

SOPHOS

Sophos SafeGuard Disk Encryption 5.50 Sophos SafeGuard Easy 5.50 Startup-Anleitung

Stand: April 2010



Inhalt

1	Einleitung	2
2	Über Sophos SafeGuard	3
3	Migration von Sophos SafeGuard Disk Encryption 4.60	6
4	Migration von SafeGuard Easy Version 4.x	7
5	Installationsschritte.....	8
6	Überprüfen der Systemanforderungen	9
7	Vorbereiten der Installation	11
8	Installieren des SafeGuard Policy Editor	14
9	Erstkonfiguration durchführen.....	15
10	Zusätzliche Konfiguration der Verschlüsselungssoftware durchführen.....	17
11	Konfigurieren des administrativen Zugangs zu Endpoint-Computern.....	28
12	Installieren der Verschlüsselungssoftware und der Verschlüsselungskonfiguration auf den Endpoint-Computern.....	31
13	Recovery-Vorgänge bei vergessenem Kennwort.....	37
14	Wiederherstellen des Zugriffs auf das System.....	40
15	Hilfe bei häufig vorkommenden Aufgaben.....	43
16	Technischer Support.....	44
17	Copyright	45

1 Einleitung

In dieser Anleitung wird beschrieben, wie Sie Sophos SafeGuard einrichten, um die Computer in Ihrem Unternehmen vor unberechtigtem Zugriff zu schützen.

Diese Anleitung gilt für folgende Produkte:

- Sophos SafeGuard Disk Encryption (SDE) 5.50, verfügbar im Bundle mit Endpoint Security and Data Protection (ESDP).
- Sophos SafeGuard Easy (SGE) 5.50. Ab Version 5.50 ist SGE der neue Produktname für die SafeGuard Enterprise Standalone-Lösung.

Wenn sich Features oder Einstellungen für die beiden Produkte voneinander unterscheiden, so wird dies in der Anleitung an den entsprechenden Stellen explizit angegeben.

Zusätzliche Informationen finden Sie in den Dokumenten “Sophos SafeGuard Administrator-Hilfe” und “Sophos SafeGuard Benutzerhilfe”, die zusätzlich zur vorliegenden Startup-Anleitung zur Verfügung stehen.

2 Über Sophos SafeGuard

Sophos SafeGuard verschlüsselt Daten transparent. Die Benutzer müssen somit nicht entscheiden, welche Daten verschlüsselt werden und bemerken den Entschlüsselungsvorgang nicht. Die Sophos SafeGuard Verschlüsselung verhindert effektiv, dass Daten von nicht autorisierten Personen gelesen oder geändert werden. Sie lässt sich auch nicht dadurch umgehen, dass die Daten über externe Speichermedien in ein anderes System eingebracht werden.

Sophos SafeGuard bietet folgende Vorteile

- Benutzerfreundlicher und effektiver Schutz der Vertraulichkeit von Daten
- Schnelle Implementation
- Sophos SafeGuard basiert auf marktführender Verschlüsselungstechnologie (FIPS 140 zertifiziert)

Bei durch Sophos SafeGuard geschützten Computern wird vor dem Betriebssystem die SafeGuard Power-on Authentication (POA) gestartet.



Die POA bietet benutzerfreundlich und sicherheitsrelevante Features wie zum Beispiel:

- Manipulationsschutz für Sophos SafeGuard Disk Encryption
- Anmeldeverzögerungen bei falscher Eingabe
- Anpassbare, Windows-entsprechende Benutzeroberfläche
- Durchgehende Anmeldung an Windows
- Unterstützung mehrere Sprachen sowie Unicode-Unterstützung

2.1 Bequemer Zugang für IT-Aufgaben

Zur Unterstützung bei der Durchführung von IT-Aufgaben auf den Endpoint-Computern bietet Sophos SafeGuard folgende Features:

- Die Power-on Authentication lässt sich zur Benutzung mit Wake-on LAN konfigurieren. Dies erleichtert zum Beispiel die Verwaltung von Patches.
- Mit Service Accounts können sich Mitglieder des IT-Teams zur Durchführung von IT-Aufgaben nach der Installation an Endpoint-Computern anmelden, ohne die Power-on Authentication zu aktivieren.
- Mit POA Access Accounts können sich Mitglieder des IT-Teams zur Durchführung von administrativen Aufgaben an verschlüsselten Endpoint-Computern anmelden, nachdem die Power-on Authentication aktiviert wurde.

2.2 Sophos SafeGuard Recovery-Szenarien

Für Recovery-Vorgänge bietet Sophos SafeGuard verschiedene Optionen, die auf unterschiedliche Recovery-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.

■ **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.

■ **System-Recovery**

Sophos SafeGuard bietet verschiedene Methoden und Tools für System-Recovery-Vorgänge, z. B. ein Sophos SafeGuard angepasstes Windows PE sowie Lenovo Rescue and Recovery. Probleme mit dem Windows-System und Sophos SafeGuard Komponenten lassen sich mit diesen Tools beheben.

■ **Schlüssel-Recovery-Datei**

Recovery-Vorgänge über Challenge/Response sowie System-Recovery-Vorgänge basieren auf einer Schlüssel-Recovery-Datei. Diese Datei wird für jeden mit Sophos SafeGuard verschlüsselten Computer erzeugt und in der Regel in einer Netzwerkfreigabe abgelegt. Der Recovery-Schlüssel stellt sicher, dass der Recovery-Vorgang nicht zur Umgehung des Schutzes der Daten zweckentfremdet wird und ist zur zusätzlichen Sicherheit verschlüsselt. Die Netzwerkfreigabe sowie die erforderlichen Zugriffsrechte werden während der Erstkonfiguration automatisch angelegt.

3 Migration von Sophos SafeGuard Disk Encryption 4.60

Sophos SafeGuard Disk Encryption (SDE) 5.50 bietet signifikante Funktionserweiterungen. Unter anderem wird die Verschlüsselung von Computern mit Windows Vista und Windows 7 (32 und 64 Bit) unterstützt.

Computer, die mit SDE 4.60 verschlüsselt wurden, können auf SDE 5.50 migriert werden. Verschlüsselte Volumes bleiben verschlüsselt und die Verschlüsselungsschlüssel werden automatisch in ein Format konvertiert, das mit Version 5.50 kompatibel ist.

Vor einer Migration der verschlüsselten Computer auf Sophos SafeGuard 5.50 sollten Sie ein neues Richtlinien-Konfigurationspaket (MSI) im SafeGuard Policy Editor erzeugen und es mit der Sophos SafeGuard 5.50 Software auf den Endpoint-Computern installieren.

Für weitere Informationen siehe die Sophos SafeGuard Administrator-Hilfe, Kapitel *Migration SafeGuard Easy 4.x/ Sophos SafeGuard Disk Encryption 4.x auf Sophos SafeGuard 5.5x* bzw. <http://www.sophos.com/support/knowledgebase/article/108561.html>.

4 Migration von SafeGuard Easy Version 4.x

SafeGuard Easy (SGE) 5.50 bietet signifikante Funktionserweiterungen. Unter anderem wird die Verschlüsselung von Computern mit Windows Vista und Windows 7 (32 und 64 Bit) unterstützt.

Computer, die mit SGE 4.3x bis 4.5x verschlüsselt wurden, können auf SDE 5.x migriert werden. Verschlüsselte Volumes bleiben verschlüsselt und die Verschlüsselungsschlüssel werden automatisch in ein Format konvertiert, das mit Version 5.50 kompatibel ist.

Für SDE 5.50 wird mit dem SafeGuard Policy Editor außerdem ein neues Administrations-Tool verwendet, das in Bezug auf SDE 4.x nicht rückwärts kompatibel ist. Vor einer Migration der verschlüsselten Computer auf Sophos SafeGuard 5.50 sollten Sie ein neues Konfigurationspaket im SafeGuard Policy Editor erzeugen und es mit der Sophos SafeGuard 5.50 Software auf den Endpoint-Computern installieren.

Für weitere Informationen siehe die Sophos SafeGuard Administrator-Hilfe, Kapitel *Migration SafeGuard Easy 4.x/ Sophos SafeGuard Disk Encryption 4.x auf Sophos SafeGuard 5.5x* bzw. <http://www.sophos.com/support/knowledgebase/article/108561.html>.

5 Installationsschritte

Wir empfehlen, Sophos SafeGuard Disk Encryption auf einem Windows Server zu installieren und die Verschlüsselungssoftware dann über ein Software Deployment Tool, z. B. Microsoft System Center Configuration Manager, auf den Endpoint-Computern zu installieren und einzurichten. Wichtige Schritte:

- Überprüfen der Systemanforderungen.
- Vorbereiten der Installation.
- Installieren des SafeGuard Policy Editor, der für die Richtlinienkonfiguration sowie für die Durchführung von Helpdesk-Aufgaben verwendet wird.
- Erstkonfiguration durchführen.
- Zusätzliche Konfiguration der Verschlüsselungssoftware durchführen.
- Installieren der Verschlüsselungssoftware und der Verschlüsselungskonfiguration auf den Endpoint-Computern.

6 Überprüfen der Systemanforderungen

6.1 Anforderungen für das Administrations-Tool

Hardware

- Intel oder AMD X86 CPU
- 1 GB RAM
- 1 GB freier Festplattenspeicher (empfohlen)

Software

Die 32 und 64 Bit Versionen der folgenden Betriebssysteme werden unterstützt, falls nicht anders angegeben. Neueste Service Packs werden empfohlen:

- Microsoft Windows XP Professional (32 Bit)
- Microsoft Windows 2003 Server
- Microsoft Windows 2003 Server R2
- Microsoft Windows Vista
- Microsoft Windows 2008 Server
- Microsoft Windows 2008 Server R2
- Microsoft Windows 7

Microsoft ASP.net: .NET Framework 3.0 SP1

6.2 Anforderungen für die Datenbank

Die folgenden 32 und 64 Bit Versionen werden unterstützt:

- Microsoft SQL Server 2005 SP2, SP3
- Microsoft SQL Server 2005 Express SP2, SP3
- Microsoft SQL Server 2008
- Microsoft SQL Server 2008 Express

6.3 Anforderungen für durch Sophos SafeGuard geschützte Computer

Hardware

- Intel oder AMD X86 CPU
- 512 MB RAM (Minimum), 1024 MB (empfohlen für Windows Vista)
- Für die Installation werden mindestens 300 MB freier Festplattenspeicherplatz benötigt. Davon müssen mindestens 100 MB einen zusammenhängenden Bereich bilden. Wenn Ihnen weniger als 5 GB Festplattenspeicherplatz zur Verfügung stehen und Ihr Betriebssystem nicht neu installiert ist, führen Sie bitte eine Defragmentierung durch. Dadurch erhöhen Sie die Chancen, dass der benötigte zusammenhängende Bereich verfügbar ist. Andernfalls kann die Installation fehlschlagen, weil nicht genügend freier zusammenhängender Speicherplatz vorhanden ist. Eine Installation kann in diesem Fall nicht unterstützt werden.

Software

Die 32 und 64 Bit Versionen der folgenden Betriebssysteme werden unterstützt, falls nicht anders angegeben. Neueste Service Packs werden empfohlen:

- Microsoft Windows XP Professional (nur 32 Bit)
- Microsoft Windows Vista Enterprise, Ultimate, Business oder Home Premium. (Vista ohne SP1 wird nicht unterstützt.)
- Microsoft Windows 7

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.
- Dynamic- und 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.

7 Vorbereiten der Installation

Vor der Installation von Sophos SafeGuard empfehlen wir die folgenden vorbereitenden Maßnahmen.

7.1 Allgemeine Überlegungen

- Wenn Sie Sophos SafeGuard über einen zentralen Rollout-Vorgang installieren möchten, empfehlen wir die Konfiguration einer Service Account-Liste. Ein IT-Administrator, der zu einer Service Account-Liste hinzugefügt wurde, kann sich nach der Installation von Sophos SafeGuard an Computern anmelden, ohne die Power-on Authentication zu aktivieren. Ein solches Vorgehen ist empfehlenswert, da normalerweise der erste Benutzer, der sich nach der Installation an einem Endpoint-Computer anmeldet, als primäres Benutzerkonto zur POA hinzugefügt wird. Für weitere Informationen, siehe [Konfigurieren von Service Account Listen](#), Seite 28.
- Einen zentralen Rollout-Vorgang können Sie mit Hilfe einer Vielzahl an System Management/Deployment Tools durchführen, z. B. mit Microsoft SCCM/SMS, IBM Tivoli und Enteo Netinstall.
- Entscheiden Sie, ob die mit Sophos SafeGuard gelieferte, empfohlene Standardrichtlinienkonfiguration verwendet werden soll. Für eine Übersicht über die Standardrichtlinien, siehe [Zusätzliche Konfiguration der Verschlüsselungssoftware durchführen](#), Seite 17. Eine detaillierte Beschreibung der Standardrichtlinien finden Sie in der Administrator-Hilfe (Kapitel *Standardrichtlinien*).
- Wenn Sie Wake-On-LAN einsetzen möchten, müssen Sie dies zuvor über eine Richtlinie des Typs **Spezifische Computereinstellungen** konfigurieren. Weitere Informationen finden Sie in der Administrator-Hilfe (Kapitel *Richtlinieneinstellungen*).
- Sophos SafeGuard kann so konfiguriert werden, dass Protokolle zur Verschlüsselung/Installation auf dem Netzwerk (UNC-Pfad) gespeichert werden. Somit kann der Administrator den Verschlüsselungsprozess von zentraler Stelle aus überprüfen. Für weitere Informationen siehe [Installieren der Verschlüsselungssoftware und der Verschlüsselungskonfiguration über Skript](#), Seite 34.

7.2 Allgemeine Vorbereitungen

- Um die Verschlüsselungssoftware zu installieren und die Sophos SafeGuard Administrations-Tools zu bedienen, benötigen Sie Windows-Administratorenrechte.
- Lesen Sie die Release Notes aufmerksam durch.

7.3 Vorbereiten der Computer für die Verschlüsselung

- Auf dem Computer muss ein Benutzerkonto eingerichtet und aktiv sein. Der Benutzer muss ein Kennwort haben.
- Schließen Sie alle geöffneten Applikationen.
- Stellen Sie sicher, dass genügend Festplattenspeicher frei ist.
- Erstellen Sie einen kompletten Backup der Daten auf dem Computer.
- Sophos stellt eine Liste für die Hardware-Konfiguration zur Verfügung, um Konflikte zwischen der POA und Ihrer Computerhardware zu vermeiden. Die Liste ist im Installationspaket der Verschlüsselungssoftware enthalten.

Wir empfehlen, vor jeder größeren Installation von Sophos SafeGuard jeweils die aktualisierte Version dieser Hardware-Konfigurationsdatei zu installieren. Die Datei wird monatlich aktualisiert und steht unter <ftp://POACFG:POACFG@ftp.ou.utimaco.de> zum Download zur Verfügung.

Weitere Informationen finden Sie in der Administrator-Hilfe (Kapitel *In der Power-on Authentication unterstützte Hotkeys*) sowie in unserer Wissensdatenbank: <http://www.sophos.com/support/knowledgebase/article/657000.html>.

- Untersuchen Sie die Festplatte(n) mit folgendem Kommando auf Fehler:

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

Sie werden eventuell dazu aufgefordert, den Computer neu zu starten und chkdsk erneut auszuführen. Weitere Informationen zu diesem Thema finden Sie in unserer Wissensdatenbank: <http://www.sophos.de/support/knowledgebase/article/107081.html>.

- Verwenden Sie das Windows-eigene „defrag“ Tool, um nach fragmentierten Boot-Dateien, Daten-Dateien und Ordner auf lokalen Volumes zu suchen und diese zu konsolidieren.

```
defrag %drive%
```

Weitere Informationen zu diesem Thema finden Sie in unserer Wissensdatenbank: <http://www.sophos.com/support/knowledgebase/article/109226.html>

- Deinstallieren Sie Third-Party Boot-Manager, z. B. „PRONetworks Boot Pro“ und „Boot-US“.
- Wenn Sie Image/Clone-Programme verwendet haben, wird empfohlen, den MBR „neu“ zu schreiben. Für die Installation von Sophos SafeGuard benötigen Sie einen sauberen, einwandfreien Master Boot Record. Möglicherweise ist der MBR aber durch den Einsatz von Image/Clone-Programmen nicht mehr in einwandfreiem, ursprünglichen Zustand.

Sie können den Master Boot Record säubern, indem Sie von einer Windows-CD booten und den Befehl FIXMBR innerhalb der Windows Recovery Console ausführen. Weitere Informationen hierzu finden Sie in unserer Wissensdatenbank:

<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. Hierbei ist es möglich, dass die Installation nicht beendet wird, 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.

8 Installieren des SafeGuard Policy Editor

Um die Verschlüsselungssoftware auf Endpoint-Computern einzurichten, installieren Sie zunächst den SafeGuard Policy Editor auf einem Windows Server. Danach können Sie ihn auf mehreren Administrator-Computern installieren, die alle mit der zentralen Sophos SafeGuard Datenbank auf dem Server verbunden sind. Der Zugriff auf die einzelnen SafeGuard Policy Editor Instanzen erfolgt jeweils über das gleiche Konto.

Voraussetzungen: .NET Framework 3.0 Service Pack 1 muss auf dem Windows Server installiert sein. Die Software steht unter <http://www.microsoft.com/downloads> kostenlos zum Download zur Verfügung.

1. Melden Sie sich an Ihrem Computer als Administrator an.
2. Installieren Sie eines der beiden folgenden Installationspakete aus dem Produktinstallationsordner. Ein Assistent führt Sie durch die notwendigen Schritte.

Sophos SafeGuard Disk Encryption	SafeGuard Easy
Doppelklicken Sie auf SDEPolicyEditor.msi.	Doppelklicken Sie auf SGNPolicyEditor.msi.

3. Übernehmen Sie in den folgenden Dialogen die Standardeinstellungen.

Datenbank-Installation: Zum Speichern der Sophos SafeGuard Richtlinieneinstellungen wird eine SQL Datenbankinstanz verwendet. Steht keine vorhandene SQL Datenbankinstanz zur Verfügung, so werden Sie während der SafeGuard Policy Editor Installation zur Installation von Microsoft SQL Server 2005 Express aufgefordert. In diesem Fall werden Ihre Windows-Anmeldedaten als SQL-Benutzerkonto verwendet.

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

Der SafeGuard Policy Editor ist installiert. Im nächsten Schritt führen Sie die Erstkonfiguration im SafeGuard Policy Editor durch.

9 Erstkonfiguration durchführen

Um die Erstkonfiguration mit dem SafeGuard Policy Editor durchzuführen, benötigen Sie Windows-Administratorenrechte.

1. Starten Sie den SafeGuard Policy Editor. Der Konfigurationsassistent wird geöffnet. Er führt Sie durch die notwendigen Schritte.
2. Bestätigen Sie die **Willkommen**-Seite mit **Weiter**.
3. Auf der **Datenbank**-Seite wird die SQL-Datenbank-Instanz angezeigt, die während der Installation des SafeGuard Policy Editor ausgewählt oder erstellt wurde. Bestätigen Sie die Standardeinstellungen mit **Weiter**. Die Datenbank wird angelegt.
4. Auf der **Sicherheitsbeauftragter**-Seite wird bereits der Name des Sicherheitsbeauftragten angezeigt. Geben Sie ein Kennwort ein und bestätigen Sie es. Dieses Kennwort benötigen Sie, um auf den SafeGuard Policy Editor zuzugreifen. Bestätigen Sie die Standardeinstellungen mit **Weiter**. Das Zertifikat für den Sicherheitsbeauftragten wird automatisch erstellt.

Bewahren Sie das Kennwort an einem sicheren Ort auf. Wenn Sie es verlieren, können Sie nicht mehr auf den SafeGuard Policy Editor zugreifen. Für Recovery-Vorgänge muss für den IT-Helpdesk Zugriff auf das Konto bestehen.

Sophos SafeGuard Disk Encryption	SafeGuard Easy
Der Name des Sicherheitsbeauftragten lautet immer Administrator.	Der aktuelle Benutzername wird angezeigt.

5. Geben Sie auf der **Unternehmen**-Seite einen **Unternehmensnamen** ein. Bestätigen Sie die Standardeinstellung mit **Weiter**. Das Unternehmenszertifikat wird automatisch erstellt.
Bei einer erneuten Installation können Sie das Zertifikat auch importieren.
6. Bestätigen Sie auf der **Zertifikats-Backup**-Seite die Standardeinstellungen mit **Weiter**.
Stellen Sie sicher, dass die Zertifikate unmittelbar nach der Erstkonfiguration an einen Speicherort exportiert werden, auf den für Recovery-Vorgänge Zugriff besteht (z. B. USB-Stick). Bewahren Sie die Zertifikate an einem sicheren Ort auf. Sie benötigen Sie zum Reparieren einer beschädigten Installation oder einer korrupten Datenbank. Weitere Informationen finden Sie in der Administrator-Hilfe.
7. Bestätigen Sie auf der **Standardrichtlinie**-Seite die Standardeinstellungen mit **Weiter**. Es werden empfohlene Standardrichtlinien sowie ein Konfigurationspaket (standard-packet.msi) mit diesen Standardrichtlinien erstellt.

Die empfohlenen Standardrichtlinien umfassen u. a. die Verschlüsselung von internen Festplatten-Volumes, die Aktivierung der Power-on Authentication sowie Einstellungen, die lokale und Remote-Recovery-Vorgänge ermöglichen. Für weitere Details, siehe [Zusätzliche Konfiguration der Verschlüsselungssoftware durchführen](#), Seite 17 sowie die Administrator-Hilfe (Kapitel *Standardrichtlinien*). Die Standardrichtlinien können nur während der Erstkonfiguration im SafeGuard Policy Editor Konfigurationsassistenten erstellt werden. Je nach Anforderung können Sie die Standardrichtlinien später ändern oder neue, benutzerdefinierte Richtlinien erstellen.

8. Übernehmen Sie auf der **Recovery-Schlüssel**-Seite die Standardeinstellung **Netzwerkfreigabe anlegen**.

Dadurch werden die Netzwerkfreigabe SafeGuardRecoveryKeys\$ sowie ein Verzeichnis auf dem Server oder dem lokalen Computer angelegt, in dem die Recovery-Schlüssel automatisch gespeichert werden. Der Helpdesk erhält die notwendigen Zugriffsrechte auf die Recovery-Netzwerkfreigabe. Wird **Netzwerkfreigabe anlegen** nicht aktiviert, so werden die Endbenutzer nach Abschluss der Verschlüsselung dazu aufgefordert, einen Speicherort für die Recovery-Schlüssel-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.

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

Die Erstkonfiguration ist nun abgeschlossen. Sie haben ein Konfigurationspaket mit Standardrichtlinien sowie eine Netzwerkfreigabe für Recovery-Schlüssel mit den notwendigen Zugriffsrechten für den Helpdesk erstellt. Wir empfehlen, vor der Installation von Sophos SafeGuard sowie der Standardrichtlinien-Konfiguration auf den Endpoint-Computern zunächst die verbleibenden Kapitel dieser Startup-Anleitung zu lesen. Für weitere Informationen zur Installation auf den Endpoint-Computern, siehe [Installieren der Verschlüsselungssoftware und der Verschlüsselungskonfiguration über Skript](#), Seite 34.

10 Zusätzliche Konfiguration der Verschlüsselungssoftware durchführen

Die Sophos SafeGuard Richtlinien enthalten alle Einstellungen, um eine unternehmensweite Sicherheitsrichtlinie auf den Endpoint-Computern zu implementieren. Sie enthalten Einstellungen für die folgenden Bereiche (Richtlinientypen):

Richtlineintyp	Inhalt	SDE	SGE
Allgemeine Einstellungen	Einstellungen für Recovery für die Anmeldung, POA-Anpassung usw.	✓	✓
Authentisierung	Einstellungen für Anmeldemodus, Anzahl der Anmeldeversuche usw.	✓	✓
Kennwörter	Einstellungen für Benutzerkennwörter, zum Beispiel Länge, unzulässige Zeichen.	✓	✓
Geräteschutz	Einstellungen für Verschlüsselung, zum Beispiel Auswahl des Volumens	Einstellungen für volume-basierende Verschlüsselung	Einstellungen für volume-basierende und dateibasierende Verschlüsselung, SafeGuardData Exchange und SafeGuard Portable
Spezifische Computereinstellungen	Einstellungen für die Computer, zum Beispiel Power-on Authentication (aktivieren/deaktivieren), Secure Wake On LAN, Anzeigeoptionen	✓	✓
Protokollierung	Legt fest, welche Ereignisse protokolliert werden.	✓	✓
Passphrasen	Einstellungen für SafeGuardData Exchange Passphrasen		✓

Mit den Standardkonfigurationsrichtlinien sind Ihre Endpoint-Computer gut geschützt:

- Die Power-on Authentication ist aktiviert.
- Die volume-basierende Verschlüsselung für alle internen Festplatten ist aktiviert.
- Recovery über Local Self Help im Fall eines vergessenen Kennworts ist aktiviert und konfiguriert.
- Darüber hinaus ist Kennwort-Recovery über Challenge/Response mit Unterstützung des Helpdesks aktiviert.
- Die benötigte Schlüssel-Recovery-Datei wird automatisch auf jedem durch Sophos SafeGuard geschützten Computer erzeugt und während der Erstkonfiguration in einer Netzwerkfreigabe gespeichert. Die notwendigen Zugangsberechtigungen für diese Netzwerkfreigabe werden standardmäßig eingestellt.
- Für SafeGuard Easy 5.50: Die dateibasierende Verschlüsselung von Wechselmedien ist aktiviert.

Die Standardkonfiguration deckt nicht die folgenden Bereiche ab, die Sie vor der Installation in Betracht ziehen sollten:

- Um den Zugang zu Endpoint-Computern für administrative Aufgaben und Aufgaben nach der Installation zu ermöglichen bzw. zu vereinfachen, definieren Sie administrative Zugangsoptionen: Service Accounts und POA Access Accounts.
- Definieren Sie erweiterte Einstellungen, erstellen Sie z. B. eigene, spezifische Fragen für Local Self Help.
- Erstellen Sie spezielle Dateien (virtuelle Clients) für Daten-Recovery-Vorgänge im Fall einer beschädigten POA. Diese Dateien sind für ein Challenge/Response-Verfahren über eine WinPE-Umgebung erforderlich.
- Passen Sie die Power-on Authentication an die spezifischen Anforderungen in Ihrem Unternehmen an.

10.1 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 Richtlinienengruppe 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.

10.2 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-Volume) angelegt werden. Weisen sie auf verschiedene Ziele werden sie addiert.

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

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

10.3 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.

10.4 Konfigurieren der 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. Um sich anzumelden, müssen Benutzer lediglich eine bestimmte Anzahl an vordefinierten Fragen in der Power-on Authentication beantworten. Sie können die zu beantwortenden Fragen im SafeGuard Policy Editor definieren. Darüber hinaus steht auch ein vordefiniertes Fragenthema zur Verfügung. Sie können die Benutzer auch dazu berechtigen, eigene Fragen zu definieren.

Hinweis: Local Self Help ist bereits in den Standardrichtlinien mit vordefinierten Fragen konfiguriert. Wenn Sie die Standardrichtlinien benutzen, müssen Sie die folgenden Konfigurationsschritte nicht ausführen.

So konfigurieren Sie spezielle Einstellungen für Local Self Help:

1. Klicken Sie im Navigationsbereich des SafeGuard Policy Editor auf **Richtlinien**.

2. Erstellen Sie eine neue Richtlinie des Typs **Allgemeine Einstellungen**.

3. Definieren Sie die Einstellungen für Local Self Help unter **Local Self Help (LSH)**:
 - a) Wählen Sie im Feld **Local Self Help aktivieren** die Einstellung **Ja**.
 - b) Legen Sie im Feld **Minimale Länge der Antworten** die Mindestanzahl an Zeichen fest, die der Benutzer bei der ersten Beantwortung der Fragen eingeben muss.
 - c) Im Feld **Willkommenstext unter Windows** können Sie einen individuellen Informationstext angeben, der beim Starten des Local Self Help Assistenten auf dem Endpoint-Computer im ersten Dialog angezeigt werden soll. Dieser Text muss zuvor erstellt und registriert werden. Detaillierte Informationen zum Erstellen und Registrieren von Informationstexten finden Sie in der Administrator-Hilfe unter *Willkommenstexte registrieren*.
 - d) Um die Benutzer dazu zu berechtigen, eigene Fragen zu definieren, wählen Sie im Feld **Benutzer dürfen eigene Fragen festlegen** die Einstellung **Ja**.

Nach der Festlegung der Richtlinieneinstellungen für die Freischaltung von Local Self Help auf den Endpoint-Computern, definieren Sie nun ein Fragenthema, das mit der Richtlinie übertragen wird.

Im **Richtlinien**-Navigationsbereich steht unter **Local Help Fragen** ein vordefiniertes Fragenthema zur Verfügung. Sie können dieses Fragenthema unverändert verwenden, es bearbeiten oder löschen. Die folgenden Schritte beschreiben, wie Sie ein neues Fragenthema anlegen und Fragen hinzufügen.

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

Eine neue Fragenzeile wird hinzugefügt.

9. Geben Sie Ihre Frage ein und drücken Sie **Enter**. Um weitere Fragen hinzuzufügen, wiederholen Sie diesen Vorgang.
Das Fragenthema muss mindestens 10 Fragen enthalten.

10. 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 freigeschaltet wird, automatisch mitgegeben.

11. Fügen Sie die Richtlinie zu einer Richtliniengruppe hinzu, die mit dem Konfigurationspaket auf den Endpoint-Computern wirksam werden soll.

Die Richtliniengruppe mit der Richtlinie vom Typ **Allgemeine Einstellungen** steht beim Erstellen eines Konfigurationspakets (über **Extras > Konfigurationspakete**), das auf den Endpoint-Computern installiert werden soll, zur Auswahl zur Verfügung. Damit die Benutzer Local Self Help nutzen können, müssen sie die Funktion zunächst durch die Beantwortung von mindestens zehn Fragen aktivieren (siehe [Aktivieren der Funktion Local Self Help auf dem Endpoint-Computer](#), Seite 24).

10.4.1 Aktivieren der Funktion Local Self Help auf dem Endpoint-Computer

Um die Funktion Local Self Help auf dem Endpoint-Computer für die Benutzung zu aktivieren, müssen die Benutzer mindestens 10 Fragen beantworten und speichern.

1. Nach dem Wirksamwerden der Richtlinie auf dem Endpoint-Computer wird ein Balloon Tool Tip angezeigt, der den Benutzer darauf hinweist, dass unbeantwortete Local Self Help Fragen vorliegen. Der Benutzer startet den Computer neu.

Der Befehl **Local Self Help** wird zum Kontextmenü des System Tray Icon in der Windows-Taskleiste hinzugefügt.

2. Der Benutzer klickt mit der rechten Maustaste auf das Sophos SafeGuard System Tray Icon und wählt **Local Self Help**.

Der **Willkommen**-Dialog des Local Self Help Assistenten wird angezeigt. Der Local Self Help Assistent führt den Benutzer durch die notwendigen Schritte für das Beantworten und Speichern der Fragen.

Nach Abschluss des Local Self Help Assistenten ist Local Self Help auf dem Computer aktiv.

10.5 Konfigurieren des Challenge/Response-Verfahrens für Daten-Recovery

Mit spezifischen Dateien, den virtuellen Clients, lassen sich auf einfache Art und Weise auch dann Recovery-Vorgänge für verschlüsselte Volumes durchführen, wenn ein Challenge-Response-Verfahren normalerweise nicht unterstützt würde (z. B. bei einer beschädigten POA). Virtuelle Clients können von verschiedenen Computern und für mehrere Challenge/Response-Verfahren verwendet werden.

Die virtuellen Clients müssen erstellt werden und dem Helpdesk vor der Durchführung des Challenge/Response-Verfahrens zur Verfügung stehen.

1. Markieren Sie im SafeGuard Policy Editor 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**. Virtuelle Clients werden in der Datenbank anhand dieses Namens identifiziert.
5. Klicken Sie auf das **Speichern**-Symbol in der Symbolleiste, um Ihre Änderungen in der Datenbank zu speichern.
6. Wählen Sie den entsprechenden virtuellen Client im Aktionsbereich aus und klicken Sie in der Symbolleiste auf **Virtuellen Client exportieren**. Wählen Sie einen Speicherort für die Datei des virtuellen Clients mit der Bezeichnung `recoverytoken.tok` aus und bestätigen Sie den Speicherort mit **OK**.

Der virtuelle Client wird in die Datei `recoverytoken.tok` exportiert.

7. Kopieren Sie die Datei `recoverytoken.tok` auf ein Wechselmedium. Wir empfehlen einen USB-Stick.

Bewahren Sie das Speichermedium an einem sicheren Ort auf. Stellen Sie die Dateien dem Helpdesk und in der Umgebung des Endpoint-Computers zur Verfügung. Sie werden für die Durchführung von Challenge/Response-Verfahren mit virtuellen Clients benötigt.

10.6 Anpassen der Power-on Authentication

Sie können die POA gemäß Ihren unternehmensspezifischen Anforderungen anpassen (z. B. Hintergrund-/Anmeldebild, Informationstext, Tastaturlayout, Sprache der Benutzeroberfläche). Erstellen Sie Bilder und Texte vorab und registrieren Sie diese im SafeGuard Policy Editor. Alle weiteren Konfigurationsschritte erfolgen über Richtlinien.

Die POA lässt sich wie folgt anpassen:

■ 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. Ihr Firmenlogo. Hintergrund- und Anmeldebilder werden über eine Richtlinie vom Typ **Allgemeine Einstellungen** konfiguriert.

Eine detaillierte Beschreibung hierzu finden Sie in der Administrator-Hilfe unter *Hintergrund- und Anmeldebild*.

■ Benutzerdefinierte Informationstexte

Sie können individuelle Informationstexte definieren, die in der POA angezeigt werden, zum Beispiel: Informationen, die beim Starten eines Challenge/Response-Verfahrens für Recovery-Vorgänge angezeigt werden, rechtliche Hinweise oder zusätzliche Informationen, die nach der Anmeldung an der POA angezeigt werden.

Je nach Typ werden diese Texte über Richtlinien der Typen **Allgemeine Einstellungen** und **Spezifische Computereinstellungen** konfiguriert.

Eine detaillierte Beschreibung hierzu finden Sie in der Administrator-Hilfe unter *Benutzerdefinierter Text in der POA*.

■ Sprache für die POA-Dialogtexte

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

Sie können die Sprache der POA-Dialogtexte über eine Richtlinie des Typs **Allgemeine Einstellungen** ändern.

Eine detaillierte Beschreibung hierzu finden Sie in der Administrator-Hilfe unter *Sprache der POA-Dialogtexte*.

■ **Tastaturlayout**

Sophos SafeGuard übernimmt als Standard das Tastaturlayout in die POA, das zum Zeitpunkt der Installation in den **Regions- und Sprachoptionen** von Windows gesetzt ist.

Sie können das Tastaturlayout über die **Regions- und Sprachoptionen** ändern.

Eine detaillierte Beschreibung hierzu finden Sie in der Administrator-Hilfe unter *Tastaturlayout*.

■ **Virtuelle Tastatur**

Sophos SafeGuard bietet eine virtuelle Tastatur für die Eingabe von Anmeldeinformationen durch Klicken auf die auf dem Bildschirm angezeigten Tasten.

Über eine Richtlinie des Typs **Spezifische Computereinstellungen** können Sie festlegen, ob die virtuelle Tastatur zur Verfügung stehen soll.

Eine detaillierte Beschreibung hierzu finden Sie in der Administrator-Hilfe unter *Virtuelle Tastatur*.

11 Konfigurieren des administrativen Zugangs zu Endpoint-Computern

Um den Zugang zu Endpoint-Computern für administrative Aufgaben nach der Installation zu ermöglichen bzw. zu vereinfachen, können Sie folgende administrative Zugangsoptionen definieren:

■ 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.

■ POA Access Accounts für die POA-Anmeldung

POA Access Accounts sind vordefinierte 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.

Detaillierte Beschreibungen dieser beiden Optionen finden Sie in der Sophos SafeGuard Administrator-Hilfe unter *Service Account Listen für die Windows-Anmeldung* und *POA Access Accounts für die POA-Anmeldung*.

11.1 Konfigurieren von Service Account Listen

Gehen Sie wie folgt vor:

1. Klicken Sie im Navigationsbereich des SafeGuard Policy Editor auf **Richtlinien**.
2. Markieren Sie im Richtlinien-Navigationsbereich den Eintrag **Service Account Listen**.
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.

9. Legen Sie eine Richtlinie vom Typ **Authentisierung** an.

10. Wählen Sie unter **Anmeldeoptionen**, die gewünschte Service Account Liste aus der Dropdownliste des Felds **Service Account Liste**.

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

12. Fügen Sie die Richtlinie zu der Richtliniengruppe hinzu, die mit dem Konfigurationspaket auf den Endpoint-Computern wirksam werden soll.

Die Richtliniengruppe mit der Richtlinie vom Typ **Authentisierung** steht beim Erstellen eines Konfigurationspakets (über **Extras > Konfigurationspakete**), das auf den Endpoint-Computern installiert werden soll, zur Auswahl zur Verfügung. Über diese Richtliniengruppe wird die Service Account Liste dem Endpoint-Computer zugewiesen.

11.2 Konfigurieren von POA Access Accounts

Gehen Sie wie folgt vor:

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

Hinweis: 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.

6. 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.

Wiederholen Sie diese Schritte, um weitere POA-Benutzer anzulegen.

In den nächsten Schritten legen Sie eine POA-Gruppe an, die bei der Erstellung von Konfigurationspaketen ausgewählt werden kann. Darüber hinaus fügen Sie die Benutzer zur Gruppe hinzu.

7. Wählen Sie im **Benutzer** Navigationsfenster unter **POA** den Knoten **POA-Gruppen**.

8. Klicken Sie im **POA-Gruppen** Kontextmenü auf **Neu > Neue Gruppe erstellen**.

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

9. Geben Sie im Feld **Vollständiger Name** einen Namen für die neue POA-Gruppe ein.

10. Klicken Sie auf **OK**.

11. Wählen Sie im **Benutzer** Navigationsfenster unter **POA, POA-Gruppe** die neue POA-Gruppe.

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

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

13. Wählen Sie den Benutzer (d. h. das POA Access Account), den Sie zur Gruppe hinzufügen möchten. Wiederholen Sie diesen Schritt, um weitere Benutzer hinzuzufügen.

Die POA-Gruppe steht beim Erstellen eines Konfigurationspakets (über **Extras > Konfigurationspakete**), das auf den Endpoint-Computern installiert werden soll, zur Auswahl zur Verfügung.

12 Installieren der Verschlüsselungssoftware und der Verschlüsselungskonfiguration auf den Endpoint-Computern

Gehen Sie wie folgt vor:

1. Bevor Sie die Verschlüsselungssoftware installieren, bereiten Sie den Endpoint-Computer für die Installation vor, siehe [Vorbereiten der Installation](#), Seite 11.
2. Um Sophos SafeGuard kennenzulernen, installieren Sie die Verschlüsselungssoftware zunächst auf einem Testcomputer.
3. Melden Sie sich zum ersten mal an.
4. Verwenden Sie dann Ihre eigenen Tools, um ein Installationspaket zu erstellen und zu verteilen. Dadurch richten Sie die Verschlüsselung zentral auf den Endpoint-Computern ein.

12.1 Durchführen einer Test-Installation

Bevor Sie die Verschlüsselungssoftware installieren, bereiten Sie den Endpoint-Computer für die Installation vor, siehe [Vorbereiten der Installation](#), Seite 11.

1. Melden Sie sich an dem Computer als Administrator an.
2. Installieren Sie das MSI-Paket SGxClientPreinstall.msi, das den Endpoint-Computer mit den notwendigen Voraussetzungen für eine erfolgreiche Installation der Verschlüsselungssoftware (z. B. den notwendigen DLLs) ausstattet.
3. Klicken Sie auf dem relevanten „Client“-MSI-Paket doppelt, um den Assistenten für die Installation der Verschlüsselungssoftware zu starten. Dieser führt Sie durch die notwendigen Schritte. Installieren Sie eine der folgenden Dateien:

Sophos SafeGuard Disk Encryption	SafeGuard Easy
SDEClient.msi für die 32-Bit-Variante oder SDEClient_x64.msi für die 64-Bit-Variante	SGNClient.msi für die 32-Bit-Variante oder SGNClient_x64.msi für die 64-Bit-Variante. Informationen zu weiteren Client-MSI-Paketen finden Sie in der Administrator-Hilfe unter <i>Installation</i> .

4. Übernehmen Sie in den folgenden Dialogen die Standardeinstellungen.
5. Wählen Sie den Installationstyp, wenn Sie dazu aufgefordert werden. Kunden, die SGNClient.msi oder SGNClient_x64.msi installieren, führen einen der beiden folgenden Handlungsschritte aus:
 - Wählen Sie **Vollständig**, um sowohl Device Protection (volume-basierende Verschlüsselung) als auch Data Exchange (dateibasierende Verschlüsselung) zu installieren.
 - Wählen Sie **Typisch**, um nur Device Protection zu installieren.
 - Wählen Sie **Angepasst** und aktivieren Sie die benötigten Features gemäß Ihren Anforderungen.

Das Feature **Data Exchange** steht mit SDE nicht zur Verfügung.

6. Übernehmen Sie in allen weiteren Dialogen die Standardeinstellungen, um den Installationsassistenten abzuschließen.
7. Wechseln Sie an den Speicherort des Standard-Konfigurationspakets (MSI), das sie während der Konfiguration des SafeGuard Policy Editor erstellt haben.
8. Installieren Sie dieses Konfigurationspaket auf dem Computer.

Sophos SafeGuard ist auf dem Endpoint-Computer installiert. Melden Sie sich nun zum ersten mal nach der Installation an dem Computer an.

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* in der Administrator-Hilfe sowie die folgenden Wissensdatenbank-Artikel:

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

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

12.2 Erste Anmeldung an den Endpoint Computer (ohne Service Account)

1. Starten Sie den Computer neu. Das Sophos SafeGuard Autologon-Fenster wird angezeigt. Danach wird der Windows-Anmeldedialog angezeigt.

Unter Windows Vista und Windows 7 müssen Sie zunächst die Tastenkombination STRG+ALT+ENTF (CTRL+ALT+DEL) drücken, um Autologon und Windows-Logon zu starten. Der Administrator kann diese Einstellungen in der MMC Konsole im Group Policy Object Editor unter Windows Settings > Security Settings > Local Policies > Deactivate Security Options (Interactive logon: CTRL+ ALT+ DEL not required) deaktivieren.
2. Geben Sie Ihren Windows-Benutzernamen und Ihr Kennwort ein.
3. Starten Sie den Computer nochmal neu. Die Sophos SafeGuard Power-on Authentication wird aktiviert.
4. Geben Sie Ihren Windows-Benutzernamen und Ihr Kennwort ein. Sie werden automatisch an Windows angemeldet.

Die Power-on Authentication ist nun aktiviert. Sie sind als Sophos SafeGuard-Benutzer registriert. Zur Bestätigung wird ein entsprechender Balloon Tool Tip angezeigt. Wenn Sie sich das nächste mal anmelden, müssen Sie nur Ihre Windows-Anmeldeinformationen in der Power-on Authentication eingeben.

Die Initialverschlüsselung startet automatisch. Bei Verwendung der Standardrichtlinien werden alle internen Festplatten verschlüsselt. Während der Verschlüsselung können Sie weiterhin mit dem Computer arbeiten. Nach Abschluss der Verschlüsselung ist kein Neustart notwendig. Die Ver- und Entschlüsselung zur Bearbeitung erfolgt transparent und ohne Benutzerinteraktion. Weitere Informationen zum Verhalten des Computers nach der Installation von Sophos SafeGuard finden Sie in der Benutzerhilfe in den Kapiteln *Erste Anmeldung nach der Installation von Sophos SafeGuard*, *Beispiel für die erste Anmeldung eines Benutzers an der POA* und *Datenverschlüsselung*.

12.3 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.

12.3.1 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).

12.4 Installieren der Verschlüsselungssoftware und der Verschlüsselungskonfiguration über Skript

Bereiten Sie vor der Installation der Verschlüsselungssoftware die Endpoint-Computer für die Installation vor, siehe [Vorbereiten der Installation](#), Seite 11.

Verwenden Sie Ihre eigenen Tools, um das Installationspaket zu erstellen, das auf den Endpoint-Computern installiert werden soll. Das Paket muss folgende Komponenten enthalten:

- **ein Skript mit einer Kommandozeile für die vorkonfigurierte Installation**

Wir empfehlen, das Windows Installer Kommandozeilen-Tool `msiexec.exe` zu verwenden, um das Skript zu erzeugen. Für weitere Informationen zu `msiexec` siehe die Administrator-Hilfe, Kapitel *Kommando für zentrale Installation* oder [http://msdn.microsoft.com/en-us/library/aa367988\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/aa367988(VS.85).aspx).

- **das vorbereitende Installationspaket von Sophos SafeGuard**

Verwenden Sie das Paket `SGxClientPreinstall.msi`. Das Paket stattet die Endpoint-Computer mit den notwendigen Voraussetzungen für eine erfolgreiche Installation der Verschlüsselungssoftware aus, z. B. mit der erforderlichen DLL `MSVCR80.dll` in der Version 8.0.50727.4053.

Hinweis: Wenn Sie dieses Paket nicht installieren, wird die Installation der Verschlüsselungssoftware abgebrochen.

- **das Installationspaket mit der Sophos SafeGuardVerschlüsselungssoftware**

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

- **Konfigurationspaket(e)**

Die zuvor im SafeGuard Policy Editor erzeugten Konfigurationspakete. Sie enthalten die Richtlinien mit der Verschlüsselungskonfiguration für die Endpoint-Computer. Verwenden Sie das Konfigurationspaket mit den vordefinierten Standardrichtlinien, um Richtlinien schnell und bequem auf den Computern umzusetzen. Sie können auch selbst erstellte Konfigurationspakete verwenden.

1. Legen Sie einen Ordner mit der Bezeichnung Software auf dem Administrator-Computer als zentralen Speicher für alle Applikationen an.
2. Um das Skript zu erstellen, geben Sie die Kommandos in der Eingabeaufforderung mit den Kommandozeilen-Parametern ein, wie im folgenden Beispiel gezeigt.

Skript-Beispiel:

```
msiexec /i F:\Software\Sophos\SafeGuard\SGxClientPreinstall.msi /qn
msiexec /i F:\Software\Sophos\SafeGuard\SDEClient.msi /qn
/L*VX G:\Temp\Sophos\SafeGuard%\%computername%\SDEClient_inst.log
InstallDir=C:\Program Files\Sophos\Sophos SafeGuard
```

```
■ msiexec /i F:\Software\Sophos\SafeGuard\SGxClientPreinstall.msi
msiexec /i F:\Software\Sophos\SafeGuard\SDEClient.msi
InstallDir=C:\Program Files\Sophos\Sophos SafeGuard
```

Installiert das vorbereitende Installationspaket und die Sophos SafeGuard Verschlüsselungssoftware aus dem angegebenen Speicherort in das Standardinstallationsverzeichnis C:\Program Files\Sophos\Sophos SafeGuard. Installiert Sophos SafeGuard Device Encryption (volume-basierende Verschlüsselung) und die Power-on Authentication.

```
■ msiexec /i F:\Software\Sophos\SafeGuard\SDEClientConfig.msi
```

Installiert das Sophos SafeGuard Konfigurationspaket aus dem angegebenen Speicherort in das Standardinstallationsverzeichnis.

```
■ /L*VX G:\Temp\Sophos%\%computername%\SDEClient_inst.log
```

Protokolliert alle Warnungs- und Fehlermeldungen in der angegebenen Protokolldatei auf dem Netzwerk und erstellt eine aussagekräftige Protokolldatei, die sich mit wilogutl.exe automatisch analysieren lässt.

```
■ /qn
```

Installiert ohne Benutzerinteraktion und zeigt keine Benutzeroberfläche an.

3. Verteilen Sie die Installations- und Konfigurationspakete über Software-Verteilungsmechanismen an die Endpoint-Computer.

Die Verschlüsselungssoftware und das/die Konfigurationspaket(e) werden auf den Endpoint-Computern installiert und die Computer werden verschlüsselt.

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* in der Administrator-Hilfe sowie den folgenden Wissensdatenbank-Artikel:

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

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

13 Recovery-Vorgänge bei vergessenem Kennwort

Sollte ein Benutzer sein Kennwort vergessen haben, so gibt es zwei verschiedene Möglichkeiten:

- Der Benutzer kann das Kennwort selbst über Local Self Help wiederherstellen (diese Möglichkeit wird empfohlen).
- Das Helpdesk stellt das Kennwort über ein Challenge/Response-Verfahren wieder her.

13.1 Wiederherstellen eines Kennworts über Local Self Help

1. Der Benutzer gibt seinen Benutzernamen in der Power-on Authentication auf dem Endpoint-Computer ein.

Die Schaltfläche **Recovery** wird aktiv.

2. Der Benutzer klickt auf **Recovery**.
 - Ist auf dem Endpoint-Computer nur Local Self Help für Recovery-Vorgänge, die die Anmeldung betreffen aktiviert, wird Local Self Help gestartet.
 - Stehen sowohl Local Self Help als auch Challenge/Response für Recovery-Vorgänge zur Verfügung, so wird ein Dialog mit beiden Recovery-Methoden zur Auswahl angezeigt. Der Benutzer klickt auf **Local Self Help**.

Der Willkommen-Dialog von Local Self Help wird angezeigt.

3. In den folgenden fünf Dialogen beantwortet der Benutzer fünf Fragen, die per Zufallsprinzip aus den auf dem Endpoint-Computer gespeicherten Fragen ausgewählt werden. Nach Beantwortung der letzten Frage bestätigt der Benutzer mit **OK**.
4. Im nächsten Dialog kann sich der Benutzer sein Kennwort anzeigen lassen, indem er Enter oder die Leertaste drückt, oder auf die blaue Anzeigebox klickt.

Das Kennwort wird für maximal 5 Sekunden angezeigt. Danach wird der Boot-Vorgang automatisch fortgesetzt. Der Benutzer kann sein Kennwort sofort verbergen, indem er Enter oder die Leertaste drückt, oder auf die blaue Anzeigebox klickt.

5. Wenn der Benutzer das Kennwort gelesen hat, klickt er auf **OK**.

Der Benutzer wird an der Power-on Authentication und an Windows angemeldet und kann das Kennwort für zukünftige Anmeldevorgänge verwenden.

13.2 Wiederherstellen eines Kennworts über Challenge/Response

Voraussetzungen:

Die Schlüssel-Recovery-Datei, die für jeden Endpoint-Computer während der Installation der Sophos SafeGuard Verschlüsselungssoftware erstellt wird, muss für den Helpdesk zugänglich sein. Außerdem muss der Name der Datei bekannt sein. Der Helpdesk benötigt die relevanten Berechtigungen zur Durchführung von Recovery-Vorgängen. Challenge/Response muss per Richtlinie für den Endpoint-Computer aktiviert sein.

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. Dadurch lässt sich das Zurücksetzen des Kennworts vermeiden. Auch ist in diesem Fall keine Unterstützung durch den Helpdesk notwendig.

1. Der Benutzer gibt seinen Benutzernamen in der Power-on Authentication auf dem Endpoint-Computer ein. Die Schaltfläche **Recovery** wird aktiv.
2. Der Benutzer klickt auf **Recovery**.
 - Wenn nur Challenge/Response für Recovery-Vorgänge, die die Anmeldung betreffen, aktiviert ist, wird Challenge/Response automatisch gestartet.
 - Wenn sowohl Challenge/Response als auch Local Self Help verfügbar sind, wählt der Benutzer **Challenge/Response**.

Ein Dialog wird angezeigt, der den Namen der erforderlichen Schlüssel-Recovery-Datei angibt.

3. Der Benutzer klickt auf **Weiter**. Ein zufallsgenerierter Challenge-Code wird angezeigt.
4. Der Benutzer kontaktiert den Helpdesk und übermittelt den Namen der erforderlichen Recovery-Datei sowie den Challenge-Code.
5. Der Helpdesk startet den Recovery-Assistenten im SafeGuard Policy Editor.
6. Der Helpdesk wählt einen Recovery-Vorgang des Typs **Sophos SafeGuard Client**, bestätigt den Schlüssel sowie den Challenge-Code und wählt die erforderliche Recovery-Aktion **Ohne Benutzeranmeldung booten**.

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

7. Der Helpdesk übermittelt den Response-Code per Telefon oder Text-Mitteilung an den Benutzer.

8. Der Benutzer klickt auf dem Endpoint-Computer im Challenge/Response Assistenten auf **Weiter** und gibt den erhaltenen Response-Code ein. Der Computer wird durch die Power-on Authentication bis zur Windows-Ebene gebootet.
9. 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. 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
10. 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.
11. 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.
12. 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.
13. 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.

Der Benutzer kann wieder mit dem Computer arbeiten.

14 Wiederherstellen des Zugriffs auf das System

Sophos SafeGuard bietet eine Reihe von Recovery-Optionen für kritische Situationen, z. B. wenn die POA beschädigt ist und der Benutzer nicht mehr auf die verschlüsselten Daten zugreifen kann, oder wenn der Master Boot Record beschädigt ist.

14.1 Daten-Recovery über Challenge/Response mit virtuellen Clients

Daten-Recovery mit virtuellen Clients basiert auf einem Challenge/Response-Verfahren. Dieser Recovery-Typ kann angewendet werden, wenn unter speziellen Umständen das Betriebssystem nicht mehr gestartet werden kann. Ursache hierfür kann z. B. eine beschädigte Treiberkonfiguration sein.

In diesem Fall kann der Zugriff auf verschlüsselte Daten wiederhergestellt werden, indem der Computer über eine Windows PE Recovery Disk gestartet wird, die für Sophos SafeGuard angepasst ist. Darüber hinaus wird ein Challenge/Response-Verfahren mit virtuellen Clients gestartet. Weitere Informationen hierzu finden Sie in der Administrator-Hilfe unter *Systemwiederherstellung*.

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. Konfigurieren Sie den virtuellen Client im SafeGuard Policy Editor.
3. Booten Sie den Computer von der Recovery Disk.
4. Importieren Sie die Datei mit dem virtuellen Client in das KeyRecovery Tool.
5. Starten Sie die Challenge im KeyRecovery Tool.
6. Bestätigen Sie den virtuellen Client im SafeGuard Policy Editor.
7. Geben Sie den Challenge-Code im SafeGuard Policy Editor ein.
8. Generieren Sie den Response-Code im SafeGuard Policy Editor.
9. Geben Sie den Response-Code im KeyRecovery Tool ein.

Der Zugriff auf die Daten, die auf dieser Partition gespeichert sind, ist wiederhergestellt.

14.2 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.

14.3 Recovery bei einem Computer mit einem beschädigten Master Boot Record

Nach der Installation von Sophos SafeGuard auf dem Endpoint-Computer wird eine Kopie des Original Master Boot Record (MBR) gespeichert und im Systemkern des Computers abgelegt. Wenn der MBR beschädigt wird, kann dies zu einem nicht bootbaren System führen. Für Recovery-Vorgänge bei Systemen mit beschädigtem MBR bietet Sophos SafeGuard das Recovery Tool BE_Restore.exe. Hier haben Sie folgende Möglichkeiten:

- Wiederherstellen des MBR aus einer Sicherungskopie
- Reparieren des MBR

Eine detaillierte Beschreibung dieses Recovery-Typs finden Sie in der Sophos SafeGuard Tools-Anleitung unter *Wiederherstellen eines beschädigten MBR*.

15 Hilfe bei häufig vorkommenden Aufgaben

Dieser Abschnitt bietet eine Übersicht zu Informationsquellen für häufig vorkommende Aufgaben. Alle weiteren Informationen finden Sie in der Sophos SafeGuard Administrator-Hilfe oder Benutzerhilfe.

Aufgabe	Handbuch/Kapitel
Anmelden an den SafeGuard Policy Editor.	Administrator-Hilfe, Am SafeGuard Policy Editor anmelden
Anmelden an den durch Sophos SafeGuard geschützten Computer	Benutzerhilfe, Die Power-on Authentication
Sicherstellen der korrekten Funktionsweise der Power-on Authentication	Administrator-Hilfe/Benutzerhilfe, In der Power-on Authentication unterstützte Hotkeys.
Anzeigen von Sophos SafeGuard spezifischen Informationen auf dem Endpoint-Computer	Benutzerhilfe, System Tray Icon und Balloon-Ausgabe
Erstellen und Gruppieren von Richtlinien	Administrator-Hilfe, Mit Richtlinien arbeiten
Exportieren von Zertifikaten	Administrator-Hilfe, Unternehmenszertifikat und Master Security Officer Zertifikat exportieren
Erstellen eines administrativen Zugangs zu Endpoint-Computern	Administrator-Hilfe, Administrative Zugangsoptionen für Endpoint-Computer
Wiederherstellen eines Kennworts über Local Self Help	Administrator-Hilfe/Benutzerhilfe, Recovery über Local Self Help
Wiederherstellen eines Kennworts über Challenge/Response	Administrator-Hilfe/Benutzerhilfe, Recovery über Challenge/Response
Daten-Recovery auf Endpoint-Computern	Administrator-Hilfe, Challenge/Response mit virtuellen Clients
Wiederherstellen eines korrupten Master Boot Records	Tools-Anleitung, Wiederherstellen eines beschädigten MBR
Migrieren von SDE 4.60 oder SGE 4.2x - 4.5x auf Sophos SafeGuard	Administrator-Hilfe, Migration SafeGuard Easy 4.x/Sophos SafeGuard Disk Encryption 4.x auf Sophos SafeGuard 5.5x

16 Technischer Support

Technischen Support zu Sophos Produkten können Sie wie folgt abrufen:

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

17 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.