

Sophos SafeGuard Disk Encryption, Sophos SafeGuard Easy Startup-Anleitung

Produktversion: 5.60

Stand: April 2011



Inhalt

1	Einleitung.....	3
2	Über Sophos SafeGuard.....	4
3	Ist eine Migration von früheren Versionen möglich?.....	6
4	Was wird installiert?.....	7
5	Installationsschritte.....	8
6	Installation des SafeGuard Policy Editor.....	9
7	Durchführen der Erstkonfiguration.....	10
8	Kopieren der Standardrichtlinie zur Bearbeitung.....	12
9	Konfigurieren der Endpoint-Computer für Service-Tasks nach der Installation.	13
10	Veröffentlichen der bearbeiteten Richtlinie in einem Konfigurationspaket.....	14
11	Installation der Verschlüsselungssoftware und des Konfigurationspakets auf den Endpoint-Computern.....	15
12	Recovery-Vorgänge bei vergessenem Kennwort.....	22
13	Hilfe bei häufig vorkommenden Aufgaben.....	25
14	Technischer Support.....	26
15	Rechtliche Hinweise.....	27

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) 5.6x, verfügbar im Bundle mit Endpoint Security and Data Protection (ESDP).
- Sophos SafeGuard Easy (SGE) 5.6x. 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 angegeben.

Weitere Informationen finden Sie auch in der SDE/SGE Administrator-Hilfe und in der SDE/SGE Benutzerhilfe.

2 Über Sophos SafeGuard

Sophos SafeGuard verschlüsselt Daten transparent. Die Benutzer müssen nicht entscheiden, welche Daten verschlüsselt werden sollen. Verschlüsselung und Entschlüsselung werden im Hintergrund ausgeführt. 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

- schnelle Implementation
- Schutz der Vertraulichkeit von Daten
- Verschlüsselung von Daten mit einer Technologie, die FIPS 140 entspricht.

Bei durch Sophos SafeGuard geschützten Computern wird vor dem Betriebssystem in der Pre-Boot-Phase des Computers die SafeGuard Power-on Authentication (POA) gestartet. Erst wenn sich der Benutzer korrekt authentisiert hat, wird das Betriebssystem gestartet und der Benutzer wird an Windows angemeldet.



Die POA bietet benutzerfreundliche 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 mehrerer Sprachen sowie Unicode-Unterstützung

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.

Sophos SafeGuard Recovery-Szenarien

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

■ Recovery für die Anmeldung mit Local Self Help

Mit Local Self Help können sich Benutzer, die ihr Kennwort vergessen haben, ohne Unterstützung durch einen Helpdesk 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 mit Challenge/Response

Für das Challenge/Response Recovery-Verfahren ist die Unterstützung durch einen Helpdesk erforderlich. Das Verfahren hilft Benutzern, die sich nicht an ihrem Computer anmelden oder nicht 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 einen 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.

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 zum Speichern dieser Dateien sowie die erforderlichen Zugriffsrechte werden während der Erstkonfiguration automatisch angelegt.

3 Ist eine Migration von früheren Versionen möglich?

Sophos SafeGuard 5.6x bietet signifikante Funktionserweiterungen.

■ Migration von Version 5.5x:

Computer, die bereits mit SDE 5.5x oder SGE 5.5x verschlüsselt wurden, können auf Version 5.6x migriert werden.

■ Migration von Version 4.x:

Computer, die mit SDE 4.6x oder SGE 4.3x bis 4.5x verschlüsselt wurden, können auf Sophos SafeGuard 5.6x migriert werden.

Ab Version 5.5x wird für Sophos SafeGuard außerdem ein neues Administrations-Tool, der SafeGuard Policy Editor, verwendet, das in Bezug auf SDE 4.x oder SGE 4.x nicht rückwärts-kompatibel ist. Verschlüsselte Volumes bleiben verschlüsselt und die Verschlüsselungsschlüssel werden in ein Format konvertiert, das mit Version 5.5x kompatibel ist.

Für Sophos SafeGuard 5.6x ist eine gültige Lizenzdatei erforderlich, die in den SafeGuard Policy Editor importiert werden muss. Sie erhalten diese Datei von Ihrem Vertriebspartner.

Vor einer Migration auf Sophos SafeGuard 5.6x sollten Sie ein neues Konfigurationspaket im SafeGuard Policy Editor erzeugen und es mit der Sophos SafeGuard 5.6x Software auf den Endpoint-Computern installieren.

Für weitere Informationen siehe die Sophos SafeGuard Administrator-Hilfe, Kapitel *Migration von SafeGuard Easy 4.x/ Sophos SafeGuard Disk Encryption 4.x auf Sophos SafeGuard 5.6x* und <http://www.sophos.de/support/knowledgebase/article/108561.html>.

4 Was wird installiert?

Sie installieren die folgenden Komponenten:

- SafeGuard Policy Editor. Der SafeGuard Policy Editor ist das Sophos SafeGuard Verwaltungs-Tool. Im SafeGuard Policy Editor können Sie die Verschlüsselungssoftware auf Endpoint-Computern verwalten und Recovery-Aufgaben durchführen.

Microsoft SQL Server 2005 Express dient zum Speichern der Sophos SafeGuard Richtlinieneinstellungen und wird beim Einrichten des SafeGuard Policy Editor automatisch installiert, wenn keine SQL Server Instanz zur Verfügung steht.

Hinweis:

Installieren Sie erst den SafeGuard Policy Editor auf einem Windows Server. Später können Sie die Software auf mehreren Administrator-Computern installieren, die alle eine Verbindung mit der zentralen Sophos SafeGuard Datenbank auf dem Server herstellen.

- Sophos SafeGuard Verschlüsselungssoftware. Verschlüsselt Daten auf Endpoint-Computern und schützt Sie vor unberechtigtem Zugriff.

Hinweis:

Wir empfehlen, die Verschlüsselungssoftware nicht auf dem Administratorcomputer, der für die Sophos SafeGuard Verwaltung benutzt wird, zu installieren.

5 Installationsschritte

Führen Sie die folgenden Schritte aus:

- Installieren Sie den SafeGuard Policy Editor.
- Führen Sie die Erstkonfiguration durch. In der Erstkonfiguration wird eine Standardrichtlinie erstellt. Darüber hinaus werden wichtige Voraussetzungen für Helpdesk-Aufgaben geschaffen.
- Kopieren Sie die Standardrichtlinie zur Bearbeitung.
- Konfigurieren Sie den Endpoint-Computer für Service-Tasks nach der Installation.
- Veröffentlichen Sie die bearbeitete Richtlinie in einem Konfigurationspaket.
- Installieren Sie die Verschlüsselungssoftware und das Konfigurationspaket auf den Endpoint-Computern.

6 Installation des SafeGuard Policy Editor

Bevor Sie beginnen:

- Überprüfen Sie, ob .NET Framework 3.0 Service Pack 1 auf dem Computer installiert ist, auf dem Sie den SafeGuard Policy Editor installieren möchten. Die Software steht kostenlos zum Download zur Verfügung: <http://www.microsoft.com/downloads>.
- Überprüfen Sie die Systemanforderungen: <http://www.sophos.de/support/knowledgebase/article/112891.html>.
- Stellen Sie sicher, dass Sie über Windows Administratorrechte verfügen.

So installieren Sie den SafeGuard Policy Editor:

1. Melden Sie sich an Ihrem Computer als Administrator an.
2. Laden Sie die Installer von der Sophos Website herunter. Sie erhalten hierzu von Ihrem Systemadministrator die entsprechende Web-Adresse und die erforderlichen Download-Anmeldeinformationen.
3. Doppelklicken Sie je nach Produkt im Produktinstallationsordner auf eine der folgenden Dateien. Ein Assistent führt Sie durch die notwendigen Schritte.

Sophos SafeGuard Disk Encryption	SafeGuard Easy
SDEPolicyEditor.msi.	SGNPolicyEditor.msi.

4. Übernehmen Sie in den folgenden Dialogen die Standardeinstellungen.
Wenn Sie dazu aufgefordert werden, Microsoft SQL Server 2005 Express zu installieren, klicken Sie auf **Ja**. In diesem Fall werden Ihre Windows-Anmeldeinformationen als SQL-Benutzerkonto verwendet.
5. Klicken Sie auf **Beenden**, um die Installation abzuschließen.

Der SafeGuard Policy Editor ist installiert. Nun führen Sie die Erstkonfiguration im SafeGuard Policy Editor durch.

7 Durchführen der Erstkonfiguration

Stellen Sie sicher, dass Sie über Windows Administratorrechte verfügen.

1. Starten Sie den SafeGuard Policy Editor über das **Start** Menü. Der Konfigurationsassistent wird gestartet und führt Sie durch die notwendigen Schritte.
2. Klicken Sie auf der **Willkommen** Seite auf **Weiter**.
3. Klicken Sie auf der **Datenbank** Seite auf **Weiter**. Die SQL-Datenbank zum Speichern von SafeGuard-Einstellungen und -Richtlinien wird erstellt.
4. Geben Sie auf der **Sicherheitsbeauftragter** Seite ein Kennwort für die Anmeldung an den SafeGuard Policy Editor ein und bestätigen Sie es. Klicken Sie auf **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.

Der Name des Sicherheitsbeauftragten wird angezeigt.

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

5. Klicken Sie auf der **Unternehmen** Seite auf **Weiter**. Das Unternehmenszertifikat dient zum Schutz der Richtlinieneinstellungen in der Datenbank und auf den Endpoint-Computern.
6. Geben Sie auf der Seite **Backup des Sicherheitsbeauftragten- und Unternehmens-Zertifikats** einen Speicherort für die Sicherungskopien der Zertifikate ein. Klicken Sie dann auf **Weiter**.

Wenn Sie die Zertifikate nun im Standard-Speicherort ablegen, exportieren Sie sie gleich nach der Erstkonfiguration an einen sicheren Speicherort, auf den Sie im Recovery-Fall Zugriff haben (z. B. USB Flash Drive). Sie benötigen Sie zum Reparieren einer beschädigten Installation oder einer korrupten Datenbank.

7. Klicken Sie auf der **Recovery-Schlüssel** Seite auf **Weiter**. Es wird eine Netzwerkfreigabe mit ausreichenden Berechtigungen für Mitarbeiter des IT-Helpdesk erstellt. Diese Freigabe dient zum Sammeln der Schlüssel-Recovery-Dateien von Endpoint-Computern. Diese Dateien werden für Recovery-Vorgänge benötigt.

Hinweis:

Die Sophos SafeGuard Software versucht für ca. vier Minuten, eine Verbindung mit der Netzwerkfreigabe herzustellen. Gelingt dies nicht, so versucht die Software, nach jeder Windows-Anmeldung die Verbindung herzustellen, bis dies gelingt oder die Recovery-Schlüsseldateien manuell gesichert werden.

8. Klicken Sie auf der **Lizenz** Seite auf [...], um nach der gültigen Lizenzdatei zu suchen, die für die Benutzung des SafeGuard Policy Editor im produktiven Betrieb erforderlich ist. Sie erhalten die Lizenzdatei von Ihrem Vertriebspartner. Wählen Sie die Datei aus und klicken Sie auf **Öffnen**. Klicken Sie auf **Weiter**.

9. Klicken Sie auf **Beenden**.

Die Erstkonfiguration ist abgeschlossen.

- Eine Standardrichtlinie zur Implementation einer unternehmensweiten Sicherheitsrichtlinie auf den Endpoint-Computern wurde angelegt.

Die Power-on Authentication ist aktiviert.

Die volume-basierende Verschlüsselung für alle internen Festplatten ist aktiviert.

Der Benutzer kann ein vergessenes Kennwort mit Local Self Help durch Beantwortung vordefinierter Fragen wiederherstellen.

Der Helpdesk kann Kennwörter mit dem Challenge/Response-Verfahren wiederherstellen.

Die dateibasierende Verschlüsselung ist aktiviert (nur für SafeGuard Easy Kunden).

- Alle notwendigen Voraussetzungen für die Durchführung von Recovery-Aufgaben durch den Helpdesk sind geschaffen.
- Eine gültige Lizenz für die Nutzung von Sophos SafeGuard im produktiven Betrieb wurde importiert.

Sobald der Konfigurationsassistent geschlossen ist, wird der SafeGuard Policy Editor gestartet.

8 Kopieren der Standardrichtlinie zur Bearbeitung

1. Klicken Sie im Navigationsbereich des SafeGuard Policy Editor auf **Richtlinien**.
2. Klicken Sie im **Richtlinien** Navigationsfenster unter **Richtliniengruppen** mit der rechten Maustaste auf **Standardrichtlinie** und klicken Sie auf **Richtlinie sichern**.
3. Geben Sie einen Dateinamen und einen Speicherort für die Kopie (XML) ein und klicken Sie auf **Speichern**.
4. Klicken Sie im Navigationsfenster mit der rechten Maustaste auf **Richtlinien-Gruppen** und klicken Sie auf **Neu**.
5. Wählen Sie die neu erstellte Kopie der Richtlinie (XML) aus und klicken Sie auf **Öffnen**.

Eine Kopie der Standardrichtlinie mit alle einzelnen Richtlinien wird zurück in den SafeGuard Policy Editor kopiert.

Bearbeiten Sie nun die kopierte Standardrichtlinie, um eine Service Account Liste für Aufgaben nach der Installation zu konfigurieren. Somit stellen Sie sicher, dass Mitarbeiter aus dem technischen Service nach der Installation der Verschlüsselungssoftware auf die Computer zugreifen und diese konfigurieren können, ohne dass sie als "Besitzer" des Computers definiert werden.

9 Konfigurieren der Endpoint-Computer für Service-Tasks nach der Installation.

Nach der Installation der Verschlüsselungssoftware müssen Mitarbeiter aus dem technischen Service u. U. auf die Endpoint-Computer zugreifen und sie vorkonfigurieren. Dies ist z. B. oft bei einem zentralen Rollout erforderlich. Der erste Benutzer, der sich nach der Installation der Verschlüsselungssoftware an dem Computer anmeldet, aktiviert jedoch die POA und wird als Sophos SafeGuard Benutzer hinzugefügt. Um dies zu vermeiden, können Sie Benutzer auf eine Service Account Liste setzen. Die in dieser Liste enthaltenen Service-Mitarbeiter, können sich dann nach der Installation am Betriebssystem des Computers anmelden und die notwendigen Aufgaben durchführen. Sie werden weder als Sophos SafeGuard Benutzer hinzugefügt, noch aktivieren sie die POA.

So konfigurieren Sie eine Service Account Liste:

1. Klicken Sie im Navigationsbereich des SafeGuard Policy Editor auf **Richtlinien**.
2. Klicken Sie im **Richtlinien** Navigationsfenster mit der rechten Maustaste auf **Service Account Listen**, dann auf **Neu** und dann auf **Service Account Liste**.
3. Geben Sie einen Namen für die Liste ein und klicken Sie auf **OK**.
4. Wählen Sie im Navigationsfenster unter **Service Account Liste** die neue Liste aus.
5. Klicken Sie im Arbeitsbereich auf der rechten Seite mit der rechten Maustaste und wählen Sie **Hinzufügen** aus dem Kontextmenü. Eine neue Benutzerzeile wird hinzugefügt.
6. Geben Sie den Windows **Benutzernamen** und den **Domänennamen** in den entsprechenden Spalten ein und drücken Sie Enter. Um weitere Benutzer hinzuzufügen, wiederholen Sie diesen Schritt. Weitere Informationen hierzu finden Sie in der Administrator-Hilfe unter *Zusätzliche Informationen zur Eingabe von Benutzer- und Domänen-Namen*.
7. Klicken Sie auf das **Speichern** Symbol in der Symbolleiste, um Ihre Änderungen in der Datenbank zu speichern.

Die Service Account Liste ist nun registriert. In den nächsten Schritten weisen Sie die Liste der Richtlinie zu.

8. Wählen Sie im Navigationsfenster unter **Richtlinien** die kopierte **Authentisierung**-Richtlinie.
9. Wählen Sie unter **Anmeldeoptionen** die Option **Service Account Liste** und wählen Sie die neu erstellte Liste aus.
10. Klicken Sie auf das **Speichern** Symbol in der Symbolleiste, um Ihre Änderungen speichern.

Die Service Account Liste ist nun konfiguriert. Die **Authentisierung**-Richtlinie und die Richtliniengruppe, der diese Richtlinie angehört, werden entsprechend aktualisiert. Veröffentlichen Sie die bearbeitete Richtlinie nun in einem Konfigurationspaket.

Hinweis:

Sie können auch weitere Richtlinieneinstellungen an Ihre Anforderungen anpassen. So können Sie z. B. die POA individualisieren, Verschlüsselung konfigurieren oder Wake On LAN aktivieren. Weitere Informationen finden Sie in der Administrator-Hilfe (Kapitel *Richtlinieneinstellungen*).

10 Veröffentlichen der bearbeiteten Richtlinie in einem Konfigurationspaket

Damit Richtlinien auf dem Endpoint-Computer zur Verfügung gestellt werden können, müssen sie zunächst in einem Konfigurationspaket veröffentlicht werden.

1. Klicken Sie im SafeGuard Policy Editor im **Extras** Menü auf **Konfigurationspakete**.
2. Klicken Sie auf **Konfigurationspaket hinzufügen**.
3. Geben Sie einen beliebigen Namen für das Konfigurationspaket ein.
4. Wählen Sie die im vorigen Schritt bearbeitete **Richtliniengruppe** aus, die auf die Endpoint-Computer angewendet werden soll.
5. Geben Sie einen Speicherort für das Konfigurationspaket an.
6. Klicken Sie auf **Konfigurationspaket erstellen**.
7. Klicken Sie auf **Schließen**.

Die Richtlinie wird in einem Konfigurationspaket (MSI) am angegebenen Speicherort veröffentlicht. Installieren Sie nun die Sophos SafeGuard Verschlüsselungssoftware und das Konfigurationspaket auf den Endpoint-Computern.

11 Installation der Verschlüsselungssoftware und des Konfigurationspakets auf den Endpoint-Computern

1. Bereiten Sie die Endpoint-Computer für die Verschlüsselung vor.
2. Um Sophos SafeGuard kennen zu lernen, installieren Sie die Verschlüsselungssoftware zunächst auf einem Testcomputer. Verwenden Sie einen anderen Computer als den, auf dem der SafeGuard Policy Editor installiert ist.
3. Melden Sie sich zum ersten Mal an.
4. Verwenden Sie eigene Tools, um die Installation und Konfigurationspakete zu verteilen und so die Verschlüsselungssoftware zentral auf den Endpoint-Computern einzurichten.

11.1 Vorbereiten der Endpoint-Computer für die Verschlüsselung

- Überprüfen Sie, ob ein Benutzerkonto angelegt und aktiv ist. Der Benutzer muss ein Kennwort haben.
- Erstellen Sie einen kompletten Backup der Daten.
- Schließen Sie alle geöffneten Applikationen.
- Stellen Sie sicher, dass Sie über Windows Administratorrechte verfügen.
- Stellen Sie sicher, dass genügend Festplattenspeicher frei ist.
- 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 größer angelegten Installation von Sophos SafeGuard die aktuelle Version dieser Hardware-Konfigurationsliste auf dem Endpoint-Computer zu installieren. Die Datei wird monatlich aktualisiert und steht hier zum Download zur Verfügung:
<ftp://POACFG:POACFG@ftp.ou.utimaco.de>

Weitere Informationen hierzu finden Sie in der Administrator-Hilfe unter *In der Power-on Authentication unterstützte Hotkeys*. Siehe auch:
<http://www.sophos.de/support/knowledgebase/article/657000.html>.

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

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

Unter Umständen werden Sie dazu aufgefordert, den Computer neu zu starten und **chkdsk** noch einmal auszuführen. Weitere Informationen finden Sie hier:
<http://www.sophos.de/support/knowledgebase/article/107081.html>.

Die Ergebnisse (Log-Datei) können Sie in der Windows-Ereignisanzeige prüfen.

Windows XP: Wählen Sie **Anwendung, Winlogon**.

Windows 7, Windows Vista: Wählen Sie **Windows Logs, Anwendung, Wininit**.

- Benutzen Sie das Windows-Tool **defrag**, um fragmentierte Boot-Dateien, Datendateien und Ordner auf lokalen Volumes aufzufinden und zu konsolidieren.

defrag %drive%

Weitere Informationen finden Sie hier:

<http://www.sophos.de/support/knowledgebase/article/109226.html>

- Deinstallieren Sie Third-Party Boot-Manager, z. B. PRONetworks Boot Pro und Boot-US.
- Wir empfehlen, den Master Boot Record (MBR) zu bereinigen. Für die Installation von Sophos SafeGuard benötigen Sie einen sauberen, einwandfreien MBR. Wenn Sie auf dem Endpoint-Computer ein Image/Clone-Programm verwendet haben, ist der MBR u. U. nicht mehr sauber.

Starten Sie den Computer von einer Windows-DVD und führen Sie den Befehl **FIXMBR** innerhalb der Windows Recovery Console aus. Weitere Informationen finden Sie hier:

<http://www.sophos.de/support/knowledgebase/article/108088.html>.

- Wenn die Bootpartition auf dem Endpoint-Computer von FAT nach NTFS konvertiert wurde, der Computer aber noch nicht neu gestartet wurde, sollten Sie den Computer einmal neu starten, bevor Sie Sophos SafeGuard installieren. Andernfalls 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.

11.2 Durchführen einer Test-Installation

Führen Sie die Test-Installation auf einem anderen Computer als dem, auf dem der SafeGuard Policy Editor installiert ist, durch.

1. Bereiten Sie die Installation auf den Endpoint-Computern vor, [siehe Vorbereiten der Endpoint-Computer für die Verschlüsselung](#) (Seite 15).
2. Melden Sie sich an dem Endpoint-Computer als Administrator an.
3. Installieren Sie das Prä-Installationspaket **SGxClientPreinstall.msi**, das den Endpoint-Computer mit den nötigen Voraussetzungen für eine erfolgreiche Installation der Verschlüsselungssoftware ausstattet.
4. Installieren Sie die Verschlüsselungssoftware auf dem Endpoint-Computer: Doppelklicken Sie auf einem der folgenden Pakete (MSI), um den Installationsassistenten der Verschlüsselungssoftware zu starten. Dieser führt Sie durch die notwendigen Schritte.

Sophos SafeGuard Disk Encryption	Sophos 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 SGNClient_x64.msi für die 64-Bit-Variante

5. Übernehmen Sie in den folgenden Dialogen die Standardeinstellungen.
6. Wenn Sie dazu aufgefordert werden, wählen Sie den Installationstyp **Vollständig**.

Sophos SafeGuard Easy: SafeGuard Device Encryption und zusätzlich SafeGuard Data Exchange werden installiert. Informationen zu weiteren Client-Installationspaketen finden Sie in der Administrator-Hilfe unter *Installation*.

Sophos SafeGuard Disk Encryption: SafeGuard Enterprise Device Encryption wird installiert. SafeGuard Data Exchange ist nicht verfügbar.

7. Übernehmen Sie in allen weiteren Dialogen die Standardeinstellungen, um den Installationsassistenten abzuschließen.
8. Wechseln Sie an den Speicherort des zuvor erstellten Konfigurationspakets (MSI).
9. Installieren Sie dieses Konfigurationspaket auf dem Endpoint-Computer. Löschen Sie jeweils immer alle veralteten Konfigurationspakete auf dem Endpoint-Computer.

Sophos SafeGuard ist nun auf dem Endpoint-Computer installiert und gemäß den zuvor erstellten Richtlinien konfiguriert. Melden Sie sich nun das erste Mal nach der Installation am Computer an, um Aufgaben nach der Installation (mit einem Service Account) durchzuführen, oder um als Besitzer des Computers definiert zu werden.

Zusätzliche Konfiguration kann erforderlich sein, damit sich die POA auf jeder Hardware-Plattform korrekt verhält. Die meisten Hardware-Konflikte lassen sich mit Hilfe des **Hotkeys**-Features beheben, das in die POA integriert ist. Hotkeys können nach der Installation konfiguriert werden, entweder in der POA selbst oder über eine zusätzliche Konfigurationseinstellung, die dem msixec Installationstool mitgegeben wird. Weitere Informationen hierzu finden Sie in der Administrator-Hilfe unter *In der Power-on Authentication unterstützte Hotkeys*. Siehe auch:

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

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

11.3 Erste Anmeldung mit einem Service Account

Melden Sie sich mit einem Service Account an, wenn Sie auf dem Computer nach der Installation Aufgaben durchführen möchten.

1. Starten Sie den Endpoint-Computer nach der Installation neu. Die Windows-Anmeldung wird angezeigt.

Unter Windows Vista und Windows 7 müssen Sie zunächst die Tastenkombination STRG+ALT+ENTF (CTRL+ALT+DEL) drücken, um die Anmeldung zu starten. Diese Einstellung kann der Administrator in der MMC-Konsole im Gruppenrichtlinien-Objekteditor unter **Windows-Einstellungen > Sicherheitseinstellungen > Lokale Richtlinien > Sicherheitsoptionen deaktivieren**. (Für die interaktive Anmeldung ist Strg+Alt+Entf nicht erforderlich.)

2. Melden Sie sich mit dem Service Account an Windows an: Geben Sie die Domäne und die Anmeldedaten, wie in der Service Account Liste im SafeGuard Policy Editor definiert, ein.

Sie werden an Windows als Gastbenutzer angemeldet. Die Power-on Authentication wird nicht aktiviert und Sie werden dem Computer nicht als Besitzer zugeordnet. Sie können nun die erforderlichen Aufgaben durchführen.

11.4 Erste Anmeldung ohne Service Account

1. Starten Sie den Computer neu. Zunächst wird Sophos SafeGuard Autologon angezeigt, dann erscheint die Windows-Anmeldung.

Unter Windows Vista und Windows 7 müssen Sie zunächst die Tastenkombination STRG+ALT+ENTF (CTRL+ALT+DEL) drücken, um Autologon und die Anmeldung zu starten. Diese Einstellung kann der Administrator in der MMC-Konsole im Gruppenrichtlinien-Objekteditor unter **Windows-Einstellungen > Sicherheitseinstellungen > Lokale Richtlinien > Sicherheitsoptionen deaktivieren**. (Für die interaktive Anmeldung ist Strg+Alt+Entf nicht erforderlich.)

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. Während der Verschlüsselung können Sie weiterhin mit dem Computer arbeiten. Nach Abschluss der Verschlüsselung ist kein Neustart notwendig. Ver- und Entschlüsselungsvorgänge laufen transparent und ohne Benutzerinteraktion ab. Weitere Informationen finden Sie in der Benutzerhilfe in den Kapiteln *Erste Anmeldung nach der Installation von Sophos SafeGuard* und *Datenverschlüsselung*.

11.5 Installation der Verschlüsselungssoftware und Konfigurationspakete über Skript

1. Bereiten Sie die Installation auf den Endpoint-Computern vor, [siehe Vorbereiten der Endpoint-Computer für die Verschlüsselung](#) (Seite 15).
2. Melden Sie sich am Administrator-Computer als Administrator an.
3. Erstellen Sie ein Verzeichnis mit der Bezeichnung **Software** als zentralen Speicherort für alle Anwendungen.

4. Verwenden Sie ein Software Deployment Tool (z. B. Microsoft System Center Configuration Manager, IBM Tivoli oder Enteo Netinstall), um die zentrale Installation auf den Endpoint-Computern durchzuführen. Folgende Komponenten müssen enthalten sein (in dieser Reihenfolge):

Option	Beschreibung
Paket	Beschreibung
Prä-Installationspaket SGxClientPreinstall.msi	Das Paket stattet Endpoint-Computer mit notwendigen Voraussetzungen für eine erfolgreiche Installation der Verschlüsselungssoftware aus. Hinweis: Wenn dieses Paket nicht installiert ist, wird die Installation der Verschlüsselungssoftware abgebrochen.
Verschlüsselungssoftware-Installationspaket <Client>*.msi	Je nach Produkt und Betriebssystem stehen unterschiedliche Installationspakete zur Verfügung. Für Windows 7 und Windows Vista können Sie z. B. die *_x64.msi Paketvariante installieren. Sie finden alle verfügbaren <Client>-Installationspakete in Ihrer Produktlieferung. Hinweis: Informationen zu allen verfügbaren <Client>-Installationspaketen finden Sie in der Administrator-Hilfe unter <i>Installation</i> .
Konfigurationspaket für Endpoint-Computer	Verwenden Sie die zuvor im SafeGuard Policy Editor erzeugten Konfigurationspakete. Löschen Sie jeweils immer alle veralteten Konfigurationspakete.
Skript mit Befehlen für die automatische Installation	Wir empfehlen, das Windows Installer Kommandozeilen-Tool msiexec.exe zu verwenden, um das Skript zu erzeugen. Weitere Informationen hierzu finden Sie in der Administrator-Hilfe unter <i>Kommando für zentrale Installation</i> . http://msdn.microsoft.com/en-us/library/aa367988(VS.85).aspx

5. Um das Skript zu erzeugen, öffnen Sie eine Befehlseingabeaufforderung und geben Sie die Scripting-Befehle ein. Für weitere Informationen, *siehe Skript-Befehl - Beispiel* (Seite 20).
6. Verteilen Sie das Prä-Installationspaket, das Client-Paket und das Konfigurationspaket über unternehmensinterne Software-Verteilungsmechanismen an die Endpoint-Computer.

Die Pakete werden auf den Endpoint-Computern ausgeführt.

Sophos SafeGuard wird auf den Endpoint-Computern gemäß den zuvor erstellten Richtlinien installiert und konfiguriert. Eine für Recovery-Vorgänge benötigte Schlüssel-Recovery-Datei wird für jeden Endpoint-Computer in dem Speicherort erstellt, der während der Erstkonfiguration des SafeGuard Policy Editor definiert wurde.

Zusätzliche Konfiguration kann erforderlich sein, damit sich die Power-on Authentication (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 Windows Installer Befehl msiexec mitgegeben wird. Weitere Informationen hierzu finden Sie in der Administrator-Hilfe unter *In der Power-on Authentication unterstützte Hotkeys*. Siehe auch:

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

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

11.6 Skript-Befehl - 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\%computename%\SDEClient_inst.log
```

```
Installdir=C:\Programme\Sophos\Sophos SafeGuard
```

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

Das Kommando bewirkt Folgendes:

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

Installiert das Prä-Installationspaket aus dem angegebenen Speicherort in das Standardinstallationsverzeichnis **C:\Program Files\Sophos\Sophos SafeGuard**. Die Endpoint-Computer werden mit den notwendigen Voraussetzungen für eine erfolgreiche Installation der Verschlüsselungssoftware ausgestattet.

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

```
InstallDir=C:\Programme\Sophos\Sophos SafeGuard
```

Installiert die Verschlüsselungssoftware, in diesem Fall SafeGuard Device Encryption mit Power-on Authentication, aus dem angegebenen Speicherort in das Standardinstallationsverzeichnis **C:\Program Files\Sophos\Sophos SafeGuard**.

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

Installiert das Konfigurationspaket aus dem angegebenen Speicherort in das Standardinstallationsverzeichnis.

```
/L*VX  
G:\Temp\Sophos\SafeGuard\%computername%__SDEClient_inst.log
```

Protokolliert alle Warnungs- und Fehlermeldungen in der angegebenen Protokolldatei auf dem Netzwerk und erstellt eine Protokolldatei für den zentralen Review des Verschlüsselungsprozesses. Diese Protokolldatei lässt sich mit Windows Installer Tool **wilogutl.exe** automatisch analysieren.

```
/qn
```

Installiert ohne Benutzerinteraktion und zeigt keine Benutzeroberfläche an.

12 Recovery-Vorgänge bei vergessenem Kennwort

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

- Der Benutzer kann das Kennwort selbst mit Local Self Help wiederherstellen. Dieses Methode wird empfohlen.
- Das Helpdesk stellt das Kennwort mit einem Challenge/Response-Verfahren wieder her.

12.1 Wiederherstellen eines Kennworts mit 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 die Funktion dann automatisch gestartet.
- Wenn sowohl Challenge/Response als auch Local Self Help für Recovery für die Anmeldung angezeigt werden, klickt der Benutzer auf **Local Self Help**.

3. In den folgenden fünf Dialogen beantwortet der Benutzer eine vordefinierte Anzahl an 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 Bootvorgang 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.

12.2 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. 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 Local Self Help kann sich der Benutzer selbst das aktuelle Benutzerkennwort anzeigen lassen und es weiterhin zur Anmeldung verwenden. Dadurch

wird ein Zurücksetzen des Kennworts vermieden. Außerdem muss der Helpdesk nicht um Hilfe gebeten werden.

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 für Recovery für die Anmeldung angezeigt werden, 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 im SafeGuard Policy Editor den **Recovery-Assistenten**.
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 gestartet.
9. Da dem Benutzer das Kennwort nicht bekannt ist, kann er es im Windows-Anmeldedialog 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. Wenn das alte Kennwort nicht angegeben werden kann, ist in Sophos SafeGuard für die Definition eines neuen Kennworts ein neues Zertifikat erforderlich. Der Benutzer muss diese Aktion bestätigen.

13. Basierend auf dem neu gewählten Windows-Kennwort wird ein neues Benutzerzertifikat erzeugt.

Der Benutzer kann sich dann an der Power-on Authentication mit dem neuen Kennwort anmelden und es für zukünftige Anmeldevorgänge verwenden.

13 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, der Benutzerhilfe oder der Tools-Anleitung.

Aufgabe	Handbuch/Hilfe
Konfigurieren zusätzlicher Instanzen des SafeGuard Policy Editor	Administrator-Hilfe, Konfigurieren zusätzlicher Instanzen des SafeGuard Policy Editor
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, Exportieren des Unternehmens- und Sicherheitsbeauftragten-Zertifikats
Erstellen eines administrativen Zugangs zu Endpoint-Computern (POA Access Accounts)	Administrator-Hilfe, Administrative Zugangsoptionen für Endpoint-Computer
Wiederherstellen des Zugriffs auf verschlüsselte Daten	Administrator-Hilfe, Challenge/Response mit virtuellen Clients
Wiederherstellen eines korrupten Master Boot Records	Tools-Anleitung, Wiederherstellen eines beschädigten MBR
Migrieren von SDE 4.6x oder SGE 4.3x - 4.5x auf Sophos SafeGuard	Administrator-Hilfe, Migration SafeGuard Easy 4.x/Sophos Disk Encryption 4.x auf Sophos SafeGuard 5.6x

14 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.

15 Rechtliche Hinweise

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

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

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

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