktop automatisch gesperrt wird. Der Standardwert beträgt 0 Minuten, in diesem Fall erfolgt kein automatisches Schließen.
<b>Bildschirm nach dem Fortsetzen sperren</b>	✔	✔	Bestimmt, ob der Bildschirm bei Reaktivierung aus dem Standby-Modus gesperrt wird.

## 16.3 Liste nicht erlaubter Kennwörter für Richtlinien erstellen

Für Richtlinien vom Typ **Kennwort** lässt sich eine Liste mit nicht erlaubten Kennwörtern anlegen. In dieser Liste definieren Sie Zeichenfolgen, die nicht in Kennwörtern verwendet werden dürfen.

**Hinweis:** In den Listen werden die nicht erlaubten Kennwörter durch jeweils neue Zeilenanfänge voneinander getrennt.

Die Textdateien mit den gewünschten Informationen müssen erstellt werden, bevor sie im SafeGuard Policy Editor registriert werden können. Die maximale Dateigröße für Textdateien beträgt **50 KB**. Sophos SafeGuard verwendet nur Unicode UTF-16 kodierte Texte. Wenn Sie die Textdateien nicht in diesem Format erstellen, werden Sie bei der Registrierung automatisch in dieses Format konvertiert.

Wenn eine Konvertierung durchgeführt wird, werden Sie durch eine Meldung darüber informiert.

So registrieren Sie die Textdateien:

1. Klicken Sie im Richtlinien-Navigationsbereich mit der rechten Maustaste auf **Informationstext** und wählen Sie **Neu > Text**.
2. Geben Sie unter **Textelementname** einen Namen für den anzuzeigenden Text ein.
3. Wählen Sie über die Schaltfläche [...] die zuvor erstellte Textdatei aus. Wenn eine Konvertierung notwendig ist, wird eine entsprechende Meldung angezeigt.
4. Klicken Sie auf **OK**.

Das neue Textelement wird als Unterknoten des Eintrags **Informationstext** im Richtlinien-Navigationsbereich angezeigt. Ist ein Textelement markiert, wird sein Inhalt im Aktionsbereich auf der rechten Seite angezeigt. Das Textelement kann jetzt beim Erstellen von Richtlinien ausgewählt werden.

Gehen Sie wie beschrieben vor, um weitere Textelemente zu registrieren. Alle registrierten Textelemente werden als Unterknoten angezeigt.




**Hinweis:** Mit der Schaltfläche **Text ändern** können Sie weiteren Text zum bestehenden Text hinzufügen. Es wird ein Dialog geöffnet, in dem eine weitere Textdatei ausgewählt werden kann. Der in dieser Datei enthaltene Text wird am Ende des bestehenden Texts eingefügt.

## 16.4 Syntaxregeln für Kennwörter



Kennwörter können sowohl Ziffern, Buchstaben als auch Sonderzeichen (wie + - ; etc.) enthalten. Verwenden Sie bei der Vergabe eines neuen Kennworts jedoch keine Zeichen mit der Kombination ALT + <Zeichen>, da dieser Eingabemodus an der Power-on Authentication nicht zur Verfügung steht. Wie Kennwörter, mit denen sich Benutzer am System anmelden, beschaffen sein müssen, wird in Richtlinien vom Typ **Kennwort** eingestellt.

**Hinweis:** Wenn im SafeGuard Policy Editor Regeln für Kennwörter definiert werden, dann sollten im Active Directory keine Regeln definiert werden.

Richtlinieneinstellung	SGE	ESDP	Erklärung
<b>RULES</b>			
<b>Mindestlänge des Kennwortes</b>	✔	✔	Zeigt an, aus wie vielen Zeichen ein Kennwort bei der Änderung durch den Benutzer mindestens bestehen muss. Der gewünschte Wert kann entweder direkt eingegeben oder durch Betätigen der Richtungstasten vergrößert bzw. verkleinert werden.
<b>Maximallänge des Kennwortes</b>	✔	✔	Zeigt an, aus wie vielen Zeichen ein Kennwort bei der Änderung durch den Benutzer maximal bestehen darf. Der gewünschte Wert kann entweder direkt eingegeben oder durch Betätigen der Richtungstasten vergrößert bzw. verkleinert werden.
<b>Mindestanzahl an Buchstaben</b> <b>Mindestanzahl an Ziffern</b> <b>Mindestanzahl an Symbolen</b>	✔	✔	Mit diesen Einstellungen wird erreicht, dass Kennwörter nicht ausschließlich Zeichen, Ziffern oder Sonderzeichen enthalten, sondern aus einer Kombination bestehen müssen (z. B. „15blume“ etc.). Diese Einstellung ist nur dann sinnvoll, wenn eine Kennwortmindestlänge definiert ist, die größer 2 ist.

Richtlinieneinstellung	SGE	ESDP	Erklärung
<b>Groß-/Kleinschreibung beachten</b>			<p>Diese Einstellung wird nur bei den Optionen <b>Liste nicht erlaubter Kennwörter verwenden</b> und <b>Benutzername als Kennwort verboten</b> wirksam.</p> <p><b>Fall 1:</b> Sie haben in der Liste der verbotenen Kennwörter „Tafel“ eingetragen. Steht die Option <b>Groß-/Kleinschreibung beachten</b> auf <b>Ja</b>, werden zusätzliche Kennwortvarianten wie z. B. „TAFEL“ oder „TaFeL“ nicht akzeptiert und die Anmeldung wird verweigert.</p> <p><b>Fall 2:</b> Der Benutzername für einen Anwender lautet „EMaier“. Steht <b>Groß-/Kleinschreibung beachten</b> auf <b>Ja</b> und <b>Benutzername als Kennwort verboten</b> auf <b>Nein</b>, darf Benutzer EMaier keine Variante seines Benutzernamens (z. B. 'emaier' oder 'eMaiEr' etc.) als Kennwort verwenden.</p>
<b>Tastaturzeile verboten</b>			<p>Tastaturzeilen sind „123“ oder „qwe“. Maximal zwei auf der Tastatur nebeneinander liegende Zeichen sind erlaubt. Tastaturzeilen beziehen sich nur auf den alphanumerischen Tastaturteil.</p>
<b>Tastaturspalte verboten</b>			<p>Als Tastaturspalten werden eingetippte Zeichenreihen wie „yaq1“, „xsw2“ oder „3edc“ (nicht aber „yse4“, „xdr5“ oder „cft6“!) bezeichnet. Erlaubt sind maximal zwei in einer Tastaturspalte befindliche Zeichen. Verbieten Sie Tastaturspalten, werden derartige Zeichenkombinationen als Kennwörter abgelehnt. Tastaturspalten beziehen sich nur auf den alphanumerischen Tastaturteil.</p>

Richtlinieneinstellung	SGE	ESDP	Erklärung
<b>Drei oder mehr aufeinanderfolgende Zeichen verboten</b>	✔	✔	<p>Verboten werden mit Aktivierung dieser Option Zeichenketten,</p> <ul style="list-style-type: none"> <li>■ die im ASCII-Code aufeinander folgen, sowohl in auf- als auch in absteigender Reihenfolge („abc“; „cba“; „;&lt;“ etc.).</li> <li>■ die aus drei oder mehr identischen Zeichen („aaa“ oder „111“) bestehen.</li> </ul>
<b>Benutzername als Kennwort verboten</b>	✔	✔	<p>Bestimmt, ob Benutzername und Kennwort identisch sein dürfen.</p> <p><b>Ja:</b> Windows-Benutzername und Kennwort müssen unterschiedlich sein.</p> <p><b>Nein:</b> Benutzer darf seinen Windows-Benutzernamen gleichzeitig als Kennwort verwenden.</p>
<b>Liste nicht erlaubter Kennwörter verwenden</b>	✔	✔	<p>Bestimmt, ob bestimmte Zeichenfolgen für Kennwörter nicht verwendet werden dürfen. Abgelegt sind die Zeichenfolgen in der Liste nicht erlaubter Kennwörter (z. B. Datei im Format .txt).</p>
<b>Liste nicht erlaubter Kennwörter</b>	✔	✔	<p>Definiert Zeichenfolgen, die in einem Kennwort ausgeschlossen sind. Wenn ein Benutzer ein verbotenes Kennwort verwendet, wird eine Fehlermeldung ausgegeben.</p> <p><b>Wichtige Voraussetzung:</b>            Eine Liste (eine Datei) mit verbotenen Kennwörtern muss im SafeGuard Policy Editor unter <b>Informationstext</b> im Richtlinien-Navigationsbereich registriert werden. Erst nach der Registrierung ist die Liste verfügbar.</p> <p>Maximale Dateigröße: 50 KB            Unterstütztes Format: Unicode</p>

Richtlinieneinstellung	SGE	ESDP	Erklärung
			<p><b>Nicht erlaubte Kennwörter definieren</b></p> <p>In der Liste werden die verbotenen Kennwörter durch einen neuen Zeilenanfang getrennt. Wildcard: An der Position, an der Sie den Zeichentyp „*“ eingeben, können mehrere beliebige Zeichen im Kennwort enthalten sein. Beispielsweise wird durch *123* jede Zeichenfolge, die 123 enthält, als Kennwort verboten.</p> <ul style="list-style-type: none"> <li>■ Wenn Sie nur die Wildcard in die Liste einfügen, können sich Benutzer nach einer erzwungenen Kennwortänderung nicht mehr im System anmelden.</li> <li>■ Benutzer dürfen auf die Datei keinen Zugriff haben.</li> <li>■ Die Option <b>Liste nicht erlaubter Kennwörter verwenden</b> muss aktiviert sein.</li> </ul>
<b>ÄNDERUNGEN</b>			
<b>Kennwortänderung erlaubt nach mindestens (Tage)</b>			<p>Legt den Zeitraum fest, in dem ein Kennwort nicht erneut geändert werden darf. Diese Einstellung verhindert, dass ein Benutzer sein Kennwort innerhalb eines bestimmten Zeitraums beliebig oft ändern kann.</p> <p><b>Beispiel:</b></p> <p>Die Benutzerin Schmidt definiert ein neues Kennwort (z. B. „13jk56“). Für sie (oder für die Gruppe, der sie zugeordnet ist) ist ein Wechsel nach mind. fünf Tagen festgelegt. Bereits nach zwei Tagen will sie das Kennwort „13jk56“ ändern. Dies wird abgelehnt, da Frau Schmidt erst nach fünf Tagen ein neues Kennwort definieren darf.</p>

Richtlinieneinstellung	SGE	ESDP	Erklärung
<b>Kennwort läuft ab nach (Tage)</b>	✔	✔	Wird die maximale Gültigkeitsdauer aktiviert, muss der Benutzer nach dem eingetragenen Zeitraum sein Kennwort wechseln und ein neues Kennwort definieren.
<b>Warnung vor Ablauf (Tage)</b>	✔	✔	Ab „n“ Tagen vor Ablauf des Kennworts wird eine Warnmeldung ausgegeben und der Benutzer darauf hingewiesen, dass er in „n“-Tagen sein Kennwort ändern muss. Er erhält daraufhin die Möglichkeit, das Kennwort sofort zu ändern.
<b>ALLGEMEIN</b>			
<b>Kennwortgenerationen</b>	✔	✔	Bestimmt, wann bereits verwendete Kennwörter wieder verwendet werden dürfen. Sinnvoll ist die Definition von Kennwortgenerationen insbesondere in Verbindung mit der Einstellung „Kennwort läuft ab nach (Tage)“.
<b>Kennwortgenerationen</b>	✔	✔	<b>Beispiel:</b> Die Anzahl der Kennwortgenerationen für den Benutzer Müller wurde auf 4 festgelegt, die der Tage, nach denen der Benutzer das Kennwort wechseln muss, auf 30. Herr Müller meldete sich bislang mit dem Kennwort „Informatik“ an. Nach Ablauf der Frist von 30 Tagen wird er aufgefordert, sein Kennwort zu ändern. Herr Müller tippt als neues Kennwort wieder „Informatik“ ein und erhält die Fehlermeldung, dass er dieses Kennwort bereits verwendet hat und ein anderes Kennwort wählen muss. „Informatik“ darf Herr Müller erst nach der vierten (da Kennwortgenerationen = 4) Aufforderung zur Eingabe eines neuen Kennworts verwenden.

## 16.5 Passphrase für SafeGuard Data Exchange

**Hinweis:** Diese Einstellungen werden mit ESDP (Endpoint Security and Data Protection) nicht unterstützt. Für eine Beschreibung von SafeGuard Data Exchange, siehe [SafeGuard Data Exchange](#), Seite 118.

Für den sicheren Datenaustausch über SafeGuard Data Exchange, muss der Benutzer eine Passphrase eingeben, die für die Erzeugung von lokalen Schlüsseln verwendet wird. Welchen Anforderungen diese Passphrase entsprechen muss, wird in Richtlinien vom Typ **Passphrase** eingestellt. Weitere Informationen zu SafeGuard Data Exchange und SafeGuard Portable finden Sie auch in der Sophos SafeGuard Benutzer-Hilfe im Kapitel *SafeGuard Data Exchange*.

Richtlinieneinstellung	SGE	ESDP	Erklärung
<b>Mindestlänge der Passphrase</b>	✔		Legt fest, aus wievielen Zeichen die Passphrase, aus der der Schlüssel erzeugt wird, mindestens bestehen muss. Der gewünschte Wert kann entweder direkt eingegeben oder durch Betätigen der Richtungstasten vergrößert bzw. verkleinert werden.
<b>Maximallänge der Passphrase</b>	✔		Legt fest, aus wievielen Zeichen die Passphrase maximal bestehen darf. Der gewünschte Wert kann entweder direkt eingegeben oder durch Betätigen der Richtungstasten vergrößert bzw. verkleinert werden.
<b>Mindestanzahl an Buchstaben</b> <b>Mindestanzahl an Ziffern</b> <b>Mindestanzahl an Symbolen</b>	✔		Mit diesen Einstellungen wird erreicht, dass eine Passphrase nicht ausschließlich Zeichen, Ziffern oder Sonderzeichen enthält, sondern aus einer Kombination bestehen muss (z. B. „15blume“ etc.). Diese Einstellung ist nur dann sinnvoll, wenn eine Mindestlänge definiert ist, die größer 2 ist.

Richtlinieneinstellung	SGE	ESDP	Erklärung
<b>Groß-/Kleinschreibung beachten</b>			Diese Einstellung wird beim Setzen der Option <b>Benutzername als Passphrase verboten</b> wirksam. <b>Beispiel:</b> Der Benutzername für einen Anwender lautet „EMaier“. Steht <b>Groß-/Kleinschreibung beachten</b> auf <b>Ja</b> und <b>Benutzername als Passphrase verboten</b> auf <b>Nein</b> , darf Benutzer EMaier keine Variante seines Benutzernamens (z. B. 'emaier' oder 'eMaiEr' etc.) als Passphrase verwenden.
<b>Tastaturzeile verboten</b>			Tastaturzeilen sind „123“ oder „qwe“. Maximal zwei auf der Tastatur nebeneinander liegende Zeichen sind erlaubt. Tastaturreihen beziehen sich nur auf den alphanumerischen Tastaturteil.
<b>Tastaturspalte verboten</b>			Als Tastaturspalten werden eingetippte Zeichenreihen wie „yaq1“, „xsw2“ oder „3edc“ (nicht aber „yse4“, „xdr5“ oder „cft6“!) bezeichnet. Erlaubt sind maximal zwei in einer Tastaturspalte befindliche Zeichen. Verbieten Sie Tastaturspalten, werden derartige Zeichenkombinationen als Passphrase abgelehnt. Tastaturspalten beziehen sich nur auf den alphanumerischen Tastaturteil.
<b>Drei oder mehr aufeinanderfolgende Zeichen verboten</b>			Verboten werden mit Aktivierung dieser Option Zeichenketten, <ul style="list-style-type: none"> <li>■ die im ASCII-Code aufeinander folgen, sowohl in auf-, als auch in absteigender Reihenfolge („abc“; „cba“; „;&lt;“ etc.)</li> <li>■ die aus drei oder mehr identischen Zeichen („aaa“ oder „111“) bestehen.</li> </ul>
<b>Benutzername als Passphrase verboten</b>			Bestimmt, ob Benutzername und Passphrase identisch sein dürfen. <b>Ja:</b> Benutzer darf seinen Windows-Benutzernamen gleichzeitig als Passphrase verwenden. <b>Nein:</b> Windows-Benutzername und Passphrase müssen unterschiedlich sein.

## 16.6 Geräteschutz

Ein Kernstück von Sophos SafeGuard ist die Verschlüsselung von Daten auf unterschiedlichen Datenträgern. Die Verschlüsselung kann volume- oder dateibasierend durchgeführt werden, mit unterschiedlichen Schlüsseln und Algorithmen. Richtlinien des Typs Geräteschutz enthalten auch Einstellungen für SafeGuard Data Exchange und SafeGuard Portable.

**Hinweis:** Weitere Informationen zu SafeGuard Data Exchange und SafeGuard Portable finden Sie auch in der Sophos SafeGuard Benutzer-Hilfe im Kapitel *SafeGuard Data Exchange*.

**Hinweis:** SafeGuard Data Exchange, SafeGuard Portable sowie dateibasierende Verschlüsselung werden mit ESDP nicht unterstützt.

Wenn Sie eine Richtlinie dieses Typs erstellen, müssen Sie zunächst ein Ziel für den Geräteschutz angeben. Mögliche Ziele sind:

- Massenspeicher (Boot-Laufwerke/Andere Volumes)
- Wechselmedien (dieses Ziel wird für Installationen mit ESDP nicht unterstützt.)
- Optische Laufwerke (dieses Ziel wird für Installationen mit ESDP nicht unterstützt.)

Für jedes Ziel muss eine eigene Richtlinie angelegt werden.



Richtlinieneinstellung	SGE	ESDP	Beschreibung
<b>Verschlüsselungsmodus für Medien</b>	✔	✔ Für diese Einstellung verfügbare Optionen: <ul style="list-style-type: none"> <li>■ <b>Keine Verschlüsselung</b></li> <li>■ <b>Volume-basierend</b></li> </ul> <b>Hinweis:</b> <b>Dateibasierende</b> Einstellungen sind mit ESDP nicht verfügbar.	Dient dem Schutz von Endgeräten (PCs, Notebooks und PDAs) und allen Arten von Wechseldatenträgern. Hauptaufgabe ist die Verschlüsselung aller auf lokalen oder externen Datenträgern gespeicherten Daten. Durch die transparente Arbeitsweise können Benutzer einfach ihre gewohnten Anwendungen, z. B. Microsoft Office, weiter benutzen. Transparente Verschlüsselung bedeutet für den Benutzer, dass alle verschlüsselt gespeicherten Daten (sei es in verschlüsselten Verzeichnissen oder Laufwerken) automatisch im Hauptspeicher entschlüsselt werden, sobald sie in einem Programm geöffnet werden. Beim Abspeichern der Datei wird diese automatisch wieder verschlüsselt.

Richtlinieneinstellung	SGE	ESDP	Beschreibung
			<p>Folgende Optionen stehen zur Verfügung:</p> <ul style="list-style-type: none"> <li>■ <b>Keine Verschlüsselung</b></li> <li>■ <b>Volume-basierend (= transparente, sektorbasierte Verschlüsselung)</b></li> </ul> <p>Stellt sicher, dass alle Daten verschlüsselt sind (inkl. Boot-Dateien, Swapfile, Datei für den Ruhezustand/Hibernation File, temporäre Dateien, Verzeichnisinformationen usw.) ohne dass sich der Benutzer in seiner Arbeitsweise anpassen oder auf Sicherheit achten muss.</p> <p><b>Hinweis:</b> Wenn für ein Volume oder einen Volume-Typ eine Verschlüsselungsrichtlinie existiert und die Verschlüsselung des Volumes schlägt fehl, darf der Benutzer nicht auf das Volume zugreifen.</p> <p><b>Windows 7 System-Partition:</b></p> <p>Für Windows 7 Professional, Enterprise und Ultimate wird auf dem Endpoint-Computer eine System-Partition angelegt, der kein Laufwerksbuchstabe zugeordnet ist. Diese Systempartition kann von Sophos SafeGuard nicht verschlüsselt werden.</p> <p><b>Zugriff auf Unidentified File System Objects:</b></p> <p>Unidentified File System Objects sind Volumes, die von Sophos SafeGuard nicht eindeutig als verschlüsselt oder unverschlüsselt identifiziert werden können. Existiert für ein Unidentified File System Volume eine Verschlüsselungsrichtlinie, so wird der Zugriff auf das Volume verweigert.</p>

Richtlinieneinstellung	SGE	ESDP	Beschreibung
			<p>Existiert keine Verschlüsselungsrichtlinie, so kann der Benutzer auf das Volume zugreifen.</p> <p><b>Hinweis:</b> Existiert für ein Unidentified File System Object eine Verschlüsselungsrichtlinie, bei der die Richtlinieneinstellung Schlüssel für die Verschlüsselung auf eine Option eingestellt ist, die die Schlüsselauswahl ermöglicht (z. B. Beliebiger Schlüssel im Schlüsselring des Benutzers), so entsteht zwischen der Anzeige des Schlüsselauswahldialogs und der Verweigerung des Zugriffs auf das Volume eine zeitliche Lücke. Während dieser Zeit kann auf das Volume zugegriffen werden. So lange der Schlüsselauswahldialog nicht vom Benutzer bestätigt wird, besteht Zugriff auf das Volume. Um dies zu vermeiden, definieren Sie einen vorausgewählten Schlüssel für die Verschlüsselung (siehe Beschreibung der Richtlinieneinstellung <b>Schlüssel für die Verschlüsselung</b>). Diese zeitliche Lücke entsteht auch dann für mit dem Endpoint-Computer verbundene Unidentified File System Objects, wenn der Benutzer zu dem Zeitpunkt, an dem die Verschlüsselungsrichtlinie wirksam wird, bereits Dateien auf dem Volume geöffnet hat oder Autorun aktiviert ist. In diesem Fall, kann nicht gewährleistet werden, dass der Zugriff auf das Volume verweigert wird, da dies zu Datenverlust führen könnte.</p>

Richtlinieneinstellung	SGE	ESDP	Beschreibung
			<p><b>Volumes mit aktivierter Autorun-Funktionalität:</b></p> <p>Ist für ein Volume, für das eine Verschlüsselungsrichtlinie existiert, die Autorun-Funktionalität aktiviert, so können folgende Probleme auftreten:</p> <ul style="list-style-type: none"> <li>■ Das Volume wird nicht verschlüsselt.</li> <li>■ Wenn es sich um ein UFO handelt, wird der Zugriff nicht verweigert.</li> <li>■ <b>Dateibasierend (= transparente, dateibasierte Verschlüsselung (Smart MediaEncryption))</b> Stellt sicher, dass alle Daten verschlüsselt sind (außer Boot Medium und Verzeichnisinformationen), mit dem Vorteil, dass auch optische Medien wie CD/DVD verschlüsselt werden können oder Daten mit Fremdrechnern, auf denen kein SafeGuard installiert ist, ausgetauscht werden können (soweit von der Richtlinie erlaubt).</li> </ul> <p><b>Hinweis:</b> Mit "Dateibasierender Verschlüsselung" verschlüsselte Daten können nicht komprimiert werden. Umgekehrt können auch komprimierte Dateien nicht dateibasierend verschlüsselt werden. Boot-Volumes werden niemals dateibasierend verschlüsselt. Sie sind automatisch von einer dateibasierenden Verschlüsselung ausgenommen, auch wenn eine entsprechende Regel definiert ist.</p>



Richtlinieneinstellung	SGE	ESDP	Beschreibung
<b>ALLGEMEINE EINSTELLUNGEN</b>			
<b>Algorithmus für die Verschlüsselung</b>	✔	✔	Setzt den Verschlüsselungsalgorithmus. Liste aller einsetzbaren Algorithmen mit ihren jeweiligen Standards: AES256: 32 Bytes (256 Bits) AES128: 16 Bytes (128 Bits)
<b>Schlüssel für die Verschlüsselung</b>	✔	✔	Legt fest, welcher Schlüssel zur Verschlüsselung verwendet wird. Für Sophos SafeGuard erfolgt die volume-basierende Verschlüsselung ausschließlich mit einem automatisch erzeugten Computerschlüssel. Für eine dateibasierende Verschlüsselung können nur vom Benutzer erzeugte lokale Schlüssel verwendet werden. Folgende Option steht zur Verfügung: <b>Definierter Computer-Schlüssel:</b> Es wird der Maschinen-Schlüssel verwendet - der Benutzer selbst kann KEINEN Schlüssel auswählen.

Richtlinieneinstellung	SGE	ESDP	Beschreibung
<b>Benutzer darf einen lokalen Schlüssel erzeugen</b>			<p>Diese Einstellung bestimmt, ob der Benutzer auf seinem Computer lokale Schlüssel erzeugen darf oder nicht. Lokale Schlüssel werden auf dem Endpoint-Computer basierend auf einer vom Benutzer eingegebenen Passphrase erzeugt. Die Anforderungen, denen eine Passphrase entsprechen muss, können in Richtlinien vom Typ <b>Passphrase</b> festgelegt werden.</p> <p><b>Hinweis:</b> Da für die dateibasierende Verschlüsselung ausschließlich lokale Schlüssel verwendet werden, darf es einem Benutzer nicht verboten werden, diese Schlüssel zu erzeugen, wenn Richtlinien für eine dateibasierende Verschlüsselung wirksam werden sollen.</p> <p>In der Standardeinstellung (nicht konfiguriert) ist es dem Benutzer erlaubt, lokale Schlüssel anzulegen.</p>
<b>VOLUME-BASIERENDE EINSTELLUNGEN</b>			
<b>Benutzer darf dem verschlüsseltem Volume Schlüssel hinzufügen oder diese entfernen</b>			<p><b>Ja:</b> Sophos SafeGuard Benutzer dürfen einen zusätzlichen Schlüssel aus ihrem Schlüsselbund einfügen/entfernen. Der Dialog wird angezeigt über den Kontextmenüeintrag <b>Verschlüsselung/Registrierkarte Verschlüsselung</b>.</p> <p><b>Nein:</b> Sophos SafeGuard Benutzer dürfen keine zusätzlichen Schlüssel einfügen.</p>

Richtlinieneinstellung	SGE	ESDP	Beschreibung
<b>Reaktion auf unverschlüsselte Volumes</b>	✔	✔	Definiert, wie Sophos SafeGuard mit unverschlüsselten Medien umgeht: Folgende Optionen stehen zur Verfügung: <ul style="list-style-type: none"> <li>■ <b>Abweisen</b> (= Klartext-Medium wird nicht verschlüsselt)</li> <li>■ <b>Nur unverschlüsselte Medien akzeptieren und verschlüsseln</b></li> <li>■ <b>Alle Medien akzeptieren und verschlüsseln</b></li> </ul>
<b>Benutzer darf Volume entschlüsseln</b>	✔	✔	Bewirkt, dass der Sophos SafeGuard Benutzer über einen Kontextmenü-Eintrag im Windows Explorer das Laufwerk entschlüsseln darf.
<b>Schnelle Initialverschlüsselung</b>	✔	✔	Wählen Sie diese Einstellung aus, um den Modus der schnellen Initialverschlüsselung für die volume-basierende Verschlüsselung zu aktivieren. Dieser Modus reduziert den Zeitraum, der für die Initialverschlüsselung auf Endpoint-Computern benötigt wird. <b>Hinweis:</b> Dieser Modus kann zu einem unsicheren Zustand führen. Für weitere Informationen, siehe <a href="#">Schnelle Initialverschlüsselung</a> , Seite 9.
<b>Bei defekten Sektoren fortfahren</b>	✔	✔	Legt fest, ob die Verschlüsselung fortgesetzt oder gestoppt werden soll, wenn defekte Sektoren entdeckt werden. Die Standardeinstellung ist <b>Ja</b> .
<b>DATEIBASIERENDE EINSTELLUNGEN</b>			
<b>Initialverschlüsselung aller Dateien</b>	✔		Bewirkt, dass die Initialverschlüsselung für ein Laufwerk automatisch nach der Benutzeranmeldung gestartet wird. Der Benutzer muss eventuell vorher einen Schlüssel aus dem Schlüsselbund auswählen.

Richtlinieneinstellung	SGE	ESDP	Beschreibung
<b>Benutzer darf Initialverschlüsselung abbrechen</b>	✔		Bewirkt, dass der Benutzer die Initialverschlüsselung abbrechen kann.
<b>Benutzer darf auf unverschlüsselte Dateien zugreifen</b>	✔		Definiert, ob ein Benutzer auf unverschlüsselte Dateien auf einem Laufwerk zugreifen darf.
<b>Benutzer darf Dateien entschlüsseln</b>	✔		Bewirkt, dass der Benutzer einzelne Dateien oder ganze Verzeichnisse entschlüsseln kann (über die Windows Explorer-Erweiterung <rechte Maustaste>).
<b>Benutzer darf eine Medien-Passphrase für Wechselmedien erzeugen</b>	✔		Bewirkt, dass der Benutzer eine Medien-Passphrase auf seinem Computer festlegen kann. Die Medien-Passphrase ermöglicht den einfachen Zugriff auf alle lokalen Schlüssel auf Computern ohne SafeGuard Data Exchange über SafeGuard Portable.
<b>Unberücksichtigte Anwendungen</b>	✔		Erlaubt die Definition von Anwendungen, die vom Sophos SafeGuard Filter-Treiber ignoriert werden sollen und damit von der transparenten Ver-/Entschlüsselung ausgenommen sind. Die einzelnen Anwendungen müssen durch ';' voneinander getrennt werden. Ein Beispiel für eine unberücksichtigte Anwendung kann ein Backup-Programm sein. Damit die Daten beim Erstellen eines Backups nicht entschlüsselt werden, kann diese Anwendung von der Verschlüsselung/Entschlüsselung ausgenommen werden. Die Daten werden verschlüsselt gesichert.





Richtlinieneinstellung	SGE	ESDP	Beschreibung
			<p><b>Hinweis:</b> Da es sich dabei um maschinenspezifische Einstellungen handelt, werden diese erst nach einem Neustart der Benutzer-Computer wirksam</p> <p><b>Unberücksichtigte Anwendungen definieren</b></p> <p>Typische Verwendung: Backup-Programme können als unberücksichtigt definiert werden, damit sie immer die verschlüsselten Daten lesen und sichern.</p> <p>Anwendungen, die bei gleichzeitiger Verwendung mit Sophos SafeGuard Funktionsstörungen auslösen können, aber keine Verschlüsselung erfordern, können generell von der Verschlüsselung ausgenommen werden.</p> <p>Zur Angabe einer unberücksichtigten Anwendung wird der vollständige Name der ausführbaren Datei (optional inklusive Pfadinformation) verwendet.</p> <p><b>Hinweis:</b> Unberücksichtigte Anwendungen können nur global für Lokale Datenträger angegeben werden. Für eine globale Richtlinie vom Typ <b>Geräteschutz</b> muss als Ziel <b>Lokale Datenträger</b> ausgewählt sein. Für alle anderen Ziele wird diese Option nicht angeboten.</p>

Richtlinieneinstellung	SGE	ESDP	Beschreibung
<p><b>Nur für Wechselmedien SafeGuard Portable auf Wechselmedien kopieren</b></p>			<p>Ist diese Option eingeschaltet, wird SafeGuard Portable auf jedes Wechselmedium, das mit dem Endpoint-Computer verbunden wird, kopiert.</p> <p>SafeGuard Portable ermöglicht den verschlüsselten Datenaustausch mit wechselbaren Medien, ohne dass der Empfänger der Daten Sophos SafeGuard installiert haben muss.</p> <p>Der Empfänger kann mit Hilfe von SafeGuard Portable und der entsprechenden Passphrase die verschlüsselten Daten entschlüsseln und auch wieder verschlüsseln. Der Empfänger kann mit SafeGuard Portable die Daten neu verschlüsseln oder den ursprünglich verwendeten Schlüssel für die Verschlüsselung verwenden.</p> <p>SafeGuard Portable muss nicht auf den Computer des Empfängers installiert oder kopiert werden, sondern kann vom wechselbaren Medium verwendet werden.</p>
<p><b>Klartext-Ordner</b></p>			<p>Der hier angegebene Ordner wird auf allen Wechselmedien erstellt. Dateien, die in diesen Ordner kopiert werden, bleiben immer unverschlüsselt.</p>

## 16.7 Spezifische Computereinstellungen - Grundeinstellungen

Richtlinieneinstellung	SGE	ESDP	Erklärung
<b>POWER-ON AUTHENTICATION (POA)</b>			
<b>Power-on Authentication aktivieren</b>	✔	✔	Definiert, ob die POA permanent ein- oder ausgeschaltet sein soll. <b>Hinweis:</b> Aus Sicherheitsgründen empfehlen wir, die POA stets zu eingeschaltet zu lassen. Bei Deaktivierung der POA reduziert sich die Systemsicherheit auf die durch die Windows-Anmeldung gegebene Systemsicherheit. Somit erhöht sich das Risiko des unautorisierten Zugriffs auf verschlüsselte Daten.
<b>Gastbenutzer nicht zulassen</b>	✔	✔	Definiert, ob ein Benutzer zur Windows-Anmeldung zugelassen wird.
<b>Sicheres Wake On LAN (WOL)</b>	✔	✔	Mit der Richtlinie „Sicheres Wake On LAN“ ist es möglich, den Endpoint-Computer für Software-Rollouts optimal vorzubereiten, indem dafür notwendige Parameter wie das temporäre Deaktivieren der POA und ein Zeitintervall für Wake On LAN dem Computer direkt mitgegeben werden können und von ihm ausgewertet werden. Das Rollout-Team kann durch die zur Verfügung gestellten Kommandos ein Scheduling-Skript so gestalten, dass die größtmögliche Sicherheit des Endpoint-Computers trotz deaktivierter POA gewährleistet bleibt. <b>Wir weisen an dieser Stelle ausdrücklich darauf hin, dass auch das zeitlich begrenzte "Ausschalten" der POA für eine bestimmte Anzahl von Boot-Vorgängen ein Absenken des Sicherheitsniveaus bedeutet.</b>




Richtlinieneinstellung	SGE	ESDP	Erklärung
			<p><b>Beispiel:</b> Das SW-Rollout Team informiert den Sophos SafeGuard Sicherheitsbeauftragten (SO) über einen geplanten SW-Roll-out für den 25. September 2010 zwischen 03:00 und 06:00 Uhr. Es sind 2 Neustarts notwendig. Der lokale SW-Rollout Agent muss sich an Windows anmelden können. Der SO erstellt folgende Richtlinie und weist sie den entsprechenden Endpoint-Computern zu.</p> <p><b>Anzahl der automatischen Anmeldungen (0 = kein WOL): 5</b>  <b>Anmeldung an Windows erlaubt während WOL: Ja</b>  <b>Beginn des Zeitfensters für externen WOL Start: 24.Sept. 2010, 12:00</b>  <b>Ende des Zeitfensters für externen WOL Start: 25.Sept. 2010, 06:00</b></p> <p>Bei den automatischen Anmeldungen sieht der SO einen Puffer von 3 vor. Das Zeitintervall setzt der SO auf 12:00 Uhr mittags auf den Tag vor dem SW-Rollout, damit das Scheduling-Skript SGMCMDDIntn.exe rechtzeitig starten kann und WOL spätestens am 25.09 um 03:00 Uhr gestartet ist.</p> <p>Das SW-Rollout-Team erstellt 2 Kommandos für das Scheduling-Skript:</p> <ul style="list-style-type: none"> <li>■ Starte am 24.Sept.2010, 12:15 Uhr SGMCMDDIntn.exe /WOLstart</li> <li>■ Starte am 26.Sept.2010, 09:00 Uhr SGMCMDDIntn.exe /WOLstop</li> </ul> <p>Das SW-Rollout-Skript wird auf den 25.09.2010, 03:00 datiert. Am Ende des Skripts kann WOL explizit wieder deaktiviert werden mit SGMCMDDIntn.exe /WOLstop.</p>

Richtlinieneinstellung	SGE	ESDP	Erklärung
			<p>Alle Endpoint-Computer, die sich bis zum 24.Sept.2010 anmelden und mit den Roll-out Servern in Verbindung treten, erhalten die neue Richtlinie und die Scheduling-Kommandos.</p> <p>Jeder Endpoint-Computer, auf dem der Scheduler zwischen dem 24.Sept. 2010,12:00 Uhr und dem 25.Sept. 2010, 06:00 Uhr das Kommando SGMCMDDIntn / WOLstart auslöst, fällt in das obige WOL-Zeitintervall und aktiviert demzufolge Wake On LAN.</p>
<b>Anzahl der automatischen Anmeldungen</b>			<p>Definiert die Anzahl der Neustarts mit ausgeschalteter Power-on Authentication für Wake On LAN.</p> <p>Diese Einstellung überschreibt temporär die Einstellung von <b>Power-on Authentication aktivieren</b>, bis die Anzahl der eingestellten automatischen Anmeldungen erreicht ist. Danach wird die Power-on Authentication wieder aktiviert. Beispiel: Die Zahl der automatischen Anmeldungen ist auf "2" gesetzt, "Power-on Authentication aktivieren" ist eingeschaltet. Der Computer bootet zweimal ohne eine Authentisierung in der POA zu verlangen.</p> <p>Wir empfehlen, für Wake On LAN, immer <b>drei Neustarts mehr als notwendig</b> zu erlauben, um unvorhergesehene Probleme zu umgehen.</p>
<b>Anmeldung an Windows währendWOL erlaubt</b>			<p>Legt fest, ob während eines Wake On LAN ein Logon an Windows erlaubt ist, z. B. für ein SW-Update. Diese Einstellung wird von der POA ausgewertet.</p>

Richtlinieneinstellung	SGE	ESDP	Erklärung
<b>Beginn des Zeitfensters für externen WOL Start</b> <b>Ende des Zeitfensters für externen WOL Start</b>	✔	✔	<p>Datum und Uhrzeit für den Beginn und das Ende des Wake On LAN (WOL) können ausgewählt oder eingegeben werden.</p> <p>Datumsformat: <i>MM/TT/JJJJ</i> Zeitformat: <i>HH:MM</i></p> <p>Folgende Eingabekombinationen sind möglich:</p> <ul style="list-style-type: none"> <li>■ Beginn und Ende des WOL werden festgelegt.</li> <li>■ Nur das Ende des WOL wird festgelegt, der Beginn bleibt offen.</li> <li>■ Keine Eingaben: es wird kein Zeitintervall für den Client festgelegt.</li> </ul> <p>Bei einem geplanten SW-Roll-out sollte der SO den Zeitrahmen für WOL so bemessen, dass das Scheduling-Skript früh genug starten und allen Endpoint-Computern genügend Zeit zum Booten bleibt.</p> <p>WOLstart: Der Startpunkt für den WOL im Scheduling-Skript muss innerhalb des hier in der Richtlinie festgelegten Zeitintervalls liegen. Wenn kein Intervall definiert ist, so wird WOL lokal am Endpoint-Computer nicht aktiviert.</p> <p>WOLstop: Dieses Kommando wird unabhängig vom hier festgelegten Endpunkt des WOL ausgeführt.</p>
<b>ANZEIGEOPTIONEN</b>			
<b>Computer-Identifikation anzeigen</b>	✔	✔	<p>Zeigt in der Titelleiste der POA entweder den Computernamen oder einen frei definierbaren Text an.</p> <p>Existiert ein Maschinename in den Windows-Netzwerkeinstellungen, wird dieser in der Grundeinstellung automatisch übernommen.</p>

Richtlinieneinstellung	SGE	ESDP	Erklärung
<b>Text für Computer-Identifikation</b>	✔	✔	Der Text, der in der Titelleiste der POA angezeigt werden soll. Ist unter <b>Computer-Identifikation anzeigen</b> die Option <b>Definierter Name</b> ausgewählt, können Sie in diesem Eingabefeld den Text eingeben.
<b>Rechtliche Hinweise anzeigen</b>	✔	✔	Zeigt eine Textbox mit frei konfigurierbarem Inhalt an, die vor der Anmeldung in der POA erscheint. In manchen Ländern ist das Erscheinen eines Textfeldes mit bestimmtem Inhalt gesetzlich vorgeschrieben. Die Box muss vom Benutzer bestätigt werden, bevor das System fortfährt. Bevor Sie einen Text angeben können, muss dieser als Textelement im <b>Richtlinien-Navigationsbereich</b> unter <b>Informationstext</b> registriert werden.
<b>Text für rechtliche Hinweise</b>	✔	✔	Text, der als rechtlicher Hinweis angezeigt werden soll. Sie können hier ein Textelement auswählen, das im <b>Richtlinien-Navigationsbereich</b> unter <b>Informationstext</b> registriert wurde.
<b>Zusätzliche Informationsanzeigen</b>	✔	✔	Zeigt eine Textbox mit frei konfigurierbarem Inhalt an, die nach den rechtlichen Hinweisen (wenn diese aktiviert sind) erscheint. Sie können festlegen ob die zusätzlichen Informationen <ul style="list-style-type: none"> <li>■ <b>Nie</b></li> <li>■ <b>Bei jedem Systemstart</b></li> <li>■ <b>Bei jeder Anmeldung</b></li> </ul> angezeigt werden.

Richtlinieneinstellung	SGE	ESDP	Erklärung
<b>Text für zusätzliche Informationen</b>	✔	✔	Text, der als zusätzliche Information angezeigt werden soll. Sie können hier ein Textelement auswählen, das im <b>Richtlinien-Navigationsbereich</b> unter <b>Informationstext</b> registriert wurde.
<b>Anzeigedauer (in Sekunden)</b>	✔	✔	Zeitraum (in Sekunden) für die Anzeige zusätzlicher Informationen. Sie können hier die Anzahl der Sekunden eingeben, nach denen die Textbox für zusätzliche Informationen automatisch geschlossen wird. Der Benutzer kann die Textbox jederzeit durch Klicken auf <b>OK</b> schließen.
<b>System Tray Icon aktivieren und anzeigen</b>	✔	✔	Über das Sophos SafeGuard System Tray Icon kann auf dem Endpoint-Computer einfach und schnell auf alle Benutzerfunktionen zugegriffen werden. Zusätzlich können für den Benutzer Informationen über den Status des Endpoint-Computers (neue Richtlinien erhalten, ...) über Balloon Tool Tips ausgegeben werden. <b>Ja:</b> System Tray Icon wird im Infobereich der Taskleiste angezeigt, der Benutzer wird über Balloon Tool Tips laufend über den Status von Sophos SafeGuard informiert. <b>Nein:</b> <b>Stumm:</b> System Tray Icon wird im Infobereich der Taskleiste angezeigt, es werden aber keine Statusinformationen für den Benutzer über Balloon Tool Tips ausgegeben.
<b>Overlay-Symbole im Explorer anzeigen</b>	✔	✔	Bestimmt, ob im Windows Explorer Schlüssel-Symbole zur Anzeige des Verschlüsselungsstatus von Volumes, Geräten, Ordnern und Dateien angezeigt werden.

Richtlinieneinstellung	SGE	ESDP	Erklärung
<b>Virtuelle Tastatur in der POA</b>			Bestimmt, ob im POA-Anmeldedialog bei Bedarf eine virtuelle Tastatur zur Eingabe des Kennworts angezeigt werden kann.
<b>INSTALLATIONSOPTIONEN</b>			
<b>Deinstallation erlaubt</b>			Bestimmt, ob die Deinstallation von Sophos SafeGuard auf den Endpoint-Computern möglich ist. Wird <b>Deinstallation erlaubt</b> auf <b>Nein</b> gesetzt, kann Sophos SafeGuard solange eine Richtlinie mit dieser Einstellung wirksam ist, auch mit Administratorrechten nicht deinstalliert werden.
<b>Sophos Manipulationsschutz aktivieren</b>			<p>Aktiviert/deaktiviert die Funktion Sophos Manipulationsschutz. Wenn Sie die Deinstallation über die Richtlinieneinstellung <b>Deinstallation erlaubt</b> als zulässig definiert haben, können Sie diese Richtlinieneinstellung auf <b>Ja</b> setzen, um Deinstallationsvorgänge durch die Funktion Sophos Manipulationsschutz überprüfen zu lassen und somit ein leichtfertiges Entfernen der Software zu verhindern.</p> <p>Erlaubt die Funktion Sophos Manipulationsschutz die Deinstallation von Sophos SafeGuard nicht, wird der Deinstallationsvorgang abgebrochen.</p> <p>Ist <b>Sophos Manipulationsschutz aktivieren</b> auf <b>Nein</b> eingestellt, werden Deinstallationsvorgänge durch die Funktion Sophos Manipulationsschutz weder geprüft noch verhindert.</p> <p><b>Hinweis:</b> Diese Einstellung gilt nur für Endpoint-Computer, auf denen Sophos Endpoint Security and Control in der Version 9.5 oder einer neueren Version installiert ist.</p>

## 16.8 Protokollierung

Ereignisse für Sophos SafeGuard werden in der Windows-Ereignisanzeige protokolliert. Um festzulegen, welche Ereignisse in der Windows-Ereignisanzeige protokolliert werden sollen, erstellen Sie eine Richtlinie vom Typ **Protokollierung** und wählen Sie die gewünschten Ereignisse per Mausklick aus.

Es steht eine Vielzahl von Ereignissen aus unterschiedlichen Kategorien (z. B. Anmeldung, Verschlüsselung usw.) zur Auswahl zur Verfügung. Es ist daher empfehlenswert, eine Vorgehensweise für die Protokollierung zu definieren und die notwendigen Ereignisse unter Berücksichtigung der Anforderungen für Berichte und Audits festzulegen.

## 17 SafeGuard Data Exchange

**Hinweis:** SafeGuard Data Exchange und SafeGuard Portable werden mit ESDP (Endpoint Security and Data Protection) nicht unterstützt.

Mit SafeGuard Data Exchange lassen sich Daten, die auf mit Sophos SafeGuard Endpoint-Computern verbundenen Wechselmedien gespeichert werden, verschlüsseln und mit anderen Benutzern austauschen. Alle Ver- und Entschlüsselungsprozesse laufen transparent und mit minimaler Benutzerinteraktion ab.

Nur Benutzer, die über die entsprechenden Schlüssel verfügen, können den Inhalt der verschlüsselten Daten lesen. Alle nachfolgenden Verschlüsselungsprozesse laufen transparent.

Als Sicherheitsbeauftragter legen Sie die spezifischen Einstellungen in einer Richtlinie vom Typ **Geräteschutz** mit **Ziel des Geräteschutzes: Wechselmedien** fest.

### 17.1 Lokale Schlüssel

SafeGuard Data Exchange unterstützt die Verschlüsselung mit lokalen Schlüsseln. Lokale Schlüssel werden auf dem Endpoint-Computer erzeugt und können zur Verschlüsselung von Wechselmedien benutzt werden. Die Schlüssel werden durch Eingabe einer Passphrase erstellt.

**Hinweis:** SafeGuard Data Exchange ist mit ESDP (Endpoint Security and Data Protection) nicht verfügbar.

Werden lokale Schlüssel zum Verschlüsseln von Dateien auf Wechselmedien verwendet, lassen sich diese Dateien auf einem Computer ohne SafeGuard Data Exchange mit SafeGuard Portable entschlüsseln. Beim Öffnen der Dateien mit SafeGuard Portable wird der Benutzer dazu aufgefordert, die Passphrase einzugeben, die beim Erzeugen des Schlüssels angegeben wurde. Wenn dem Benutzer die Passphrase bekannt ist, kann er die Datei öffnen.

Mit SafeGuard Portable erhält jeder Benutzer, der die entsprechende Passphrase kennt, Zugang zu verschlüsselten Dateien auf Wechselmedien. Auf diese Weise ist ein Austausch von verschlüsselten Daten mit Partnern, die nicht über Sophos SafeGuard verfügen, möglich. Sie benötigen lediglich SafeGuard Portable sowie die Passphrase für die Dateien, auf die sie zugreifen sollen.

Durch Verwendung von verschiedenen lokalen Schlüsseln für die Verschlüsselung von Dateien auf Wechselmedien lässt sich der Zugang zu den Dateien sogar selektiv einschränken. Zum Beispiel: Sie verschlüsseln die Dateien auf einem USB-Stick mit einem Schlüssel mit der Passphrase `my_localkey`. Für eine einzelne Datei mit dem Dateinamen `Partner.doc` verwenden Sie die Passphrase `partner_lokalerSchlüssel`.

Wenn Sie den USB-Stick nun an einen Partner weitergeben und ihm die Passphrase `partner_lokaler` Schlüssel mitteilen, hat dieser nur Zugriff auf die Datei `FürPartner.doc`.

**Hinweis:** Standardmäßig wird SafeGuard Portable automatisch auf alle mit dem System verbundenen Wechselmedien kopiert. Um SafeGuard Portable nicht automatisch auf die Wechselmedien zu kopieren, deaktivieren Sie die Option **SafeGuard Portable auf Wechselmedien kopieren** in einer Richtlinie vom Typ **Geräteschutz**.

## 17.2 Medien-Passphrase

SafeGuard Data Exchange ermöglicht es Ihnen auch festzulegen, dass eine einzige Medien-Passphrase für alle Wechselmedien - mit Ausnahme von optischen Medien - auf den Endpoint-Computern erstellt werden muss. Die Medien-Passphrase ermöglicht den Zugriff auf alle in SafeGuard Portable verwendeten lokalen Schlüssel. Der Benutzer muss nur eine einzige Passphrase eingeben und erhält Zugriff auf alle verschlüsselten Dateien in SafeGuard Portable. Dabei spielt es keine Rolle, welcher lokale Schlüssel für die Verschlüsselung verwendet wurde.

Auf jedem Endpoint-Computer wird automatisch ein einzigartiger Medienverschlüsselungsschlüssel für die Datenverschlüsselung für jedes Medium erstellt. Dieser Schlüssel ist durch die Medien-Passphrase gesichert. Auf einem Computer mit SafeGuard Data Exchange ist es daher nicht notwendig, die Medien-Passphrase einzugeben, um auf die verschlüsselten Dateien auf Wechselmedien zuzugreifen. Der Zugriff wird automatisch gewährt, wenn sich der entsprechende Schlüssel im Schlüsselring des Benutzers befindet.

Die Medien-Passphrase-Funktionalität steht zur Verfügung, wenn die Option **Benutzer darf eine Medien-Passphrase für Wechselmedien erzeugen** in einer Richtlinie vom Typ **Geräteschutz** aktiviert ist.

Nach dem Wirksamwerden dieser Einstellung auf dem Computer wird der Benutzer automatisch aufgefordert, eine Medien-Passphrase einzugeben, wenn er zum ersten Mal Wechselmedien mit dem Computer verbindet. Der Benutzer kann die Medien-Passphrase auch ändern. In diesem Fall findet automatisch eine Synchronisierung statt, wenn die Medien-Passphrase auf dem Computer und die Medien-Passphrase der Wechselmedien nicht mehr synchron sind.

Sollte der Benutzer die Medien-Passphrase vergessen, so kann er diese ohne Helpdesk-Unterstützung wiederherstellen.

**Hinweis:** Um die Medien-Passphrase zu aktivieren, aktivieren Sie die Option **Benutzer darf eine Medien-Passphrase für Wechselmedien erzeugen** in einer Richtlinie vom Typ **Geräteschutz**.

Auf einem durch Sophos SafeGuard geschützten Computer ohne aktivierte Medien-Passphrase-Funktionalität stehen nach der Installation keine Schlüssel zur Verfügung, da Sophos SafeGuard Endpoint-Computer nur lokale Schlüssel verwenden. Vor der Benutzung der Verschlüsselung muss der Benutzer einen Schlüssel erzeugen.

Ist die Medien-Passphrase-Funktionalität in einer Wechselmedienrichtlinie für Endpoint-Computer aktiviert, so wird der Medienverschlüsselungsschlüssel automatisch auf dem Endpoint-Computer erzeugt und kann direkt nach Abschluss der Installation für die Verschlüsselung verwendet werden. Der Schlüssel steht als „vordefinierter“ Schlüssel im Schlüsselring des Benutzers zur Verfügung und wird in Dialogen als <user name> für die Schlüsselauswahl angezeigt.

Falls verfügbar, werden die Medienverschlüsselungsschlüssel auch für alle initialen Verschlüsselungsvorgänge verwendet.

## 18 Die Power-on Authentication (POA)

Sophos SafeGuard identifiziert den Benutzer bereits, bevor das Betriebssystem startet. Hierbei startet vorher ein Sophos SafeGuard eigener Systemkern, der gegen Modifikationen geschützt und versteckt auf der Festplatte gespeichert ist. Erst wenn sich der Benutzer in der POA korrekt authentisiert hat, wird das eigentliche Betriebssystem (Windows) von der verschlüsselten Partition gestartet und der Benutzer später automatisch an Windows angemeldet. Analog wird verfahren, wenn der Endpoint-Computer aus dem Ruhezustand (Hibernation (Suspend to Disk)) wieder eingeschaltet wird.



Die Sophos SafeGuard Power-on Authentication bietet unter anderem folgende Vorteile:

- Grafische Benutzeroberfläche, mit Mausunterstützung und verschiebbaren Fenstern, und damit einfache, übersichtliche Bedienung.
- Vom Firmenkunden per Richtlinie anpassbares grafisches Layout (Hintergrundbild, Anmeldebild, Willkommensmeldung etc.).
- Unterstützung von Windows-Benutzerkonten und Kennwörtern bereits zum Pre-Boot Zeitpunkt, keine separaten Zugangsdaten mehr, die sich der Benutzer merken muss.
- Unterstützung von Unicode und damit auch fremdsprachigen Kennwörtern bzw. Benutzeroberflächen.

### 18.1 Anmeldeverzögerung

Auf einem durch Sophos SafeGuard geschützten Computer wird eine Anmeldeverzögerung ausgelöst, wenn ein Benutzer während der Anmeldung an Windows oder an die Power-on Authentication falsche Anmeldeinformationen eingibt. Mit jedem fehlgeschlagenen Anmeldeversuch verlängert sich jeweils die Anmeldeverzögerung. Nach einer fehlgeschlagenen Anmeldung erscheint ein Dialog, der die verbleibende Verzögerungszeit anzeigt.

Sie können die Anzahl an erlaubten Anmeldeversuchen in einer Richtlinie vom Typ **Authentisierung** über die Option **Maximalanzahl von erfolglosen Anmeldeversuchen** festlegen.

## 18.2 Computersperre

In einer Richtlinie vom Typ **Authentisierung** können Sie außerdem festlegen, dass der Computer nach der eingestellten Anzahl an fehlgeschlagenen Anmeldeversuchen gesperrt wird. Wählen Sie hierzu bei der Option **Computer sperren** die Einstellung **Ja**. Um eine Computersperre aufzuheben, kann der Benutzer ein Challenge/Response-Verfahren starten.

## 18.3 Power-on Authentication konfigurieren

Der POA-Dialog besteht aus folgenden Komponenten:

- Anmeldebild
- Dialogtexte
- Sprache des Tastaturlayouts



Das Erscheinungsbild des POA-Dialogs können Sie u. a. über Richtlinieneinstellungen im SafeGuard Policy Editor an Ihre jeweiligen Anforderungen anpassen.

### 18.3.1 Hintergrund- und Anmeldebild

In der Standardeinstellung werden Bilder im SafeGuard-Design als Hintergrund- und Anmeldebild angezeigt. Es ist jedoch möglich, andere Bilder anzuzeigen, z. B. das Firmenlogo.

Hintergrund- und Anmeldebilder werden über eine Richtlinie vom Typ **Allgemeine Einstellungen** festgelegt.

Hintergrund- und Anmeldebilder müssen bestimmten Anforderungen entsprechen, damit sie in Sophos SafeGuard verwendet werden können:

#### **Hintergrundbild in der POA**

Maximale Dateigröße für alle Hintergrundbilder: **500 KB**

Sophos SafeGuard unterstützt für Hintergrundbilder zwei Varianten:

- **1024x768** (VESA-Modus)

Farben: keine Einschränkung

Option im Richtlinientyp **Allgemeine Einstellungen: Hintergrundbild in der POA**

- **640x480** (VGA-Modus)

Farben: 16

Option im Richtlinientyp **Allgemeine Einstellungen: Hintergrundbild in der POA (niedrige Auflösung)**

#### **Anmeldebild in der POA**

Maximale Dateigröße für alle Anmeldebilder: **100 KB**

Sophos SafeGuard unterstützt für Anmeldebilder zwei Varianten:

- **413x140**

Farben: keine Einschränkung

Option im Richtlinientyp **Allgemeine Einstellungen: Anmeldebild in der POA**

- **413x140**

Farben: 16

Option im Richtlinientyp **Allgemeine Einstellungen: Anmeldebild in der POA (niedrige Auflösung)**

Bilder, Informationstexte und Listen müssen zunächst als Dateien (BMP, PNG, JPG oder Textdateien) erstellt werden und können dann im Navigationsbereich registriert werden.

### 18.3.1.1 Bilder registrieren

So registrieren Sie Bilder:

1. Klicken Sie im **Richtlinien** Navigationsbereich mit der rechten Maustaste auf **Bilder** und wählen Sie **Neu > Bild**.
2. Geben Sie unter **Bildname** einen Namen für das Bild ein.
3. Wählen Sie über die Schaltfläche [...] das zuvor erstellte Bild aus.
4. Klicken Sie auf **OK**.

Das neue Bild wird als Unterknoten des Eintrags **Bilder** im Richtlinien-Navigationsbereich angezeigt. Ist ein Bild markiert, wird es im Aktionsbereich angezeigt. Das Bild kann jetzt beim Erstellen von Richtlinien ausgewählt werden.

Sie können so weitere Bilder registrieren. Alle registrierten Bilder werden als Unterknoten angezeigt.

**Hinweis:** Mit der Schaltfläche **Bild ändern** können Sie das zugeordnete Bild austauschen. Es wird ein Dialog geöffnet, in dem ein anderes Bild ausgewählt werden kann.

### 18.3.2 Benutzerdefinierter Text in der POA

Sie können in der POA folgende **benutzerdefinierte Informationstexte** anzeigen lassen:

- Infotext beim Starten eines Challenge/Response-Verfahrens zur Hilfe bei der Anmeldung (z. B.: "Bitte rufen Sie Ihren Support unter der Telefonnummer 01234-56789 an.").

Option im Richtlinientyp **Allgemeine Einstellungen: Informationstext**

- Rechtliche Hinweise nach der Anmeldung an der POA

Option im Richtlinientyp **Spezifische Computereinstellungen: Text für rechtliche Hinweise**

- Text für zusätzliche Informationen nach der Anmeldung an der POA

Option im Richtlinientyp **Spezifische Computereinstellungen: Text für zusätzliche Informationen**

### 18.3.2.1 Informationstexte registrieren

Die Textdateien mit den gewünschten Informationen müssen erstellt werden, bevor sie im SafeGuard Policy Editor registriert werden können. Die maximale Dateigröße für Informationstexte beträgt **50 KB**. Sophos SafeGuard verwendet nur Unicode UTF-16 kodierte Texte. Wenn Sie die Textdateien nicht in diesem Format erstellen, werden Sie bei der Registrierung automatisch in dieses Format konvertiert.

Wenn eine Konvertierung durchgeführt wird, werden Sie durch eine Meldung darüber informiert.

So registrieren Sie die Textdateien:

1. Klicken Sie im **Richtlinien** Navigationsbereich mit der rechten Maustaste auf **Informationstext** und wählen Sie **Neu > Text**.
2. Geben Sie unter **Textelementname** einen Namen für den anzuzeigenden Text ein.
3. Wählen Sie über die Schaltfläche [...] die zuvor erstellte Textdatei aus. Wenn eine Konvertierung notwendig ist, wird eine entsprechende Meldung angezeigt.
4. Klicken Sie auf **OK**.

Das neue Textelement wird als Unterknoten des Eintrags **Informationstext** im Richtlinien-Navigationsbereich angezeigt. Ist ein Textelement markiert, wird sein Inhalt im Aktionsbereich angezeigt. Das Textelement kann jetzt beim Erstellen von Richtlinien ausgewählt werden.

Sie können weitere Textelemente registrieren. Alle registrierten Textelemente werden als Unterknoten angezeigt.

**Hinweis:** Mit der Schaltfläche **Text ändern** können Sie weiteren Text zum bestehenden Text hinzufügen. Es wird ein Dialog geöffnet, in dem eine weitere Textdatei ausgewählt werden kann. Der in dieser Datei enthaltene Text wird am Ende des bestehenden Texts eingefügt.

### 18.3.3 Sprache der POA-Dialogtexte

Alle Texte in der POA werden nach der Installation der Sophos SafeGuard Verschlüsselungs-Software mit den Standardeinstellungen in der Sprache angezeigt, die bei der Installation von Sophos SafeGuard in den Regions- und Sprachoptionen von Windows als Standardsprache am Endpoint-Computer eingestellt ist.

Nach der Installation kann die Sprache in der POA nur über eine im SafeGuard Policy Editor angelegte Richtlinie geändert werden. Das Ändern der Standardsprache unter Windows bewirkt keine Änderung der Sprache in der POA.

Die Sprache in der POA wird über eine Richtlinie vom Typ **Allgemeine Einstellungen** (Option **Sprache am Client**) festgelegt.

### 18.3.4 Tastaturlayout

Beinahe jedes Land hat ein eigenes Tastaturlayout, d. h. die Tastenbelegung ist unterschiedlich. In der POA macht sich bei der Eingabe von Benutzernamen, Kennwort und Response Code bemerkbar.

Sophos SafeGuard übernimmt als Standard das Tastaturlayout in die POA, das zum Zeitpunkt der Installation in den Regions- und Sprachoptionen von Windows gesetzt ist. Ist unter Windows „Deutsch“ als Tastaturlayout gesetzt, wird in der POA das deutsche Tastaturlayout verwendet.

Die Sprache des verwendeten Tastaturlayouts wird in der POA angezeigt, z. B. „EN“ für Englisch. Neben dem Standard-Tastaturlayout kann das US-Tastaturlayout (Englisch) gewählt werden.

Es gibt bestimmte Ausnahmefälle:

- Das Tastaturlayout wird zwar unterstützt, aufgrund fehlender Schriften (z. B. bei Bulgarisch) werden im Feld **Benutzername** aber nur Sonderzeichen angezeigt.
- Es ist kein spezielles Tastaturlayout verfügbar (z. B. Dominikanische Republik). In solchen Fällen greift die POA auf das Original-Tastaturlayout zurück. Für die Dominikanische Republik ist dies „Spanisch“.

**Hinweis:** Alle nicht unterstützten Tastaturlayouts verwenden als Standard das US-Tastaturlayout. Das bedeutet, dass auch nur Zeichen erkannt und eingegeben werden können, die im US-Tastaturlayout unterstützt werden. Benutzer können sich demnach nur an der POA anmelden, wenn ihre Benutzernamen und Kennwörter sich aus Zeichen zusammensetzen, die vom US-Tastaturlayout oder dem entsprechenden Original-Layout unterstützt werden.

#### 18.3.4.1 Virtuelle Tastatur

Sophos SafeGuard bietet die Möglichkeit, in der POA eine virtuelle Tastatur anzeigen zu lassen. Der Benutzer kann dann z. B. Anmeldeinformationen durch Klick auf die am Bildschirm angezeigten Tasten eingeben.

Als Sicherheitsbeauftragter können Sie die Anzeige der virtuellen Tastatur in einer Richtlinie vom Typ **Spezifische Computereinstellungen** über die Option **Virtuelle Tastatur** aktivieren/deaktivieren.

Die Unterstützung der virtuellen Tastatur muss über eine Richtlinieneinstellung aktiviert/deaktiviert werden.

Für die virtuelle Tastatur werden verschiedene Layouts angeboten und das Layout kann mit den gleichen Einstellungen wie das normale Tastaturlayout geändert werden.

### 18.3.4.2 Tastaturlayout ändern

Das normale wie das virtuelle Tastaturlayout der Power-on Authentication kann nachträglich geändert werden.

So ändern Sie die Sprache des Tastaturlayouts:

1. Wählen Sie **Start > Systemsteuerung > Regions- und Sprachoptionen**.
2. Wählen Sie auf der Registerkarte **Regionale Einstellungen** die gewünschte Sprache aus.
3. Aktivieren Sie dann auf der Registerkarte **Erweitert** unter **Standardeinstellungen für Benutzerkonten** die Option **Alle Einstellungen auf das aktuelle Benutzerkonto und Standardbenutzerprofil anwenden**.
4. Bestätigen Sie die vorgenommenen Einstellungen mit **OK**.

Die POA merkt sich das bei der letzten erfolgreichen Anmeldung verwendete Tastaturlayout und aktiviert dieses beim nächsten Anmelden automatisch. Wenn dieses gemerkte Tastaturlayout über die **Regions- und Sprachoptionen** abgewählt wird, bleibt es dem Anwender noch so lange erhalten, bis er eine andere Sprache ausgewählt hat.

Falls die gewünschte Sprache nicht im System vorhanden ist, werden Sie von Windows evtl. aufgefordert, die Sprache zu installieren. Danach müssen Sie den Computer zweimal neu starten, damit das neue Tastaturlayout von der Power-on Authentication eingelesen werden und dann auch über diese eingestellt werden kann.

Sie können das gewünschte Tastaturlayout der Power-on Authentication mit der Maus oder mit der Tastatur (**Alt+Shift**) ändern.

Sie können über **Start > Ausführen > regedit > HKEY\_USERS\DEFAULT\Keyboard Layout\Preload** einsehen, welche Sprachen auf dem System installiert und damit verfügbar sind.

## 18.4 In der Power-on Authentication unterstützte Hotkeys

Bestimmte Hardware-Einstellungen und -Funktionalitäten können Probleme beim Booten des Endpoint-Computers verursachen, die dazu führen, dass der Rechner im Startvorgang hängen bleibt. Die Power-on Authentication unterstützt eine Reihe von Hotkeys, mit denen sich Hardware-Einstellungen modifizieren und Funktionalitäten modifizieren lassen. Darüber hinaus sind in die auf dem Computer zu installierenden .MSI-Datei Grey Lists und Black Lists integriert, die Funktionen abdecken, von denen ein solches Problemverhalten bekannt ist.

Wir empfehlen, vor jeder größer angelegten Sophos SafeGuard Installation die aktuelle Version der POA-Konfigurationsdatei zu installieren. Die Datei wird monatlich aktualisiert und steht hier zum Download zur Verfügung:

`ftp://POACFG:POACFG@ftp.ou.utimaco.de`

Sie können diese Datei gemäß der Hardware einer bestimmten Umgebung anpassen.

**Hinweis:** Wenn Sie eine angepasste Datei definieren, wird nur diese verwendet, nicht die in der .msi-Datei integrierte Datei. Die Standarddatei wird nur dann verwendet, wenn keine POA-Konfigurationsdatei definiert ist oder gefunden wird.

Um die POA-Konfigurationsdatei zu installieren, geben Sie folgenden Befehl ein:

```
MSIEXEC /i <Client-MSI-Paket> POACFG=<Pfad der POA-Konfigurationsdatei>
```

Weitere Informationen finden Sie in unserer Wissensdatenbank: <http://www.sophos.com/support/knowledgebase/article/65700.html>

**Die folgenden Hotkeys werden in der POA unterstützt:**

- **Shift F3** = USB Legacy Unterstützung (Aus/An)
- **Shift F4** = VESA Grafikmodus (Aus/An)
- **Shift F5** = USB 1.x und 2.0 Unterstützung (Aus/An)
- **Shift F6** = ATA Controller (Aus/An))
- **Shift F7** = nur USB 2.0 Unterstützung (Aus/An)

USB 1.x Unterstützung bleibt wie über Shift F5 gesetzt.

- **Shift F9** = ACPI/APIC (Aus/An)

### USB Hotkeys Abhängigkeitsmatrix

Shift F3	Shift F5	Shift F7	Legacy	USB 1.x	USB 2.0	Comment
aus	aus	aus	an	an	an	3.
an	aus	aus	aus	an	an	Standard
aus	an	aus	an	aus	aus	1., 2.
an	an	aus	an	aus	aus	1., 2.
aus	aus	an	an	an	aus	3.
an	aus	an	aus	an	aus	
aus	an	an	an	aus	aus	
an	an	an	an	aus	aus	2.

1. Shift F5 deaktiviert sowohl die Unterstützung von USB 1.x als auch von USB 2.0.

**Hinweis:** Durch Drücken von Shift F5 reduziert sich die Wartezeit bis zum Starten der POA erheblich. Beachten Sie jedoch, dass bei Benutzung einer USB-Tastatur oder einer USB-Maus am betreffenden Computer diese Geräte durch Drücken von Shift F5 möglicherweise deaktiviert werden.

2. Wenn die USB-Unterstützung nicht aktiviert ist, versucht die POA, BIOS SMM zu benutzen anstatt den USB-Controller zu sichern und wiederherzustellen. Der Legacy-Modus kann in diesem Szenario funktionieren.
3. Die Legacy-Unterstützung ist aktiviert, die USB-Unterstützung ist aktiviert. Die POA versucht, den USB-Controller zu sichern und wiederherzustellen. Der Computer kann sich je nach eingesetzter BIOS-Version aufhängen.

Es besteht die Möglichkeit, Änderungen, die über Hotkeys vorgenommen werden können, bei der Installation der Sophos SafeGuard Verschlüsselungs-Software über eine mst Datei bereits vorzudefinieren. Verwenden Sie dazu den entsprechenden Aufruf in Verbindung mit msiexec.

NOVESA	Definiert, ob VESA oder VGA Modus verwendet werden. 0 = VESA Modus (Standard), 1 = VGA Modus
NOLEGACY	Definiert, ob nach der POA-Anmeldung Legacy-Unterstützung aktiviert ist. 0 = Legacy Support aktiviert, 1 = kein Legacy Support (Standard)
ALTERNATE:	Definiert, ob USB Geräte von der POA unterstützt werden. 0 = USB-Unterstützung ist aktiviert (Standard), 1 = keine USB-Unterstützung
NOATA	Definiert, ob der Int13 Gerätetreiber verwendet wird. 0 = Standard ATA Gerätetreiber (Standard), 1 = Int13 Gerätetreiber

ACPIAPIC	Definiert, ob die ACPI/APIC-Unterstützung benutzt wird. 0 = Keine ACPI/APIC-Unterstützung, 1 = ACPI/APIC-Unterstützung ist aktiv.
NOVESA	Definiert, ob VESA oder VGA-Modus verwendet wird. 0 = VESA-Modus (Standard), 1 = VGA-Modus

## **18.5 Deaktivierte POA und Lenovo Rescue and Recovery**

Sollte auf dem Computer die Power-on Authentication deaktiviert sein, so sollte zum Schutz vor dem Zugriff auf verschlüsselte Dateien aus der Rescue and Recovery Umgebung heraus die Rescue and Recovery Authentisierung eingeschaltet sein.

Detaillierte Informationen zur Aktivierung der Rescue and Recovery Authentisierung finden Sie in der Lenovo Rescue and Recovery Dokumentation.

## 19 Recovery-Optionen

Sophos SafeGuard bietet verschiedene Recovery-Optionen, die auf unterschiedliche Szenarien zugeschnitten sind:

### ■ Recovery für die Anmeldung über Local Self Help

Mit Local Self Help können sich Benutzer, die ihr Kennwort vergessen haben, ohne Unterstützung eines Helpdesks wieder an Ihrem Computer anmelden. So erhalten Benutzer auch in Situationen, in denen sie keine Telefon- oder Netzwerkverbindung und somit auch kein Challenge/Response-Verfahren nutzen können (z. B. an Bord eines Flugzeugs), wieder Zugang zu ihrem Computer. Um sich anzumelden, müssen sie lediglich eine bestimmte Anzahl an vordefinierten Fragen in der Power-on Authentication beantworten.

Local Self Help reduziert die Anzahl an Helpdesk-Anforderungen für Recovery-Vorgänge, die die Anmeldung betreffen. Helpdesk-Mitarbeitern werden somit Routine-Aufgaben abgenommen und sie können sich auf komplexere Support-Anforderungen konzentrieren.

Für detaillierte Informationen, siehe [Recovery über Local Self Help](#), Seite 133.

### ■ Recovery über Challenge/Response

Das Challenge/Response-Verfahren ist ein sicheres und effizientes Recovery-System, das Benutzer unterstützt, die sich nicht mehr an ihrem Computer anmelden oder nicht mehr auf verschlüsselte Daten zugreifen können. Während eines Challenge/Response-Verfahrens übermittelt der Benutzer einen auf dem Endpoint-Computer erzeugten Challenge-Code an den Helpdesk-Beauftragten. Dieser erzeugt auf der Grundlage des Challenge-Codes einen Response-Code, der den Benutzer zum Ausführen einer bestimmten Aktion auf dem Computer berechtigt.

Mit Recovery über Challenge/Response bietet Sophos SafeGuard verschiedene Workflows für typische Recovery-Szenarien, für die die Unterstützung durch ein Helpdesk erforderlich ist.

Für detaillierte Informationen, siehe [Recovery über Challenge/Response](#), Seite 139.

### ■ System-Recovery

Sophos SafeGuard bietet verschiedene Methoden und Tools für Recovery-Vorgänge in Bezug auf wichtige System- und Sophos SafeGuard Komponenten, z. B.:

- Korrupter MBR
- Probleme in Bezug auf den Sophos SafeGuard Kernel
- Probleme in Bezug auf Volume-Zugriff
- Probleme in Bezug auf Windows-Boot-Vorgänge
- Probleme in Bezug auf die GINA

Für detaillierte Informationen, siehe [Systemwiederherstellung](#), Seite 156.

## 20 Recovery über Local Self Help

Sophos SafeGuard bietet für durch Sophos SafeGuard geschützte Endpoint-Computer die Funktion Local Self Help. Über Local Self Help können sich Benutzer, die Ihr Kennwort vergessen haben, ohne Unterstützung des Helpdesks wieder an ihrem Computer anmelden.

Mit Local Self Help erhalten Benutzer auch in Situationen, in denen sie keine Telefon- oder Netzwerkverbindung und somit auch kein Challenge/Response-Verfahren nutzen können (z. B. an Bord eines Flugzeugs), wieder Zugang zu ihrem Computer. Um sich anzumelden, muss der Benutzer lediglich eine bestimmte Anzahl an vordefinierten Fragen in der Power-on Authentication beantworten.

Die zu beantwortenden Fragen können Sie als zuständiger Sicherheitsbeauftragter zentral vordefinieren und per Richtlinie an die Computer verteilen. Als Vorlage liefern wir Ihnen ein vordefiniertes Fragenthema, das Sie unverändert benutzen oder modifizieren können. Sie können die Benutzer auch per Richtlinie berechtigen, selbst Fragen zu definieren.

Für die initiale Beantwortung und spätere Bearbeitung der Fragen steht dem Benutzer nach der Aktivierung der Funktion auf seinem Computer der Local Self Help Assistent zur Verfügung. Detaillierte Informationen zu Local Self Help auf dem Endpoint-Computer finden Sie in der Sophos SafeGuard Benutzerhilfe im Kapitel *Recovery über Local Self Help*.

Local Self Help reduziert die Anzahl an Helpdesk-Anforderungen für Notfälle, die die Anmeldung betreffen. Helpdesk-Mitarbeitern werden somit Routine-Aufgaben abgenommen und sie können sich auf komplexere Support-Anforderungen konzentrieren.

### 20.1 Parameter für Local Self Help über eine Richtlinie definieren

Die Einstellungen für Local Self Help definieren Sie in einer Richtlinie vom Typ **Allgemeine Einstellungen** unter **Recovery für die Anmeldung - Local Self Help aktivieren**. Hier aktivieren Sie die Funktion zur Benutzung auf den Endpoint-Computern und legen weitere Berechtigungen und Parameter fest.

#### 20.1.1 Local Self Help aktivieren

Um die Funktion Local Self Help für die Benutzung auf Endpoint-Computern zu aktivieren, wählen Sie im Feld **Local Self Help** die Option **Local Self Help aktivieren**.

Nach dem Wirksamwerden der Richtlinie auf den Computern sind die Benutzer aufgrund dieser Einstellung berechtigt, Local Self Help für Recovery-Vorgänge, die die Anmeldung betreffen, zu benutzen.

Hierzu müssen die Benutzer die Funktion auf Ihrem Computer durch Beantwortung der erhaltenen Fragen oder durch Erstellung und Beantwortung eigener Fragen (je nach Berechtigung) aktivieren.

Nach dem Erhalt der von Ihnen erstellten Richtlinie und dem Neustart des Computers steht den Benutzern dafür der Local Self Help Assistent über das System Tray Icon in der Windows Task-Leiste zur Verfügung.

### 20.1.2 Weitere Einstellungen definieren

Neben der Aktivierung von Local Self Help können Sie in einer Richtlinie vom Typ **Allgemeine Einstellung** folgende Parameter für Local Self Help definieren:

#### ■ Minimale Länge der Antwort

Legen Sie hier die Mindestlänge der Antworten in Zeichen fest. Die Standardeinstellung ist 1.

#### ■ Willkommenstext unter Windows

Hier können Sie einen individuellen Informationstext angeben, der beim Starten des Local Self Help Assistenten auf dem Benutzercomputer im ersten Dialog angezeigt werden soll. Dieser Text muss zuvor erstellt und registriert werden.

#### ■ Benutzer dürfen eigene Fragen festlegen

Für die Hinterlegung der Fragen und Antworten für Local Self Help gibt es folgende Möglichkeiten:

- Sie definieren als Sicherheitsbeauftragter die Fragen und verteilen Sie an die Benutzer. Die Benutzer sind nicht dazu berechtigt, eigene Fragen zu definieren.
- Sie definieren als Sicherheitsbeauftragter die Fragen und verteilen Sie an die Benutzer. Die Benutzer sind dazu berechtigt, zusätzlich eigene Fragen zu definieren. Bei der Beantwortung der für die Aktivierung von Local Self Help notwendigen Mindestanzahl an Fragen können die Benutzer zwischen vorgegebenen und eigenen Fragen wählen oder eine Kombination aus beiden verwenden.
- Sie berechtigen die Benutzer dazu, eigene Fragen zu definieren und geben keine vordefinierten Fragen vor. Die Benutzer aktivieren Local Self Help durch Definition und Beantwortung eigener Fragen.

Um die Benutzer zur Definition eigener Fragen zu berechtigen, wählen Sie im Feld **Benutzer dürfen eigene Fragen festlegen** die Einstellung **Ja**.

## 20.2 Fragen definieren

Voraussetzung dafür, dass Local Self Help auf dem Endpoint-Computer verwendet werden kann, ist die Hinterlegung von mindestens zehn beantworteten Fragen. Um sich über Local Self Help an der Power-on Authentication anzumelden, muss der Benutzer fünf Fragen, die per Zufallsprinzip aus diesen zehn Fragen ausgewählt werden, korrekt beantworten.

Wenn der Benutzer nicht dazu berechtigt ist, eigene Fragen zu definieren, müssen Sie mindestens zehn vordefinierte Fragen mit der Richtlinie an den Computer für die Aktivierung von Local Self Help weitergeben.

Für die Definition und Bearbeitung von Local Self Help Fragen benötigen Sie als Sicherheitsbeauftragter die Berechtigung **Self Help Fragen ändern**.

### 20.2.1 Vorlage verwenden

Für Local Self Help liefern wir Ihnen ein vordefiniertes Fragenthema. Dieses Fragenthema steht standardmäßig in den Sprachen Deutsch und Englisch im Richtlinien-Navigationsbereich unter **Local Self Help Fragen** zur Verfügung.

Das Fragenthema steht optional auch in den Sprachen Französisch, Italienisch, Spanisch, und Japanisch zur Verfügung. Diese Sprachversionen lassen sich zusätzlich in den Navigationsbereich importieren.

**Hinweis:** Bei der Eingabe von Antworten auf Japanisch zur Aktivierung von Local Self Help auf Endpoint-Computern müssen die Benutzer Romajii-Zeichen (römische/lateinische Zeichen) verwenden. Andernfalls wird bei der Eingabe der Antworten in der Power-on Authentication keine Übereinstimmung erreicht.

Sie können das vordefinierte Fragenthema unverändert verwenden, bearbeiten oder löschen.

Wenn Sie die beiden Sprachversionen des vordefinierten Fragenthemas unverändert belassen und Local Self Help über eine Richtlinie vom Typ **Allgemeine Einstellungen** aktivieren, werden die beiden vordefinierten Fragenthemen automatisch mit dieser Richtlinie an die Endpoint-Computer weitergegeben.

## 20.3 Fragenthemen importieren

Über den Importvorgang können Sie zusätzliche Sprachversionen des vordefinierten Fragenthemas (oder eigene, als .XML-Datei erstellte Fragenlisten) importieren.

So importieren Sie ein Fragenthema:

1. Erstellen Sie ein neues Fragenthema.
2. Markieren Sie im **Richtlinien** Navigationsbereich das neue Fragenthema unter **Local Self Help Fragen**.
3. Klicken Sie im Arbeitsbereich mit der rechten Maustaste. Das Kontextmenü für das Fragenthema wird geöffnet. Wählen Sie **Importieren**.
4. Wählen Sie das Verzeichnis, in dem das Fragenthema abgelegt ist, sowie das gewünschte Fragenthema und klicken Sie auf **Öffnen**.

Die importierten Fragen werden im Arbeitsbereich angezeigt. Sie können das Fragenthema nun unverändert speichern oder bearbeiten.

## 20.4 Neues Fragenthema erstellen und Fragen hinzufügen

**Hinweis:** Neben Fragenthemen in verschiedenen Sprachen können Sie auch neue Fragenthemen zu unterschiedlichen Themenbereichen erstellen. Somit können Sie Benutzern mehrere Fragenthemen zur Verfügung stellen, aus denen sie das für sie am besten geeignete Thema auswählen können.

So erstellen Sie ein neues Fragenthema und fügen Fragen hinzu:

1. Markieren Sie im **Richtlinien** Navigationsbereich den Eintrag **Local Self Help Fragen**.
2. Klicken Sie mit der rechten Maustaste auf **Local Self Help Fragen** und wählen Sie **Neu > Fragenthema**.
3. Geben Sie einen Namen für das Fragenthema ein und klicken Sie auf **OK**.
4. Markieren Sie im **Richtlinien** Navigationsbereich das neue Fragenthema unter **Local Self Help Fragen**.
5. Klicken Sie im Arbeitsbereich mit der rechten Maustaste. Das Kontextmenü für das Fragenthema wird geöffnet. Wählen Sie **Hinzufügen**.

6. Eine neue Fragenzeile wird hinzugefügt. Geben Sie Ihre Frage ein und drücken Sie **Enter**. Um weitere Fragen hinzuzufügen, wiederholen Sie diesen Vorgang.
7. Speichern Sie Ihre Änderungen, indem Sie auf das **Speichern**-Symbol in der Symbolleiste klicken.

Ihr Fragenthema ist registriert und wird der Richtlinie vom Typ **Allgemeine Einstellungen**, über die Local Self Help auf den Endpoint-Computern aktiviert wird, automatisch mitgegeben.

## 20.5 Fragenthemen bearbeiten

So bearbeiten Sie bereits vorhandene Fragenthemen:

1. Markieren Sie das gewünschte Fragenthema unter **Local Self Help Fragen** im **Richtlinien** Navigationsbereich.
2. Sie können nun Fragen hinzufügen, ändern oder löschen.
  - Um Fragen hinzuzufügen, klicken Sie im Arbeitsbereich mit der rechten Maustaste und wählen Sie im Kontextmenü **Hinzufügen**. Geben Sie nun in der neu angezeigten Zeile Ihre Frage ein.
  - Um Fragen zu ändern, klicken Sie auf den Fragentext im Arbeitsbereich. Bei der gewählten Frage wird ein Stiftsymbol angezeigt. Geben Sie auf der Fragenzeile Ihre Änderungen ein.
  - Um Fragen zu löschen, markieren Sie die gewünschte Frage durch Klicken auf das graue Kästchen zu Beginn der Fragenzeile im Arbeitsbereich und wählen Sie im Kontextmenü des Frageneintrags **Löschen**.
3. Speichern Sie Ihre Änderungen an der Fragenliste, indem Sie auf das **Speichern**-Symbol in der Symbolleiste klicken.

Das geänderte Fragenthema ist registriert und wird der Richtlinie vom Typ **Allgemeine Einstellungen**, über die Local Self Help auf den Endpoint-Computern aktiviert wird, automatisch mitgegeben.

## 20.6 Fragenthemen löschen

Um ein Fragenthema zu löschen, klicken Sie mit der rechten Maustaste auf das Fragenthema unter **Local Self Help Fragen** im **Richtlinien** Navigationsbereich und wählen Sie **Löschen**.

**Hinweis:** Wenn Sie ein Fragenthema löschen, nachdem die Benutzer bereits Fragen aus diesem Thema zur Aktivierung von Local Self Help auf ihren Computern beantwortet haben, werden die Antworten der Benutzer ungültig, da die Fragen nicht mehr vorhanden sind.

## 20.7 Willkommenstexte registrieren

Sie können im Richtlinien-Navigationsbereich des SafeGuard Policy Editor einen Willkommenstext registrieren, der im ersten Dialog des Local Self Help Assistenten angezeigt werden soll.

Die Textdateien mit den gewünschten Informationen müssen erstellt werden, bevor sie im SafeGuard Policy Editor registriert werden können. Die maximale Dateigröße für Informationstexte beträgt 50 KB. Sophos SafeGuard verwendet nur Unicode UTF-16 kodierte Texte. Wenn Sie die Textdateien nicht in diesem Format erstellen, werden Sie bei der Registrierung automatisch in dieses Format konvertiert.

Wenn eine Konvertierung durchgeführt wird, werden Sie durch eine Meldung darüber informiert.

So registrieren Sie Informationstexte:

1. Klicken Sie im **Richtlinien** Navigationsbereich mit der rechten Maustaste auf **Informationstext** und wählen Sie **Neu > Text**.
2. Geben Sie unter **Textelementname** einen Namen für den anzeigenden Text ein.
3. Wählen Sie über die Schaltfläche [...] die zuvor erstellte Textdatei aus. Wenn eine Konvertierung notwendig ist, wird eine entsprechende Meldung angezeigt.
4. Klicken Sie auf **OK**.

Das neue Textelement wird als Unterknoten des Eintrags **Informationstext** im **Richtlinien** Navigationsbereich angezeigt. Ist ein Textelement markiert, wird sein Inhalt im Aktionsbereich angezeigt. Das Textelement kann jetzt beim Erstellen von Richtlinien ausgewählt werden.

Um weitere Textelemente zu registrieren, gehen Sie wie beschrieben vor. Alle registrierten Textelemente werden als Unterknoten angezeigt.

## 21 Recovery über Challenge/Response

Zur Optimierung von Workflows im Unternehmen und zur Reduzierung von Helpdesk-Kosten bietet Sophos SafeGuard eine Challenge/Response Recovery-Lösung. Mit einem benutzerfreundlichen Challenge/Response-Verfahren unterstützt Sophos SafeGuard Benutzer, die sich an ihrem Computer nicht mehr anmelden oder nicht auf verschlüsselte Daten zugreifen können.

Diese Funktionalität ist im SafeGuard Policy Editor in Form eines Recovery-Assistenten integriert.

### 21.1 Nutzen und Vorteile des Challenge/Response-Verfahrens

Das Challenge/Response-Verfahren ist ein sicheres und effizientes Recovery-System.

- Während des gesamten Vorgangs werden keine vertraulichen Daten in unverschlüsselter Form ausgetauscht.
- Informationen, die unberechtigte Dritte durch Mitverfolgen dieses Vorgangs erhalten könnten, lassen sich weder zu einem späteren Zeitpunkt noch auf anderen Geräten verwenden.
- Der Benutzer kann schnell wieder mit dem Computer arbeiten. Es gehen keine verschlüsselten Daten verloren, nur weil der Benutzer das Kennwort vergessen hat.

### 21.2 Typische Situationen, in denen Hilfe beim Helpdesk angefordert wird

- Ein Benutzer hat sein Kennwort für die Anmeldung auf der POA-Ebene vergessen. Der Computer ist gesperrt.

**Hinweis:** Wir empfehlen, in erster Linie Local Self Help einzusetzen, um ein vergessenes Kennwort wiederherzustellen. Mit Recovery über Local Self Help kann sich der Benutzer selbst das aktuelle Benutzerkennwort anzeigen lassen und es weiterhin zur Anmeldung verwenden. Dadurch lässt sich das Zurücksetzen des Kennworts vermeiden. Auch ist in diesem Fall keine Unterstützung durch den Helpdesk notwendig. Für weitere Informationen, siehe [Recovery über Local Self Help](#), Seite 133.

- Der Local Cache der Power-on Authentication ist teilweise beschädigt.

Sophos SafeGuard bietet für diese typischen Notfälle unterschiedliche Recovery- Workflows, die dem Benutzer wieder den Zugang zu seinem Computer ermöglichen.

## 21.3 Challenge/Response Workflow

Das Challenge/Response-Verfahren basiert auf zwei Komponenten:

- Endpoint-Computer, auf dem der Challenge Code erzeugt wird.
- SafeGuard Policy Editor, in dem Sie als Helpdesk-Beauftragter mit ausreichenden Rechten einen Response-Code erstellen, der den Benutzer zur Ausführung der angeforderten Aktion auf dem Computer berechtigt.

1. Der Benutzer fordert auf dem Endpoint-Computer einen Challenge-Code an. Je nach Recovery-Typ wird der Challenge-Code in der Power-on Authentication oder über das KeyRecovery Tool angefordert.

Ein Challenge-Code in Form einer ASCII-Zeichenfolge wird generiert und angezeigt.

2. Der Benutzer wendet sich an den Helpdesk und übermittelt seine notwendige Identifikation sowie den Challenge-Code.
3. Der Helpdesk-Beauftragte startet den Recovery-Assistenten im SafeGuard Policy Editor.
4. Der Helpdesk-Beauftragte wählt den entsprechenden Recovery-Typ, bestätigt die Identifikationsinformationen sowie den Challenge-Code und wählt die gewünschte Recovery-Aktion aus.

Ein Response-Code in Form einer ASCII-Zeichenfolge wird generiert und angezeigt.

5. Der Helpdesk-Beauftragte übermittelt dem Benutzer den Response-Code, z. B. über das Telefon oder über eine Textmitteilung.
6. Der Benutzer gibt den Response-Code ein. Je nach Recovery-Typ erfolgt dies in der POA oder über das KeyRecovery Tool.

Der Benutzer kann die autorisierte Aktion, z. B. Zurücksetzen des Kennworts, ausführen und wieder mit dem Computer arbeiten.

## 21.4 Recovery-Assistenten starten

Damit Sie in der Lage sind, ein Recovery-Verfahren auszuführen, stellen Sie sicher, dass Sie über die erforderlichen Rechte und Berechtigungen verfügen.

1. Melden Sie sich am SafeGuard Policy Editor an.
2. Klicken Sie auf **Extras > Recovery** in der Menüleiste.

Der SafeGuard Recovery-Assistent wird gestartet. Sie können den angeforderten Recovery-Typ auswählen.

## 21.5 Recovery-Typen

Wählen Sie den Recovery-Typ, den Sie verwenden möchten. Folgende Recovery-Typen stehen zur Verfügung:

### ■ Challenge Response für Sophos SafeGuard Client

Sophos SafeGuard bietet Challenge/Response für Recovery-Vorgänge, wenn der Benutzer sein Kennwort vergessen oder es zu oft falsch eingegeben hat.

**Hinweis:** Beachten Sie hierzu auch die Recovery-Methode Local Self Help für die Anmeldung. Diese Methode erfordert keine Unterstützung durch einen Helpdesk.

### ■ Challenge/Response mit virtuellen Clients

Recovery-Vorgänge für verschlüsselte Volumes lassen sich in Fällen, in denen ein Challenge/Response-Vorgang normalerweise nicht unterstützt würde (z. B. bei einer korrupten POA), auf einfache Art und Weise unter Anwendung von spezifischen Dateien mit der Bezeichnung virtuelle Clients durchführen.

## 21.6 Challenge/Response für Sophos SafeGuard Client

Sophos SafeGuard bietet Challenge/Response für Recovery-Vorgänge, z. B. wenn der Benutzer sein Kennwort vergessen oder es zu oft falsch eingegeben hat. Die für Challenge/Response-Vorgänge benötigten Recovery-Informationen basieren in diesem Fall auf der Schlüssel-Recovery-Datei. Auf jedem Sophos SafeGuard Endpoint-Computer wird während der Sophos SafeGuard Installation automatisch eine Schlüssel-Recovery-Datei generiert.

Steht diese Schlüssel-Recovery-Datei dem Helpdesk zur Verfügung (z. B. über eine Netzwerkfreigabe) kann das POA Challenge/Response-Verfahren für einen durch Sophos SafeGuard geschützten Computer durchgeführt werden.

Um die Suche nach und die Gruppierung von Recovery-Dateien zu vereinfachen, enthalten die Dateinamen den Namen des Computers: computername.GUID.xml. Somit sind Suchvorgänge mit Asterisken (\*) als Platzhalter möglich, z. B.: \*.GUID.xml.

**Hinweis:** Wenn ein Computer umbenannt wird, wird er im Local Cache nicht automatisch entsprechend umbenannt. Im Local Cache werden alle Schlüssel, Richtlinien, Benutzertifikate und Audit-Dateien gespeichert. Für die Datei-Generierung muss der neue Computernamen daher aus dem Local Cache entfernt werden, so dass nur der vorige Name verbleibt, auch wenn der Computer unter Windows umbenannt werden.

### 21.6.1 POA-Recovery-Aktionen

Für einen Endpoint-Computer muss in den folgenden Situationen ein POA Challenge/Response-Verfahren gestartet werden:

- Der Benutzer hat sein Kennwort auf POA-Ebene zu oft falsch eingegeben und der Computer wurde gesperrt.
- Der Benutzer hat sein Kennwort vergessen.
- Ein beschädigter Local Cache muss repariert werden.

Für einen durch Sophos SafeGuard geschützten Computer ist nur der definierte Computerschlüssel, jedoch kein Benutzerschlüssel in der Datenbank verfügbar. Somit ist in einem Challenge/Response-Verfahren nur die Recovery-Aktion **SGN Client ohne Benutzeranmeldung booten** möglich.

Das Challenge/Response-Verfahrens ermöglicht das Booten des Computers durch die Power-on Authentication. Der Benutzer kann sich dann an Windows anmelden.

Mögliche Recovery-Anwendungsfälle:

**Der Benutzer hat das Kennwort auf POA-Ebene zu oft falsch eingegeben und der Computer wurde gesperrt.**

Der Computer ist gesperrt und der Benutzer wird dazu aufgefordert, ein Challenge/Response-Verfahren zu starten, um wieder Zugriff auf den Computer zu erhalten. Da in diesem Fall das Kennwort nicht zurückgesetzt werden muss, weil der Benutzer das Kennwort noch weiß, ermöglicht das Challenge/Response-Verfahren das Booten des Computers durch die Power-on Authentication. Der Benutzer kann dann das korrekte Kennwort auf Windows-Ebene eingeben und den Computer wieder benutzen.

### **Der Benutzer hat das Kennwort vergessen**

**Hinweis:** Wir empfehlen, in erster Linie Local Self Help einzusetzen, um ein vergessenes Kennwort wiederherzustellen. Mit Recovery über Local Self Help kann sich der Benutzer selbst das aktuelle Benutzerkennwort unter Wahrung der Vertraulichkeit in der Power-on Authentication anzeigen lassen und es weiterhin zur Anmeldung verwenden. Für weitere Informationen siehe [Recovery über Local Self Help](#), Seite 133.

Wenn das Kennwort über ein Challenge/Response-Verfahren wiederhergestellt wird, muss das Kennwort zurückgesetzt werden.

1. Das Challenge/Response-Verfahren ermöglicht das Booten des Computers durch die Power-on Authentication.
2. Da dem Benutzer das Kennwort nicht bekannt ist, kann er es im Windows-Dialog nicht eingeben. Das Kennwort muss daher auf Windows-Ebene zurückgesetzt werden. Hierzu sind weitere Recovery-Vorgänge außerhalb von Sophos SafeGuard erforderlich, die über Windows-Standard-Verfahren durchgeführt werden müssen.
3. Wir empfehlen, die folgenden Methoden für das Zurücksetzen des Kennworts auf Windows-Ebene:
  - Über ein Service-Benutzerkonto oder ein Administratorkonto mit den erforderlichen Windows-Rechten auf dem Endpoint-Computer
  - Über eine Windows-Kennwortrücksetz-Diskette auf dem Endpoint-Computer
4. Der Benutzer gibt das vom Helpdesk zur Verfügung gestellte neue Kennwort auf Windows-Ebene ein. Unmittelbar danach ändert der Benutzer das Kennwort in ein nur ihm bekanntes Kennwort.
5. Sophos SafeGuard stellt fest, dass das neu gewählte Kennwort nicht mehr dem aktuellen Sophos SafeGuard Kennwort entspricht, das in der POA verwendet wird. Der Benutzer wird aufgefordert, das alte Kennwort einzugeben. Da er das Passwort vergessen hat, muss er auf **Abbrechen** klicken.
6. Da beim Zurücksetzen eines Kennworts ohne Angabe des alten Kennworts in Sophos SafeGuard ein neues Zertifikat generiert werden muss, muss der Benutzer diesen Vorgang bestätigen.
7. Ein neues Benutzerzertifikat wird basierend auf dem neu gewählten Windows-Kennwort erstellt. Dies ermöglicht es dem Benutzer, sich wieder an seinem Computer und an der Power-on Authentication mit dem neuen Kennwort anzumelden.

### **Schlüssel für SafeGuard Data Exchange**

Wenn der Benutzer das Windows-Kennwort vergessen hat und ein neues eingeben muss, wird auch ein neues Zertifikat erstellt. In diesem Fall kann der Benutzer daher nicht mehr die bereits für SafeGuard Data Exchange erstellten Schlüssel verwenden. Damit bereits für SafeGuard Data Exchange generierte Benutzerschlüssel weiterhin verwendet werden können, müssen dem Benutzer die SafeGuard Data Exchange Passphrasen zur Reaktivierung dieser Schlüssel bekannt sein.

SafeGuard Data Exchange ist mit ESDP (Endpoint Security and Data Protection) nicht verfügbar.

### **Der Local Cache muss repariert werden**

Im Local Cache werden alle Schlüssel, Richtlinien, Benutzertifikate und Audit-Dateien gespeichert. Standardmäßig ist der Recovery-Vorgang deaktiviert, wenn der Local Cache korrupt ist, d. h. der Local Cache wird automatisch aus seiner Sicherungskopie wiederhergestellt. In diesem Fall ist kein Challenge/Response-Verfahren für die Reparatur notwendig. Soll die Reparatur des Local Cache explizit über ein Challenge/Response-Verfahren durchgeführt werden, kann der Recovery-Vorgang über eine Richtlinie aktiviert werden. In diesem Fall wird der Benutzer automatisch bei der Anmeldung an der Power-on Authentication aufgefordert, ein Challenge/Response-Verfahren zu starten.

## **21.6.2 Response mit einer Schlüssel-Recovery-Datei erzeugen**

Die Schlüssel-Recovery-Datei, die während der Installation der Sophos SafeGuard Verschlüsselungs-Software erzeugt wird, muss an einem Speicherort abgelegt sein, auf den der Helpdesk-Beauftragte Zugriff hat. Außerdem muss der Name der Datei bekannt sein.

So erzeugen Sie eine Response:

1. Wählen Sie im SafeGuard Policy Editor in der Menüleiste **Extras > Recovery**, um den Recovery-Assistenten zu öffnen.
2. Wählen Sie unter **Recovery-Typ** die Option **Sophos SafeGuard Client**.
3. Klicken Sie auf **Browse**, um die erforderliche Recovery-Datei auszuwählen. Zur Vereinfachung der Identifizierung tragen die Recovery-Dateien den Namen des Computers: `computername.GUID.xml`.
4. Geben Sie den vom Benutzer erhaltenen Challenge-Code ein und klicken Sie auf **Weiter**. Der Challenge-Code wird geprüft.

Wenn der Challenge-Code korrekt eingegeben wurde, werden die vom Sophos SafeGuard Endpoint-Computer angeforderte Recovery-Aktion sowie die möglichen Recovery-Aktionen angezeigt. Wenn der Code nicht korrekt eingegeben wurde, wird unterhalb des Blocks, der den Fehler enthält, der Text **Ungültig** angezeigt.

5. Wählen Sie die vom Benutzer durchzuführende Aktion aus und klicken Sie auf **Weiter**.
6. Es wird ein Response-Code erzeugt. Teilen Sie den Response-Code dem Benutzer mit. Hierzu steht eine Buchstabierhilfe zur Verfügung. Sie können den Response-Code auch in die Zwischenablage kopieren.

Der Benutzer kann den Response-Code eingeben, die angeforderte Aktion ausführen und dann wieder mit dem Computer arbeiten.

## 21.7 Challenge/Response mit virtuellen Clients

Mit Recovery über Challenge/Response mit virtuellen Clients bietet Sophos SafeGuard ein Recovery-Verfahren für verschlüsselte Volumes in komplexen Notfallsituationen, z. B. wenn die POA korrupt ist. Challenge/Response mit virtuellen Clients basiert auf folgenden Komponenten:

### ■ Schlüssel-Recovery-Datei

Diese Datei wird während der Konfiguration der Sophos SafeGuard Verschlüsselung erstellt und enthält den Verschlüsselungsschlüssel für den Endpoint-Computer. Diese Schlüssel-Recovery-Datei wird für jeden durch Sophos SafeGuard geschützten Computer erzeugt und enthält den definierten Computerschlüssel, der mit dem Unternehmenszertifikat verschlüsselt ist. Die Datei muss an einem Speicherort abgelegt sein, auf den der Helpdesk Zugriff hat (z. B. USB-Stick oder Netzwerkfreigabe).

### ■ Virtueller Client

Im SafeGuard Policy Editor werden spezifische Dateien mit der Bezeichnung virtueller Client erstellt und als Referenzinformation in der Datenbank verwendet.

### ■ Sophos SafeGuard modifizierte Windows PE Recovery Disk

Die Recovery Disk wird zum Booten des Endpoint-Computers vom BIOS verwendet.

### ■ KeyRecovery Tool

Mit diesem Tool wird das Challenge/Response-Verfahren gestartet. Es steht bereits auf der Sophos SafeGuard modifizierten Windows PE Recovery Disk zur Verfügung. Darüber hinaus finden Sie es im Tools-Verzeichnis Ihrer Sophos SafeGuard Software-Lieferung.

### **21.7.1 Virtuelle Clients**

Virtuelle Clients sind spezifische, verschlüsselte Schlüsseldateien, die für Recovery-Vorgänge bei einem verschlüsselten Volume verwendet werden, wenn in der Datenbank keine Referenzinformationen zum betreffenden Computer zur Verfügung stehen und normalerweise Challenge/Response-Verfahren nicht unterstützt würden. Der virtuelle Client wird während eines Challenge/Response-Verfahrens als Identifizierungs- und Referenzinformation verwendet und wird in der Datenbank gespeichert.

Um ein Challenge/Response-Verfahren in komplexen Notfallsituationen zu ermöglichen, müssen die virtuellen Clients vor der Durchführung eines solchen Verfahrens erstellt und an den Benutzer übermittelt werden. Der Zugriff auf den Computer kann dann mit Hilfe dieser virtuellen Clients, dem KeyRecovery Tool und einer SafeGuard-modifizierten Windows PE Recovery Disk wiederhergestellt werden.

### **21.7.2 Recovery Workflow mit virtuellen Clients**

Über folgenden allgemeinen Workflow lässt sich der Zugang zum verschlüsselten Computer wiederherstellen:

1. Sie erhalten die Sophos SafeGuard Recovery Disk vom technischen Support.
2. Für den Helpdesk steht die Windows PE Recovery Disk mit den aktuellen Sophos SafeGuard Filter-Treibern auf der Sophos Support-Website zum Download zur Verfügung. Weitere Informationen finden Sie in der Wissensdatenbank: <http://www.sophos.com/support/knowledgebase/article/108805.html>
3. Erstellen Sie den virtuellen Client im SafeGuard Policy Editor.
4. Exportieren Sie den virtuellen Client in eine Datei.
5. Booten Sie den Computer von der Recovery Disk.
6. Importieren Sie die Datei mit dem virtuellen Client in das KeyRecovery Tool.
7. Starten Sie die Challenge im KeyRecovery Tool.
8. Bestätigen Sie den virtuellen Client im SafeGuard Policy Editor.
9. Wählen Sie die erforderliche Recovery-Aktion.
10. Geben Sie den Challenge-Code im SafeGuard Policy Editor ein.
11. Generieren Sie den Response-Code im SafeGuard Policy Editor.

12. Geben Sie den Response-Code im KeyRecovery Tool ein.  
Auf den Computer kann wieder zugegriffen werden.

### **21.7.3 Virtuellen Client anlegen**

Virtuelle Clients sind spezifische, verschlüsselte Schlüsseldateien, die in einem Challenge/Response-Verfahren als Referenzinformation für den Computer verwendet werden.

Virtuelle Clients können für verschiedene Computer und in mehreren Challenge/Response-Verfahren benutzt werden.

1. Klicken Sie im SafeGuard Policy Editor auf den Bereich **Virtuelle Clients**.
2. Klicken Sie im Navigationsfenster auf der linken Seite auf **Virtuelle Clients**.
3. Klicken Sie in der Symbolleiste auf **Virtuellen Client hinzufügen**.
4. Geben Sie einen eindeutigen Namen für den virtuellen Client ein und klicken Sie auf **OK**. Die virtuellen Clients werden anhand der hier eingegebenen Namen in der Datenbank identifiziert.
5. Klicken Sie auf das **Speichern**-Symbol in der Symbolleiste, um Ihre Änderungen in der Datenbank zu speichern.

Der neue virtuelle Client wird im Aktionsbereich angezeigt. Im nächsten Schritt exportieren Sie den virtuellen Client in eine Datei.

### **21.7.4 Virtuellen Client exportieren**

Virtuelle Clients müssen in Dateien exportiert werden, um sie an die Endpoint-Computer zu verteilen und sie in Recovery-Vorgängen nutzen zu können. Diese Dateien haben immer die Bezeichnung `recoverytoken.tok`.

1. Klicken Sie im SafeGuard Policy Editor auf den Bereich **Virtuelle Clients**.
2. Klicken Sie im Navigationsfenster auf der linken Seite auf **Virtuelle Clients**.
3. Klicken Sie im Aktionsbereich auf das Lupensymbol, um nach dem gewünschten virtuellen Client zu suchen. Die verfügbaren virtuellen Clients werden angezeigt.
4. Wählen Sie den gewünschten Eintrag im Aktionsbereich aus und klicken Sie in der Symbolleiste auf **Virtuellen Client exportieren**.



Der Inhalt des verschlüsselten Laufwerks ist im Dateimanager nicht sichtbar. In den Eigenschaften des verschlüsselten Laufwerks werden weder das Dateisystem, noch die Kapazität sowie der verwendete/freie Speicherplatz angegeben.

2. Klicken Sie unten im Bereich **Quick Launch** des Dateimanagers auf das KeyRecovery-Symbol, um das KeyRecovery Tool zu öffnen. Das Key Recovery Tool zeigt die Schlüssel-ID verschlüsselter Laufwerke.



3. Suchen Sie nach der Schlüssel-ID des Laufwerks, auf das Sie zugreifen möchten. Die Schlüssel-ID wird später abgefragt.

Im nächsten Schritt importieren Sie den virtuellen Client in das Key Recovery Tool.

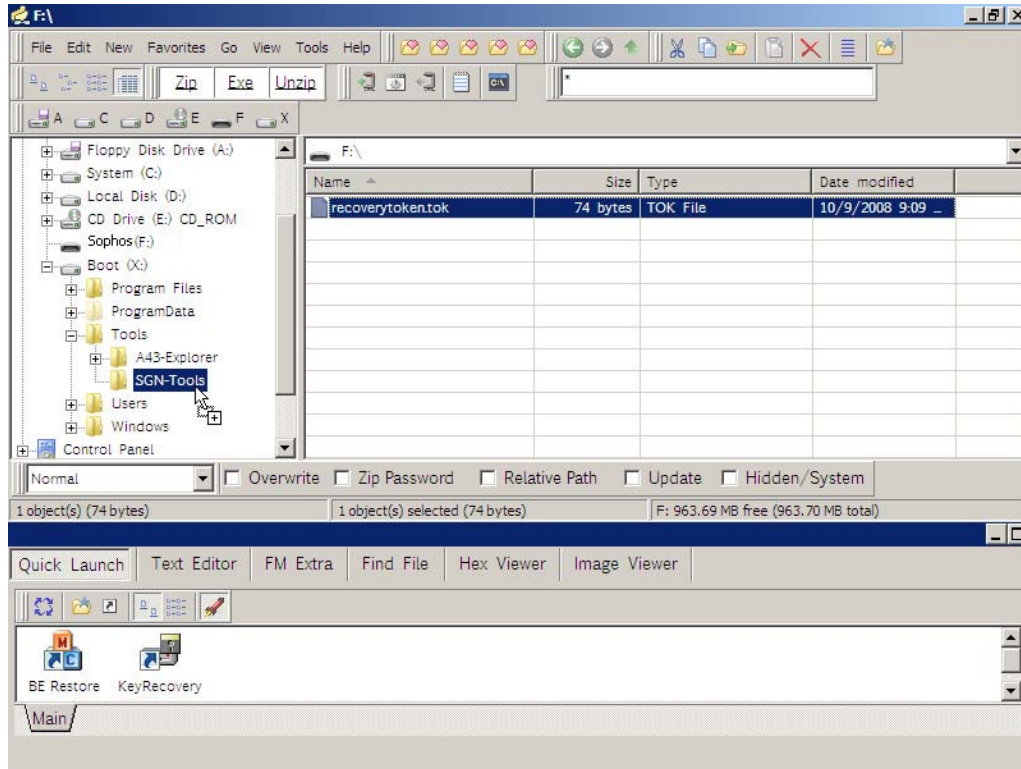
### 21.7.6 Virtuellen Client in das KeyRecovery Tool importieren

#### Voraussetzungen:

- Der Computer wurde von der Recovery Disk gebootet.
- Stellen Sie sicher, dass das USB-Laufwerk mit der Datei recoverytoken.tok erfolgreich bereitgestellt wurde.

1. Wählen Sie im Windows PE Dateimanager das Laufwerk aus, auf dem der virtuelle Client gespeichert ist. Die Datei recoverytoken.tok wird auf der rechten Seite angezeigt.

2. Wählen Sie die Datei recoverytoken.tok aus und ziehen Sie sie auf das Laufwerk, auf dem sich das KeyRecovery Tool befindet. Legen Sie die Datei hier im Verzeichnis Tools\SGN-Tools ab.



### 21.7.7 Challenge im KeyRecovery Tool starten

1. Klicken Sie unten im Bereich **Quick Launch** des Dateimanagers auf das KeyRecovery-Symbol, um das KeyRecovery Tool zu öffnen. Das Key Recovery Tool zeigt die Schlüssel-ID verschlüsselter Laufwerke.

Das Tool startet und zeigt eine Liste aller Volumes mit den jeweiligen Verschlüsselungsinformationen (Schlüssel-ID).



2. Wählen Sie das Volume, das Sie entschlüsseln möchten, und klicken Sie auf Import mit C/R, um den Challenge-Code zu erzeugen.

Die Datei mit dem virtuellen Client wird als Referenz in der Sophos SafeGuard Datenbank verwendet und in der Challenge angegeben. Der Challenge-Code wird erzeugt und angezeigt.

3. Übermitteln Sie den Namen des virtuellen Clients und den Challenge-Code an den Helpdesk, z. B. über Telefon oder eine Textmitteilung. Hierzu steht eine Buchstabierhilfe zur Verfügung.

## 21.7.8 Response mit virtuellen Clients erzeugen

Um auf einen durch Sophos SafeGuard geschützten Computer zuzugreifen und eine Response mit virtuellen Clients zu erzeugen, sind zwei Aktionen erforderlich:

1. Bestätigen Sie den virtuellen Client in der SafeGuard Policy Editor Datenbank.
2. Wählen Sie die erforderliche Recovery-Aktion aus. Da für die Entschlüsselung nur die Schlüssel-Recovery-Datei verfügbar ist, muss diese Datei ausgewählt werden, damit ein Response-Code erzeugt werden kann.

### 21.7.8.1 Virtuellen Client bestätigen

#### **Voraussetzung:**

Der virtuelle Client muss im SafeGuard Policy Editor unter **Virtuelle Clients** angelegt worden sein und er muss in der Datenbank zur Verfügung stehen.

1. Klicken Sie im SafeGuard Policy Editor auf **Extras > Recovery**, um den Recovery-Assistenten zu öffnen.
2. Wählen Sie unter **Recovery-Typ** die Option **Virtueller Client**.
3. Geben Sie den Namen des virtuellen Client ein, den Sie vom Benutzer erhalten haben. Hierzu gibt es verschiedene Möglichkeiten:
  - Geben Sie den eindeutigen Namen direkt ein.
  - Wählen Sie einen Namen, indem Sie auf [...] im Abschnitt **Virtueller Client** des Dialogs **Recovery-Typ** klicken. Klicken Sie anschließend auf **Jetzt suchen**. Eine Liste mit virtuellen Clients wird angezeigt. Wählen Sie den gewünschten virtuellen Client aus und klicken Sie auf **OK**. Der Name des virtuellen Clients wird nun im Fenster **Recovery-Typ** unter **Virtueller Client** angezeigt.
4. Klicken Sie auf **Weiter**, um den Namen der Datei mit dem virtuellen Client zu bestätigen.

Im nächsten Schritte wählen Sie die erforderliche Recovery-Aktion aus.

### 21.7.8.2 Schlüssel-Recovery-Datei auswählen

**Voraussetzung:**

Sie müssen den erforderlichen virtuellen Client im Recovery-Assistenten des SafeGuard Policy Editor ausgewählt haben.

Die Schlüssel-Recovery-Datei, die zur Wiederherstellung des Zugriffs auf den Computer erforderlich ist, muss dem Helpdesk zur Verfügung stehen, z. B. über eine Netzwerkfreigabe.

1. Wählen Sie im Recovery-Assistenten unter Virtueller Client die erforderliche Recovery-Aktion **Schlüssel angefordert** und klicken Sie auf **Weiter**.
2. Aktivieren Sie die Option **Schlüssel-Recovery-Datei mit Recovery-Schlüssel auswählen**.
3. Klicken Sie neben dieser Option auf [...], um nach der entsprechenden Datei zu suchen. Zur Vereinfachung tragen die Recovery-Dateien den Namen des jeweiligen Computers: `computername.GUID.xml`.
4. Bestätigen Sie Ihre Auswahl mit **Weiter**. Das Fenster für die Eingabe des Challenge-Codes wird angezeigt.
5. Geben Sie den vom Benutzer erhaltenen Challenge-Code ein und klicken Sie auf **Weiter**. Der Challenge-Code wird geprüft.

Wenn der Challenge-Code korrekt eingegeben wurde, wird der Response-Code erzeugt. Wurde der Code nicht korrekt eingegeben, wird unterhalb des Blocks, der den Fehler enthält, der Text **Ungültig** angezeigt.

6. Teilen Sie dem Benutzer den Response-Code mit. Hierzu steht eine Buchstabierhilfe zur Verfügung. Sie können den Response-Code auch in die Zwischenablage kopieren.

### 21.7.9 Response-Code im KeyRecovery Tool eingeben

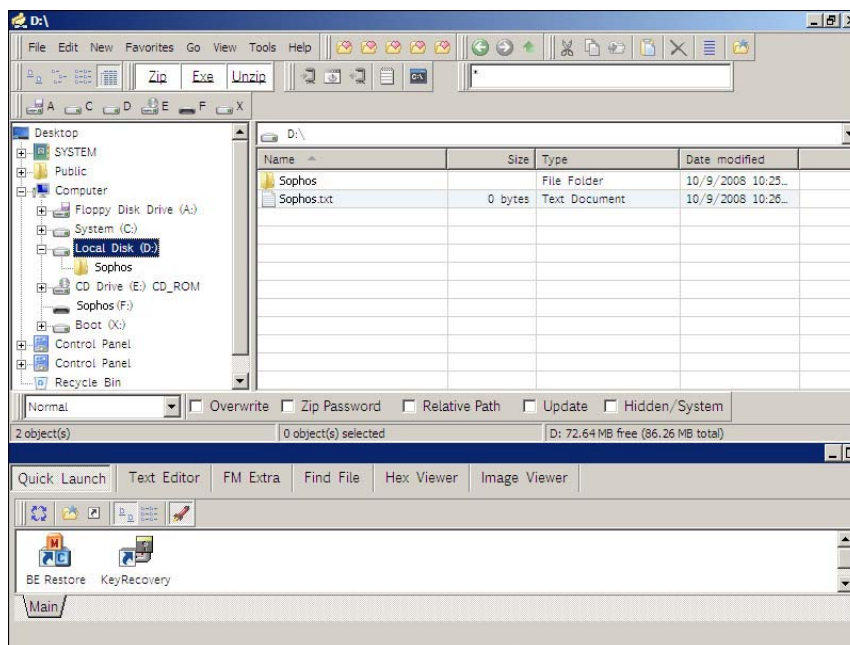
1. Geben Sie im KeyRecovery Tool auf dem Endpoint-Computer den Response-Code ein, den Sie vom Helpdesk erhalten haben.

Mit dem Response-Code wird der erforderliche Recovery-Schlüssel übertragen.

2. Klicken Sie auf **OK**. Das für das Challenge/Response-Verfahren gewählte Laufwerk wird entschlüsselt.



3. Um sicherzustellen, dass die Entschlüsselung erfolgreich durchgeführt werden konnte, wählen Sie das entschlüsselte Laufwerk im Windows PE Dateimanager aus:



Der Inhalt des entschlüsselten Laufwerks wird nun im Dateimanager angezeigt. Das Dateisystem und die Kapazität sowie der benutzte/freie Speicherplatz werden nun in den Eigenschaften des entschlüsselten Laufwerks angegeben.

Der Zugriff auf die in dieser Partition gespeicherten Daten ist wiederhergestellt. Nach der erfolgreichen Entschlüsselung haben Sie auf dem entsprechenden Laufwerk Lese- und Schreibzugriff für Daten. Sie können Daten vom und auf das Laufwerk kopieren.

### **21.7.10 Virtuelle Clients löschen**

Sie können virtuelle Clients, die nicht mehr benötigt werden, aus der Datenbank löschen.

1. Klicken Sie im SafeGuard Policy Editor auf **Virtuelle Clients**.
2. Klicken Sie im Navigationsfenster auf der linken Seite auf **Virtuelle Clients**.
3. Klicken Sie im Aktionsbereich auf das Lupensymbol, um nach dem gewünschten virtuellen Client zu suchen. Die verfügbaren virtuellen Clients werden angezeigt.
4. Wählen Sie den gewünschten Eintrag im Aktionsbereich aus und klicken Sie in der Symbolleiste auf **Virtuellen Client löschen**.
5. Klicken Sie auf das **Speichern**-Symbol in der Symbolleiste, um Ihre Änderungen in der Datenbank zu speichern.

Der virtuelle Client wird aus der Datenbank gelöscht und kann nicht mehr für Challenge/Response-Verfahren benutzt werden.

## 22 Systemwiederherstellung

Sophos SafeGuard 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 Sophos SafeGuard Module nicht verfügbar sind oder nicht funktionieren.

Die folgenden Abschnitte beschreiben mögliche Fehlerquellen und Recovery-Verfahren.

### 22.1 Daten-Recovery durch Booten von einem externen Medium

Dieser Recovery-Typ kann angewendet werden, wenn sich der Benutzer zwar noch an der POA anmelden, jedoch nicht mehr auf das verschlüsselte Volume zugreifen kann. In diesem Fall kann der Zugriff auf die verschlüsselten Daten durch Booten des Computers über eine für Sophos SafeGuard angepasste Windows PE Recovery Disk wiederhergestellt werden.

Voraussetzungen:

- Der Benutzer, der vom externen Medium bootet, muss dazu berechtigt sein. Dieses Recht kann entweder im SafeGuard Policy Editor innerhalb einer Richtlinie vom Typ **Authentisierung** konfiguriert werden (**Benutzer darf Volume entschlüsseln auf Ja** eingestellt), oder es kann für die einmalige Benutzung über ein Challenge/Response-Verfahren erlangt werden.
- Der Computer muss das Booten von anderen Medien außer von der fest eingebauten Festplatte unterstützen.

So erhalten Sie wieder Zugriff auf die verschlüsselten Daten auf dem Computer:

1. Sie erhalten die Sophos SafeGuard Recovery Disk vom technischen Support.

Für den Helpdesk steht die Windows PE Recovery Disk mit den aktuellen Sophos SafeGuard Filtertreibern auf der Sophos Support-Website zum Download zur Verfügung. Weitere Informationen finden Sie in unserer Wissensdatenbank: <http://www.sophos.com/support/knowledgebase/article/108805.html>.

2. Melden Sie sich an der Power-on Authentication mit Ihren Anmeldeinformationen an.
3. Legen Sie die Windows PE Recovery Disk ein.
4. Wählen Sie im POA-Anmeldedialog unter **Weiterbooten von:** die Option **externes Medium**. Der Computer wird gestartet.

Der Zugriff auf die auf dieser Partition gespeicherten Daten ist wiederhergestellt.

## 22.2 Beschädigter MBR

Zur Problembeseitigung im Fall eines beschädigten MBR bietet Sophos SafeGuard das Tool BE\_Restore.exe.

Eine detaillierte Beschreibung zur Wiederherstellung eines beschädigten MBR finden Sie in der SafeGuard Tools-Anleitung unter BE\_Restore.exe.

## 22.3 Volumes

Sophos SafeGuard bietet die laufwerksbezogene Verschlüsselung. Dies beinhaltet die Speicherung von Verschlüsselungsinformationen bestehend aus Bootsektor, primärer bzw. Backup-KSA und Originalbootsektor auf jedem Laufwerk selbst.

Sobald eine dieser Einheiten beschädigt ist, besteht kein Zugriff mehr auf das Volume:

- eine der beiden Key Storage Areas (KSA)
- Original-MBR

### 22.3.1 Bootsektor

Der Bootsektor eines Volumes wird bei der Verschlüsselung gegen den Sophos SafeGuard Bootsektor ausgetauscht.

Der Sophos SafeGuard Bootsektor enthält Informationen über

- den Ort der primären und Backup-KSA in Clustern und Sektoren bezogen auf den Start der Partition
- die Größe der KSA

Auch wenn der Sophos SafeGuard Bootsektor zerstört ist, ist kein Zugriff auf verschlüsselte Volumes möglich.

Das Tool BE\_Restore kann den zerstörten Bootsektor wiederherstellen. Eine detaillierte Beschreibung dieses Tools finden Sie in der SafeGuard Tools-Anleitung.

### 22.3.2 Originaler Bootsektor

Beide KSAs enthalten den originalen Bootsektor. Das ist jener, der ausgeführt wird, nachdem der DEK (Data Encryption Key) entschlüsselt wurde und der Algorithmus und der Schlüssel in den BE Filtertreiber geladen wurden.

Ist dieser Bootsektor defekt, kann Windows nicht auf das Volume zugreifen. Normalerweise wird die bekannte Fehlermeldung „Gerät ist nicht formatiert. Möchten Sie es jetzt formatieren? Ja/Nein“ angezeigt.

Sophos SafeGuard wird den DEK für dieses Volume dennoch laden. Jedes Tool, das den Bootsektor reparieren kann, soll dennoch laufen - vorausgesetzt, es passiert den Sophos SafeGuard Upper Volume Filter.

## 22.4 Setup WinPE für Sophos SafeGuard

Um Zugriff auf verschlüsselte Laufwerke mit dem BOOTKEY eines Computers innerhalb einer WinPE Umgebung zu erhalten, stellt Sophos SafeGuard WinPE mit notwendigen Sophos SafeGuard Funktionsmodulen wie Treibern zur Verfügung. Um SetupWinPE zu starten, geben Sie folgenden Befehl ein:

```
SetupWinPE -pe2 <WinPE Image-Datei>
```

WinPE Image-Datei ist dabei die vollständige Pfadangabe des I386 Verzeichnisses für eine WinPE-CD.

SetupWinPE führt alle erforderlichen Änderungen durch.

**Hinweis:** Beachten Sie, dass über eine derartige WinPE-Umgebung nur auf verschlüsselte Laufwerke zugegriffen werden kann, die mit dem BOOTKEY verschlüsselt sind.

## 23 Deinstallation von Sophos SafeGuard auf Endpoint-Computern verhindern

Um den Schutz von Endpoint-Computern noch zu erweitern, können Sie die lokale Deinstallation von Sophos SafeGuard über eine Richtlinie vom Typ **Spezifische Computereinstellungen** als unzulässig definieren. Um die lokale Deinstallation zu verhindern, setzen Sie das Feld **Deinstallation erlaubt** in einer **Spezifische Computereinstellungen** Richtlinie auf **Nein** und übermitteln Sie die Richtlinie an die Endpoint-Computer. Nach Wirksamwerden einer solchen Richtlinie auf dem Endpoint-Computer werden Deinstallationsvorgänge abgebrochen. Jeder unautorisierte Versuch, Sophos SafeGuard zu installieren, wird protokolliert.

**Hinweis:** Wenn Sie eine Demoversion verwenden, sollten Sie diese Richtlinieneinstellung nicht aktivieren bzw. vor Ablauf der Demoversion deaktivieren, damit die Demo-Version auf einfache Art und Weise deinstalliert werden kann.

### 23.1 Sophos Manipulationsschutz

Wenn die Option **Deinstallation erlaubt** in einer für den Endpoint-Computer gültigen Richtlinie vom Typ **Spezifische Computereinstellungen** auf **Ja** oder **nicht konfiguriert** gesetzt ist, verhindert die Funktion Sophos Manipulationsschutz, dass Sophos SafeGuard leichtfertig deinstalliert wird.

**Hinweis:** Sophos Manipulationsschutz ist nur für Endpoint-Computer, auf denen Sophos Endpoint Security and Control in der Version 9.5 oder in einer neueren Version installiert ist, verwendbar.

Sie können die Funktion Sophos Manipulationsschutz in einer Richtlinie des Typs **Spezifische Computereinstellungen** aktivieren. Wenn das Feld **Deinstallation erlaubt** in einer solchen Richtlinie auf **Ja** oder **nicht konfiguriert** gesetzt ist, steht die Option **Sophos Manipulationsschutz aktivieren** zur Auswahl zur Verfügung.

Wenn Sie **Sophos Manipulationsschutz aktivieren** auf **Ja** setzen, wird jeder Versuch, Sophos SafeGuard zu installieren, explizit durch die Funktion Sophos Manipulationsschutz geprüft. Wenn die Funktion Sophos Manipulationsschutz die Deinstallation nicht erlaubt, wird der Vorgang abgebrochen.

Wenn Sie **Sophos Manipulationsschutz aktivieren** auf **Nein** setzen, wird die Deinstallation von Sophos SafeGuard nicht verhindert oder geprüft.

Wenn das Feld **Sophos Manipulationsschutz aktivieren** auf **nicht konfiguriert** eingestellt ist, gilt der Standardwert **Ja**.

## 24 Sophos SafeGuard aktualisieren

Die Aktualisierung von Sophos SafeGuard umfasst die folgenden Komponenten, die in der angegebenen Reihenfolge aktualisiert werden müssen:

1. Sophos SafeGuard Datenbank
2. SafeGuard Policy Editor
3. Durch Sophos SafeGuard geschützter Computer

Eine Aktualisierung auf Sophos SafeGuard 5.50 lässt sich direkt von SafeGuard Enterprise Standalone Version 5.35 oder einer neueren Version aktualisieren, ohne das dazu vorher definierte Einstellungen geändert werden. Wenn Sie eine Aktualisierung von einer älteren Version durchführen möchten, müssen Sie zunächst eine Aktualisierung auf Version 5.40 durchführen.

### 24.1 Datenbank aktualisieren

#### Voraussetzungen

- Eine Sophos SafeGuard Datenbank in der Version 5.35 oder höher (ehemaliger Produktname bis Version 5.40: SafeGuard Enterprise Standalone) muss installiert sein. Ältere Versionen müssen zunächst auf Version 5.40 aktualisiert werden.
- Die auszuführenden SQL-Skripte müssen auf dem Datenbank-Rechner vorhanden sein.
- Für die erfolgreiche Aktualisierung auf die neueste Version muss .NET Framework 3.0 Service Pack 1 installiert sein.
- Sie benötigen Windows Administratorenrechte.
- Führen Sie ein Backup der Datenbank durch, bevor Sie mit der Aktualisierung beginnen.

Im Tools-Verzeichnis Ihrer Software-Lieferung finden Sie mehrere SQL-Skripte für die Aktualisierung der Datenbank.

So aktualisieren Sie die Datenbank:

1. Schließen Sie den SafeGuard Policy Editor.
2. Um die SQL-Skripts ausführen zu können, stellen Sie die Datenbank auf den SINGLE\_USER-Modus um.

3. Die Datenbank muss Version für Version auf die aktuelle Version konvertiert werden. Starten Sie je nach installierter Version nacheinander die folgenden SQL-Skripte:
  - a) 5.35 > 5.40: MigrateSGN535\_SGN540.sql ausführen
  - b) 5.4x > 5.50: MigrateSGN540\_SGN550.sql ausführen
4. Stellen Sie relevante Datenbank wieder auf den MULTI\_USER-Modus zurück.

Nach Aktualisierung der Datenbank sind unter Umständen die kryptographischen Prüfsummen einiger Tabellen nicht mehr korrekt. Wenn Sie den SafeGuard Policy Editor starten, werden entsprechende Warnmeldungen angezeigt. Sie können die Tabellen dann in den entsprechenden Dialogen reparieren.

Die aktuelle Version der Sophos SafeGuard Datenbank ist dann einsatzbereit.

## 24.2 SafeGuard Policy Editor aktualisieren

### Voraussetzungen

- Ein SafeGuard Policy Editor in der Version 5.35 oder höher muss installiert sein. Ältere Versionen müssen zunächst auf Version 5.40 aktualisiert werden.
- Es ist keine Deinstallation des SafeGuard Policy Editor nötig.
- Die Aktualisierung der Sophos SafeGuard Datenbank auf die aktuelle Version wurde bereits durchgeführt.
- Für die erfolgreiche Aktualisierung auf die aktuelle Version muss .NET Framework 3.0 Service Pack 1 installiert sein. Die Software steht unter <http://www.microsoft.com/downloads> zum kostenlosen Download zur Verfügung.
- ASP.NET muss auf die Version 2.0 umgestellt sein.
- Sie benötigen Windows Administratorenrechte.

So aktualisieren Sie den SafeGuard Policy Editor:

1. Installieren Sie die neueste Version des SafeGuard Policy Editor Installationspakets. Nach der Installation müssen Sie den Konfigurationsassistenten nicht noch einmal ausführen.

Der SafeGuard Policy Editor wird auf die neueste Version aktualisiert.

## 24.3 Durch Sophos SafeGuard geschützte Computer aktualisieren

Der SafeGuard Policy Editor in der Version 5.50 kann durch Sophos SafeGuard geschützte Computer in der Version 5.35 oder höher verwalten.

### Voraussetzungen

- Version 5.35 oder eine höhere Version des SafeGuard Client Installationspakets muss installiert sein. Ältere Versionen müssen zunächst auf Version 5.40 aktualisiert werden.
- Die Aktualisierung der Sophos SafeGuard Datenbank und des SafeGuard Policy Editor wurde bereits durchgeführt.
- Sie benötigen Windows Administratorenrechte.

So aktualisieren Sie durch Sophos SafeGuard geschützte Computer:

1. Installieren Sie das vorbereitende MSI-Paket SGxClientPreinstall.msi, das den Endpoint-Computer mit den nötigen Voraussetzungen für eine erfolgreiche Installation der Verschlüsselungs-Software ausstattet, zum Beispiel mit den relevanten DLLs.

**Note:** Alternativ können Sie auch die Datei vcredist\_x86.exe installieren, die Sie hier herunterladen können:<http://www.microsoft.com/downloads/details.aspx?FamilyID=766a6af7-ec73-40ff-b072-9112bab119c2>oder sicherstellen, dass sich die DLL MSVCR80.dll in der Version 8.0.50727.4053 im Verzeichnis Windows\WinSxS auf dem Computer befindet.

2. Installieren Sie die neueste Version des entsprechenden Client-Installationspakets.

Der Windows Installer erkennt die bereits installierten Module und installiert nur diese Module neu. Ist die Power-on Authentication installiert, so steht nach einer erfolgreichen Installation auch ein aktualisierter POA-Kernel zur Verfügung (Richtlinien, Schlüssel usw.). Sophos SafeGuard wird auf dem Computer automatisch neu gestartet.

- Wenn sich die Sophos SafeGuard Konfiguration nicht geändert hat, müssen Sie kein neues Konfigurationspaket installieren. Aus Sicherheitsgründen empfehlen wir jedoch, alle veralteten und nicht mehr benutzten Konfigurationspakete zu löschen.
- Sie müssen nur dann ein neues Konfigurationspaket erstellen und neu installieren, wenn Änderungen an der Konfiguration vorgenommen wurden, z. B. wenn Richtlinieneinstellungen geändert wurden. Wenn Sie ein neues Sophos SafeGuard Konfigurationspaket erstellen, löschen Sie das veraltete Paket.

**Hinweis:** Wenn Sie versuchen, ein älteres Sophos SafeGuard Konfigurationspaket über ein neueres zu installieren, wird eine Fehlermeldung angezeigt.

## 24.4 Sophos SafeGuard mit volume-basierender Verschlüsselung ausstatten

**Hinweis:** Diese Beschreibung gilt nicht für Sophos SafeGuard mit ESDP (Endpoint Security and Data Protection).

Wenn Sie einen durch Sophos SafeGuard geschützten Computer, auf dem lediglich SafeGuard Data Exchange mit dateibasierender Verschlüsselung installiert ist, zu einem Sophos SafeGuard Client mit volume-basierender Verschlüsselung sowie SafeGuard Data Exchange mit dateibasierender Verschlüsselung erweitern möchten, müssen Sie die folgenden Schritte durchführen. Diese Schritte sind notwendig, um eine korrekte und sichere Anmeldung an der Power-on Authentication zu gewährleisten.

1. Deinstallieren Sie das SafeGuard Data Exchange Installationspaket (SGNClient\_withoutDE.msi/SGNClient\_withoutDE\_x64.msi).
2. Deinstallieren Sie das Sophos SafeGuard Konfigurationspaket.
3. Installieren Sie das Sophos SafeGuard Device Encryption Paket mit volume-basierender Verschlüsselung und wählen Sie die Features Device Encryption und Data Exchange aus (SGNClient.msi/SGNClient\_x64.msi).
4. Erzeugen Sie ein neues Sophos SafeGuard Konfigurationspaket und installieren Sie es auf dem Computer.

Die Schlüssel-Recovery-Datei sowie die lokalen Schlüssel, die während der Installation des Data Exchange Pakets erzeugt wurden, werden nicht gelöscht, sondern bleiben erhalten.

## 25 Migration von Sophos SafeGuard 5.5x auf SafeGuard Enterprise

Sophos SafeGuard 5.5x kann leicht auf die zentrale Management-Variante SafeGuard Enterprise erweitert werden, um den vollen Funktionsumfang von SafeGuard Enterprise nutzen zu können.

Dazu müssen Sie die folgenden Schritte durchführen:

- Der SafeGuard Policy Editor muss auf das SafeGuard Management Center migriert werden.
- Die mit Sophos SafeGuard verschlüsselten Endpoint-Computer müssen auf durch SafeGuard Enterprise geschützte Computer migriert werden.

### 25.1 SafeGuard Policy Editor auf SafeGuard Management Center migrieren

Sie können den SafeGuard Policy Editor auf das SafeGuard Management Center migrieren, um umfassende Management-Features zu nutzen, zum Beispiel Benutzer- und Computerverwaltung oder Protokollierung.

#### **Voraussetzungen**

- Sie müssen den SafeGuard Policy Editor nicht deinstallieren.
- Richten Sie vor der Migration den SafeGuard Enterprise Server ein.

#### **SafeGuard Policy Editor migrieren**

Für die Migration installieren Sie einfach das SGNManagementCenter.msi Paket auf dem Computer, auf dem der SafeGuard Policy Editor eingerichtet ist.

1. Starten Sie SGNManagementCenter.msi aus dem Installationsordner Ihrer Software-Lieferung.
2. Klicken Sie im Willkommen-Fenster auf **Weiter**.
3. Akzeptieren Sie die Lizenzvereinbarung.
4. Wählen Sie einen Installationspfad.
5. Bestätigen Sie die erfolgreiche Installation.

6. Starten Sie Ihren ggf. Computer neu.
7. Führen Sie die Konfiguration des SafeGuard Management Centers durch.

Der SafeGuard Policy Editor wurde auf das SafeGuard Management Center migriert.

## 25.2 Sophos SafeGuard Konfigurationen auf SafeGuard Enterprise migrieren

Sie können eine Sophos SafeGuard Konfiguration eines Endpoint-Computers auf eine SafeGuard Enterprise Konfiguration migrieren. Die Computer werden dann im SafeGuard Management Center zu Objekten, die verwaltet werden können und eine Verbindung zum SafeGuard Enterprise Server haben.

**Hinweis:** Der umgekehrte Weg, die Migration von einer SafeGuard Enterprise Konfiguration zu einer Sophos SafeGuard Konfiguration ist nicht zu empfehlen. Dies erfordert eine komplette Neuinstallation der Sophos SafeGuard Verschlüsselungs-Software auf dem Endpoint-Computer.

### Voraussetzungen

- Der SafeGuard Policy Editor muss bereits auf das SafeGuard Management Center migriert worden sein.
- Es ist keine Deinstallation der Sophos SafeGuard Verschlüsselungssoftware auf dem Endpoint-Computer nötig.
- Führen Sie ein Backup des Endpoint-Computers durch, bevor Sie die Migration starten.
- Sie benötigen Windows Administratorenrechte.

### Sophos SafeGuard Konfigurationen auf SafeGuard Enterprise migrieren

Für die Migration müssen Sie lediglich ein anderes Konfigurationspaket im SafeGuard Management Center erzeugen und es den entsprechenden Computern zuweisen.

1. Erstellen Sie im SafeGuard Management Center unter **Extras > Konfigurationspakete > Konfigurationspaket (Managed) erstellen** das Konfigurationspaket für den SafeGuard Enterprise Client (managed).
2. Weisen Sie dieses Paket den Sophos SafeGuard Endpoint-Computern über eine Gruppenrichtlinie zu.

Bei der Migration werden alle Benutzer und Zertifikate gelöscht und die Power-on Authentication deaktiviert, da die Benutzer-Computer-Zuordnung nicht migriert wird. Nach der Migration sind die Endpoint-Computer damit ungeschützt!

3. Führen Sie deshalb nach der Migration zwei Neustarts durch: Die erste Anmeldung erfolgt noch über Autologon. Den Benutzern werden neue Schlüssel und Zertifikate zugewiesen, so dass sie sich erst beim zweiten Neustart an der Power-on Authentication anmelden können. Erst nach dem zweiten Neustart sind die Computer wieder geschützt.

Die Sophos SafeGuard Konfiguration auf dem Endpoint-Computer ist nun eine SafeGuard Enterprise Konfiguration.

## **26 Migration SafeGuard Easy 4.x/Sophos SafeGuard Disk Encryption 4.x auf Sophos SafeGuard 5.5x**

SafeGuard Easy von Version 4.5x sowie Sophos SafeGuard Disk Encryption Version 4.60 können direkt auf Sophos SafeGuard 5.50 migriert werden, indem einfach das SafeGuard Device Encryption Client-Installationspaket auf dem Computer installiert wird.

Die direkte Migration wurde getestet und wird unterstützt für SafeGuard Easy ab Version 4.5x. Eine direkte Migration sollte auch für Versionen zwischen 4.3x und 4.4x funktionieren. Für ältere Versionen wird die direkte Migration nicht unterstützt. Versionen vor 4.3x müssen zunächst auf SafeGuard Easy 4.50 aktualisiert werden.

Die Verschlüsselung von Festplatten bleibt bestehen. Diese müssen nicht entschlüsselt und neu verschlüsselt werden, und SafeGuard Easy oder Sophos SafeGuard Disk Encryption muss auch nicht manuell deinstalliert werden.

Dieses Kapitel beschreibt, wie Sie eine Migration auf Sophos SafeGuard durchführen und zeigt, welche Features migriert werden können und welche Einschränkungen bestehen.

## 26.1 Voraussetzungen

Folgende Voraussetzungen müssen erfüllt sein:

- Die direkte Migration wurde getestet und wird unterstützt für SafeGuard Easy ab Version 4.5x. Eine direkte Migration sollte auch für Versionen zwischen 4.3x und 4.4x funktionieren. Für ältere Versionen wird die direkte Migration nicht unterstützt. Versionen vor 4.3x müssen zunächst auf SafeGuard Easy 4.50 aktualisiert werden.
- Die direkte Migration wird unterstützt für Sophos SafeGuard Disk Encryption Version 4.6x.
- SafeGuard Easy/Sophos SafeGuard Disk Encryption muss auf folgendem Windows Betriebssystem laufen:
  - Windows XP Professional Workstation Service Pack 2, 3
- Windows Installer Version 3.01 oder höher muss installiert sein.
- Die Hardware muss mit den Systemvoraussetzungen für Sophos SafeGuard 5.50 übereinstimmen.
- Wenn Sie spezifische Software (z. B. Lenovo-Middleware) verwenden, so muss diese mit den Systemvoraussetzungen für Sophos SafeGuard 5.50 übereinstimmen.
- Festplatten müssen mit den folgenden Algorithmen verschlüsselt sein, um migriert werden zu können: AES128, AES256, 3DES, IDEA.

### 26.1.1 Einschränkungen

Folgende Einschränkungen bestehen für die Migration:

- Es kann nur das SafeGuard Device Encryption Installationspaket mit dem Standard-Funktionsumfang installiert werden (SGNClient.msi/SDEClient.msi). Wenn zusätzlich das Modul SafeGuard Data Exchange installiert werden soll, muss dies in einem separaten Schritt erfolgen. (Beachten Sie, dass SafeGuard Data Exchange mit ESDP nicht unterstützt wird.)

Das Installationspaket ohne volume-basierende Verschlüsselung (SGNClient\_withoutDE.msi) wird für die Migration auf Sophos SafeGuard nicht unterstützt.

- Die folgenden Installationen können nicht auf Sophos SafeGuard migriert werden. In diesen Fällen sollten Sie nicht versuchen, Sophos SafeGuard zu installieren.

**Hinweis:** Wenn Sie in den nachfolgend genannten Fällen eine Migration vornehmen, erhalten Sie eine Fehlermeldung (Fehlernummer 5006).

- Twin Boot Installationen
- Installationen mit aktivem Compaq Switch
- Lenovo Computrace Installationen

- Festplatten, die nur teilweise verschlüsselt sind, z. B. nur mit Verschlüsselung des Boot-Sektors
  - Festplatten mit versteckten Partitionen
  - Festplatten, die mit einem der folgenden Algorithmen verschlüsselt sind: XOR, STEALTH, DES, RIJNDAEL, Blowfish-8, Blowfish-16
  - Multi-Boot Szenarien mit einer zweiten Windows- oder Linux-Partition
- Wechselmedien, die mit eine der folgenden Algorithmen verschlüsselt sind, können nicht migriert werden: XOR, STEALTH, DES, RIJNDAEL, Blowfish-8, Blowfish-16.

**Hinweis:** Es besteht die Gefahr von Datenverlust, wenn ein Wechselmedium mit einem der Algorithmen XOR, STEALTH, DES, RIJNDAEL, Blowfish-8, Blowfish-16 in SafeGuard Easy verschlüsselt wurde. Die Daten auf dem Wechselmedium können nach der Migration mit Sophos SafeGuard nicht mehr gelesen werden!

- Wechselmedien mit Super Floppy-Volumen können nach der Migration nicht umgewandelt werden.
- Wechselmedien können in das Sophos SafeGuard Format konvertiert werden. Nach der Konvertierung kann ein verschlüsselter Datenträger nur noch mit Sophos SafeGuard und nur auf dem Endpoint-Computer gelesen werden, an dem die Konvertierung durchgeführt wurde.

**Hinweis:** Verschlüsselung und Migration von Wechselmedien ist für ESDP nicht verfügbar.

## 26.2 Welche Funktionalität wird migriert

Die folgende Tabelle zeigt, welche Funktionalität migriert wird und wie diese in Sophos SafeGuard abgebildet wird.

SafeGuard Easy/Sophos SafeGuard Disk Encryption	Migration	Sophos SafeGuard
Verschlüsselte Festplatten	Ja	Die Festplatten sind durch die Sophos SafeGuard Power-on Authentication geschützt. Der Festplattenschlüssel ist somit zu keiner Zeit exponiert. Wenn der Modus "Boot Protection" gewählt wurde, muss die bisherige SafeGuard Easy Version deinstalliert werden. Der Verschlüsselungsalgorithmus der Festplatte wird bei der Migration nicht verändert. Daher kann sich der tatsächliche Algorithmus einer solchen migrierten Festplatte von der allgemeinen Sophos SafeGuard Richtlinie unterscheiden.
Verschlüsselte Wechselmedien (gilt nicht für Sophos SafeGuard Disk Encryption mitESDP)	Ja	Verschlüsselte Datenträger, z.B. USB-Sticks, können in das Sophos SafeGuard Format konvertiert werden. Hinweis: Nach der Konvertierung kann ein verschlüsselter Datenträger nur noch mit Sophos SafeGuard und nur auf dem Endpoint-Computer gelesen werden, an dem die Konvertierung durchgeführt wurde. Die Konvertierung muss jeweils bestätigt werden
Verschlüsselungsalgorithmen	Teilweise	Die für die Migration geeigneten Algorithmen AES128, AES256, 3DES, IDEA werden migriert. AES-128 and 3-DES stehen jedoch nicht im SafeGuard Policy Editor für neu zu verschlüsselnde Medien zur Auswahl.
Challenge/Response	Teilweise	Das Challenge/Response-Verfahren bleibt erhalten.

SafeGuard Easy/Sophos SafeGuard Disk Encryption	Migration	Sophos SafeGuard
Benutzername	Nein	Da in Sophos SafeGuard die Windows-Benutzernamen verwendet werden, ist eine Übernahme der SafeGuard Easy/Sophos SafeGuard Disk Encryption Benutzernamen nicht nötig. Die Registrierung der migrierten Computer erfolgt deshalb wie bei einer Neuinstallation von Sophos SafeGuard: durch zentrales Zuweisen oder lokales Registrieren der Computer-Benutzer. <b>Hinweis:</b> Nach der Migration wird der erste Benutzer, der sich an Windows anmeldet, als primärer Benutzer innerhalb der POA definiert (es sei denn, der Benutzer ist auf einer Service Account Liste aufgeführt).
Benutzerkennwörter	Nein	Da die Windows Kennwörter in Sophos SafeGuard verwendet werden, müssen die SafeGuard Easy/Sophos Disk Encryption Kennwörter nicht übernommen werden. SafeGuard Easy/Sophos Disk Encryption Kennwörter werden deshalb nicht migriert.
Richtlinien, Einstellungen (z. B. Mindestpasswortlänge)	Nein	Zur Sicherstellung der Konsistenz der gesamten Einstellungen ist eine automatische Übernahme nicht vorgesehen. Die Einstellungen müssen im SafeGuard Policy Editor neu gesetzt werden.
Pre-Boot Authentication	Nein	Die Pre-Boot Authentication (PBA) wird durch die Sophos SafeGuard Power-on Authentication (POA) ersetzt.
Installationen ohne GINA	Ja	Installationen ohne GINA werden zu Sophos SafeGuard mit installierter SGNGINA migriert.
Token/Smartcards	Nein	Die Authentisierung mit Token/Smartcards wird in Sophos SafeGuard nicht unterstützt. Wenn Sie Token/Smartcards verwenden möchten, empfehlen wir, auf SafeGuard Enterprise zu migrieren.
Anmeldung mit Lenovo Fingerabdruck-Leser	Teilweise <b>Hinweis:</b> Die Anmeldung mit Fingerabdruck ist mit ESDP nicht verfügbar.	Die Anmeldung per Fingerabdruck kann in SafeGuard Enterprise weiterhin benutzt werden. Die Hardware sowie die Software für den Fingerabdruck-Leser muss von SafeGuard Enterprise unterstützt werden. Außerdem müssen die Benutzerdaten erneut ausgerollt werden. Weitere Informationen zur Anmeldung per Fingerabdruck finden Sie in der Benutzerhilfe.

## 26.3 Vorbereitungen für die Migration

Folgende Maßnahmen sollten Sie treffen, bevor Sie die Installation von Sophos SafeGuard starten:

- Erzeugen Sie vor der Migration der Endpoint-Computer ein Sophos SafeGuard Konfigurationspaket im SafeGuard Policy Editor. Verteilen Sie dieses Konfigurationspaket nach der Installation der Verschlüsselungssoftware an die Endpoint-Computer. Die mit dem ersten Konfigurationspaket übertragenen Richtlinien müssen der früheren Konfiguration von SafeGuard Easy/Sophos SafeGuard Disk Encryption Computern entsprechen.

Wenn mit der Migration kein Konfigurationspaket übertragen wird, bleiben alle mit SafeGuard Easy/Sophos SafeGuard Disk Encryption verschlüsselten Volumes weiterhin verschlüsselt.

- Erstellen Sie zum Schutz vor Datenverlust ein komplettes Backup der zu migrierenden Computer.
- Führen Sie die vor der Installation empfohlenen Schritte durch, siehe [Installation vorbereiten](#), Seite 16, verwenden Sie z.B. chkdsk“ und „defrag“. Details zu „chkdsk“ und „defrag“ finden Sie in unserer Wissensdatenbank:
  - chdsk: <http://www.sophos.de/support/knowledgebase/article/107081.html>
  - defrag: <http://www.sophos.de/support/knowledgebase/article/109226.html>
- Erstellen Sie einen gültigen Kernel-Backup und legen Sie diesen an einem Speicherort ab, auf den immer zugegriffen werden kann, zum Beispiel ein Netzwerkpfad. Für weitere Informationen siehe die SafeGuard Easy 4.5x/Sophos SafeGuard Disk Encryption 4.60 Handbücher/Hilfe, Kapitel *Notfallmedien erstellen und Systemkern sichern*.
- Legen Sie bei der ersten Migration zur Sicherheit eine Testumgebung an.
- Migrieren Sie ältere Versionen von SafeGuard Easy zuerst auf die Version 4.50.
- Lassen Sie die Computer während des gesamten Migrationsprozesses eingeschaltet.
- Der Sicherheitsbeauftragte sollte die Windows-Anmeldeinformationen der Benutzer bereithalten, falls diese nach der erfolgreichen Migration ihre Windows-Kennwörter vergessen haben. Dieser Fall kann eintreten, wenn die Benutzer sich früher an der Pre-Boot Authentisierung angemeldet haben und eventuell zu einem späteren Zeitpunkt über das Windows Secure Autologon (SAL) angemeldet wurden. Die Benutzer haben daher ihre Windows Anmeldeinformationen nie benutzt.

**Hinweis:** Benutzern muss vor der Migration ein Kennwort zur Windows-Anmeldung bekannt sein. Dies ist wichtig, da ein Windows-Kennwort nicht nachträglich nach der Migration und Installation von Sophos SafeGuard gesetzt werden kann. Wenn die Benutzer Ihr Windows-Kennwort nicht kennen, weil Sie sich über SAL in SafeGuard Easy/Sophos SafeGuard Disk Encryption angemeldet haben, können sie sich an Sophos SafeGuard nicht anmelden. Die automatische Anmeldung an Windows wird in diesem Fall abgewiesen und die Benutzer können sich nicht mehr an Sophos SafeGuard anmelden. Es besteht die Gefahr des Datenverlusts, da Benutzer nicht in der Lage sind, auf ihre Computer zuzugreifen.

## 26.4 Migration starten

**Hinweis:** Die Installation kann auf einem laufenden SafeGuard Easy/Sophos Disk Encryption System durchgeführt werden. Verschlüsselte Festplatten oder Wechselmedien müssen nicht vorab entschlüsselt werden.

**Hinweis:** Benutzen Sie das SafeGuard Device Encryption Client-Paket (SGNClient.msi/SDEClient.msi) aus dem Installationsverzeichnis mit dem Standard-Funktionsumfang. Das Client-Paket SGNClient\_withoutDE.msi kann nicht verwendet werden. Für eine erfolgreiche Migration sollte die Installation am besten zentral im unbeaufsichtigten Modus erfolgen. Die lokale Installation über das Setup-Verzeichnis wird nicht empfohlen!

Gehen Sie folgendemmaßen vor:

1. Doppelklicken Sie im SafeGuard Easy/Sophos SafeGuard Disk Encryption Programmordner des zu migrierenden Computers auf WIZLDR.exe. Der Migrationsassistent wird gestartet.
2. Geben Sie im Migrationsassistenten das SYSTEM-Kennwort ein und bestätigen Sie mit **Weiter**. Bestätigen Sie in **Zielordner** die Standardeinstellung mit **Weiter** und klicken Sie auf **Beenden**, um die Aktion abzuschließen. Die Migrations-Konfigurationsdatei SGEMIG.cfg wird erzeugt.
3. Benennen Sie diese Datei im Windows Explorer von SGEMIG.cfg in SGE2SGN.cfg um.  
**Hinweis:** "Ersteller / Besitzer"-Rechte müssen für diese Datei und den Dateipfad gesetzt sein, auf dem sie während der Migration gespeichert wird. Andernfalls schlägt die Migration fehl und eine Meldung wird ausgegeben, dass SGE2SGN.cfg nicht gefunden werden konnte.
4. Geben Sie das Kommando "msiexec" in der Eingabeaufforderung ein, um das vorbereitende Installationspaket sowie das Sophos SafeGuard Installationspaket mit der Verschlüsselungssoftware auf dem SafeGuard Easy/Sophos SafeGuard Disk Encryption Computer auszuführen. Fügen Sie den Parameter MIGFILE mit dem Pfad der Migrationsdatei SGE2SGN.cfg hinzu:

**Beispiel:**

```
msiexec /i \\Distributionserver\Software\Sophos\SafeGuard\SGxClientPreinstall.msi
```

```
msiexec /i \\Distributionserver\Software\Sophos\SafeGuard\SDEClient.msi
```

```
/L*VX“\Distributionserver\Software\Sophos\SafeGuard\%Computername%.log“
```

```
MIGFILE=\\Distributionserver\Software\Sophos\SafeGuard\SGE2SGN.cfg
```

- Wenn die Migration erfolgreich durchgeführt wurde, kann Sophos SafeGuard auf dem Computer benutzt werden.
- Schlägt die Migration fehl, kann SafeGuard Easy/Sophos SafeGuard Disk Encryption immer noch auf dem Computer benutzt werden. In diesem Fall wird Sophos SafeGuard automatisch entfernt.

## 26.5 Migrierte Endpoint-Computer konfigurieren

Die Endpoint-Computer werden initial über Konfigurationspakete konfiguriert, die zum Beispiel die Power-on Authentication aktivieren.

Während der Migration sollten daher zuerst das vorbereitende Installationspaket und das Installationspaket mit der Verschlüsselungssoftware installiert werden. Erst wenn die POA aktiviert wurde und der Benutzer sich erfolgreich an Windows angemeldet hat, sollte die Konfiguration des Computers erfolgen.

1. Erstellen Sie das erste Konfigurationspaket im SafeGuard Policy Editor über **Extras > Konfigurationspakete** mit den entsprechenden Richtlinien-Einstellungen.
2. Installieren Sie das Konfigurationspaket auf den Endpoint-Computern.

**Hinweis:** Die mit dem ersten Sophos SafeGuard Konfigurationspaket übertragenen Richtlinien müssen der früheren Konfiguration des SafeGuard Easy/Sophos SafeGuard Disk Encryption Computers entsprechen.

## 26.6 Nach der Migration

Nach erfolgreicher Migration steht Ihnen in Sophos SafeGuard nach der Anmeldung an der Power-on Authentication folgendes zur Verfügung:

- die Schlüssel und Algorithmen der verschlüsselten Festplatten
- die Schlüssel und Algorithmen für verschlüsselte Wechselmedien (dies gilt nur für eine Migration von SafeGuard Easy).

Verschlüsselte Volumes bleiben verschlüsselt und die Verschlüsselungsschlüssel werden automatisch in ein Sophos SafeGuard kompatibles Format konvertiert.

**Hinweis:** Um in der Lage zu sein, die Festplatte zu entschlüsseln und Schlüssel für die Festplattenverschlüsselung hinzuzufügen und zu entfernen, muss der Benutzer zunächst den Computer neu starten.

Die Richtlinien sollten im SafeGuard Policy Editor entsprechend der früheren SafeGuard Easy/Sophos SafeGuard Disk Encryption Konfiguration der Computer neu gesetzt werden.

### 26.6.1 Wechselmedienmigration

**Hinweis:** Die Wechselmedienmigration gilt nicht für Sophos SafeGuard Disk Encryption mit ESDP.

Verschlüsselte Wechselmedien bleiben verschlüsselt. Die Schlüssel müssen jedoch in ein mit Sophos SafeGuard kompatibles Format konvertiert werden.

**Hinweis:** Deshalb kann ein verschlüsseltes Wechselmedium nach der Konvertierung nur mit Sophos SafeGuard gelesen werden und nur an dem Endpoint-Computer, an dem es während der Migration konvertiert wurde!

Um Wechselmedien zu entschlüsseln oder Schlüssel für Wechselmedien hinzuzufügen oder zu entfernen, muss der Benutzer zunächst das Wechselmedium vom Computer entfernen und es danach wieder mit dem Computer verbinden.

Wenn der Benutzer nach der Migration auf Wechselmedien zugreift, muss er aktiv die Umwandlung der Verschlüsselungsschlüssel in ein Sophos SafeGuard kompatibles Format bestätigen. Um die Umwandlung überhaupt erst zu initiieren, muss auf dem Computer die entsprechende Richtlinie für volume-basierende Verschlüsselung vorliegen. Ansonsten findet die Formatumwandlung nicht statt.

Der Benutzer wird aufgefordert, die Umwandlung für alle Wechselmedien zu bestätigen. Eine entsprechende Meldung wird angezeigt.

- Bestätigt der Benutzer die Umwandlung, so ist der Zugriff auf die migrierten Daten in vollem Umfang möglich.
- Lehnt der Benutzer die Umwandlung ab, lassen sich die migrierten Daten noch zum Lesen und Schreiben öffnen.

Neu hinzukommende Wechselmedien werden wie bei jedem Sophos SafeGuard Computer verschlüsselt, wenn die entsprechende Richtlinie am Endpoint-Computer vorliegt.

## 27 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](mailto: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.

## **28 Copyright**

Copyright © 1996 - 2010 Sophos Group und Utimaco Safeware AG. Alle Rechte vorbehalten.

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.

Sophos ist ein eingetragenes Warenzeichen von Sophos Plc und der Sophos Group. SafeGuard ist ein eingetragenes Warenzeichen von Utimaco Safeware AG - a member of the Sophos Group. Alle anderen erwähnten Produkt- und Unternehmensnamen sind Warenzeichen oder eingetragene Warenzeichen der jeweiligen Inhaber.

Alle SafeGuard Produkte unterliegen dem Urheberrecht der Utimaco Safeware AG - a member of the Sophos Group, oder, sofern anwendbar, ihrer Lizenzinhaber. Alle weiteren Sophos Produkte unterliegen dem Urheberrecht der Sophos Plc oder, sofern anwendbar, ihrer Lizenzinhaber.

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