

SOPHOS

Sophos SafeGuard Disk Encryption für Mac Benutzerhilfe

Stand: Januar 2011



Inhaltsverzeichnis

1	Sophos SafeGuard Disk Encryption für Mac	2
2	Sophos SafeGuard Disk Encryption System-Menü.....	3
3	Power-on Authentication	4
4	Benutzerverwaltung.....	8
5	Disk-Verwaltung.....	12
6	Benutzung von Sophos SafeGuard Disk Encryption über Terminal.....	14
7	Time Machine Backups.....	21
8	Unterstützte Hardware und Konfigurationen	22
9	Nicht unterstützte Hardware, Konfigurationen und Vorgänge.....	24
10	Technischer Support.....	27
11	Rechtlicher Hinweis.....	28

1 Sophos SafeGuard Disk Encryption für Mac

Sophos SafeGuard Disk Encryption für Mac bietet Power-on Authentication für Ihren Mac und verschlüsselt Festplatten oder Partitionen auf Ihrem Mac.

Mit der **Power-on Authentication (POA)** müssen sich Benutzer bereits während der Pre-Boot-Phase anmelden, das heißt, bevor das Betriebssystem gestartet wird. Erst wenn sich der Benutzer in der POA korrekt authentisiert hat, wird das eigentliche Betriebssystem gestartet und der Benutzer wird automatisch an OS X angemeldet, wenn das System für die automatische Anmeldung konfiguriert ist.

Sophos SafeGuard Disk Encryption verschlüsselt die Daten auf einem Mac partitionsbasierend. Ein SafeGuard Admin-Benutzer legt fest, welche Festplatten oder Partitionen verschlüsselt werden sollen. Ein regulärer SafeGuard-Benutzer (User) ist nicht dazu berechtigt, diese Einstellungen zu ändern.

Die Dateien auf einer verschlüsselten Partition werden transparent verschlüsselt. Sie werden beim Öffnen, Bearbeiten und Speichern von Dateien nicht zur Verschlüsselung oder Entschlüsselung aufgefordert. Wenn Sie Dateien öffnen, werden diese entschlüsselt und Sie können sie bearbeiten. Wenn Sie die Dateien schließen oder speichern, werden sie wieder verschlüsselt.

Hinweis: Nach der Installation von Sophos SafeGuard Disk Encryption for Mac erhält die Systempartition, auf der die Software installiert ist, ein neues Symbol (das Festplattensymbol mit dem SafeGuard-Schild). Dieses Symbol gibt lediglich an, dass SafeGuard installiert ist. Diese Partition ist nicht verschlüsselt! Datenpartitionen erhalten dieses Symbol, wenn sie verschlüsselt wurden.

2 Sophos SafeGuard Disk Encryption System-Menü

Ein Symbol am rechten Ende der Menüleiste steht für das Sophos SafeGuard Disk Encryption System-Menü. Über dieses Menü können Sie schnell auf die Funktionen von Sophos SafeGuard Disk Encryption zugreifen. Außerdem zeigt es den Status von Sophos SafeGuard Disk Encryption.

Das Sophos SafeGuard Disk Encryption System-Menü enthält folgende Menübefehle:

- **Über SafeGuard:** Zeigt Informationen zu Sophos SafeGuard Disk Encryption, z. B. Versions- und Copyright-Informationen.
- **Disk-Verwaltung:** Öffnet die Disk-Verwaltung. Nur SafeGuard Admin-Benutzer sind dazu berechtigt, Einstellungen in der Disk-Verwaltung zu ändern. Ein regulärer SafeGuard-Benutzer ist nur dazu berechtigt, die Einstellungen einzusehen..
- **Benutzerverwaltung:** Öffnet die Benutzerverwaltung. Nur SafeGuard Admin-Benutzer sind dazu berechtigt, Einstellungen in der Benutzerverwaltung zu ändern. Ein regulärer SafeGuard-Benutzer ist nur dazu berechtigt, die Einstellungen einzusehen.
- **Statusinformationen:** Bei laufender Ver-/Entschlüsselung werden als Statusinformationen der Name der relevanten Partition sowie der Fortschritt der Ver-/Entschlüsselung angezeigt.

3 Power-on Authentication

Mit der **Power-on Authentication (POA)** müssen sich Benutzer bereits während der Pre-Boot-Phase anmelden, das heißt, bevor das Betriebssystem gestartet wird. Erst wenn sich der Benutzer in der POA korrekt authentisiert hat, wird das eigentliche Betriebssystem gestartet und der Benutzer wird automatisch an OS X angemeldet, wenn die automatische Anmeldung konfiguriert ist.

Solange noch keine SafeGuard-Benutzer vorhanden sind, zeigt die POA das "Secured by SOPHOS"-Logo. Nach etwa einer Sekunde wird das Betriebssystem gestartet.

Sind SafeGuard-Benutzer vorhanden, so wird der Anmeldedialog angezeigt. Die Power-on Authentication ist immer aktiviert, unabhängig davon ob verschlüsselte Partitionen vorhanden sind oder nicht.

3.1 Anmeldung an der POA

Die Anmeldung an der POA erfolgt mit den Sophos SafeGuard Disk Encryption Benutzeranmeldedaten. Diese Anmeldedaten erhalten Sie von Ihrem Systemadministrator oder der Person die Sophos SafeGuard Disk Encryption auf Ihrem Mac installiert und/oder konfiguriert hat.

Geben Sie zum Anmelden Ihren SafeGuard Benutzernamen und das Kennwort in die Eingabefelder ein.

Wird das Sophos SafeGuard Disk Encryption Benutzerkonto akzeptiert, so erfolgt die Anmeldung an das Betriebssystem bei entsprechender Konfiguration automatisch.

3.2 Fehlerbehebung in der POA

Sophos SafeGuard Disk Encryption bietet Optionen zur Fehlerbehebung in der Power-on Authentication:

- Recover
- Partition permanent entschlüsseln
- Log anzeigen

Diese Optionen sind hilfreich, wenn z. B. Ihre Sophos SafeGuard Disk Encryption Installation beschädigt ist, das Betriebssystem nicht startet usw.

Wenn Sie im Anmeldedialog auf **Fehlerbehebung** klicken, wird ein Menü mit den Optionen für die Fehlerbehebung geöffnet.

3.2.1 Recover

Neben Recovery-Vorgängen für die Anmeldung bei vergessenen Kennwörtern bietet Sophos SafeGuard Disk Encryption weitere Recovery-Optionen, die sicherstellen, dass sich auch beschädigte Systeme auf einfache Art und Weise wiederherstellen lassen.

Voraussetzung für jede Recovery-Aktion ist, dass der Kernel und die Authentisierungsdaten direkt nach dem Installieren der Software und dem Anlegen von Benutzern exportiert werden.

Hinweis: Darüber hinaus müssen Sie die Authentisierungsdaten immer dann exportieren, wenn Sie Benutzer hinzufügen oder deren Anmeldedaten ändern, um die Backups auf dem aktuellen Stand zu halten. Wenn Sie die Sophos SafeGuard Disk Encryption Software auf Ihrem Mac aktualisiert haben, müssen Sie den Kernel auch wieder exportieren.

3.2.1.1 Erstellen der Recovery-Medien

So exportieren Sie Recovery-Daten:

1. Klicken Sie auf das Sophos SafeGuard Disk Encryption Symbol und wählen Sie **Benutzerverwaltung**.
2. Geben Sie Ihre SafeGuard-Anmeldedaten (Admin, Benutzer, Recovery) ein und klicken Sie auf **OK**.
3. Das **Aktion** Menü enthält drei Optionen:

Maschinenunabhängiges Recovery-Medium erzeugen

Wählen Sie **Maschinenunabhängiges Recovery-Medium erzeugen**, wenn Sie universelle Recovery-Medien für Ihre Macs erzeugen wollen. Mit diesen Medien können Sie Recovery-Vorgänge auf jeder Maschine durchführen, wenn die Authentisierungsdaten korrekt sind.

Um das Medium zu erstellen, klicken Sie auf **Maschinenunabhängiges Recovery-Medium erzeugen**. Wählen Sie im angezeigten Dialog den gewünschten Speicherort, belassen Sie die Option **Speichern in Disk Image** ausgewählt und klicken Sie auf **Maschinenunabhängiges Recovery-Medium erzeugen**.

Hinweis: Unabhängig davon, welchen Speicherort Sie gewählt haben (bereits auf USB-Stick oder vorübergehend auf der Festplatte Ihres Mac), müssen Sie das Disk Image danach mit der Disk Utility Ihres Mac im Stammverzeichnis des USB-Sticks wiederherstellen. Dies ist erforderlich, damit das Recovery-Medium fehlerfrei funktioniert.

Authentisierungsdaten exportieren

Wählen Sie **Authentisierungsdaten exportieren**, um einen Backup aller Benutzeranmeldedaten zu erstellen. Sie sollten die Benutzeranmeldedaten an einem sicheren Speicherort ablegen, auf den Sie im Notfall zugreifen können.

Maschinenspezifisches Recovery-Medium erzeugen

Wählen Sie **Maschinenspezifisches Recovery-Medium** erzeugen, wenn Sie als Einzelbenutzer ein Recovery-Paket erstellen möchten, das alle im Notfall benötigten Daten enthält. Der Vorgang ist mit dem Erstellen eines maschinenunabhängigen Mediums identisch.

Alle diese Recovery-Aktionen können in der Power-on Authentication gestartet werden.

3.2.1.2 Durchführen von Recovery-Vorgängen

Im allgemeinen sind Recovery-Vorgänge in zwei Situationen erforderlich:

- Beschädigte Anmeldedaten In diesem Fall wird in der Power-on Authentication oder vom Betriebssystem die entsprechende Meldung angezeigt.
- Kernel-Probleme, die z. B. durch defekte Sektoren auf Ihrer Festplatte verursacht werden.

Beschädigte Anmeldedaten

1. Stecken Sie einen USB-Stick an, der die exportierten Anmeldedaten enthält. Starten Sie Ihren Mac.
2. Wählen Sie in der Power-on Authentication die Option **Fehlerbehebung** und klicken Sie im **Fehlerbehebung** Menü auf **Recover**.
3. Sophos SafeGuard Disk Encryption sucht auf allen mit dem Mac verbundenen Wechselmedien nach Anmelde- und Schlüsseldaten. Diese müssen sich im Stammverzeichnis befinden.
4. Werden Daten gefunden, so müssen Sie bestätigen, dass Sie die Anmeldedaten wiederherstellen möchten. Danach werden die lokalen Anmeldedaten durch die auf dem USB-Stick enthaltenen ersetzt.
5. Wenn Sie die erfolgreiche Durchführung des Recovery-Vorgangs bestätigt haben, wechseln Sie wieder in die Power-on Authentication und melden Sie sich wie üblich an.

Kernel Recovery

In diesem Fall müssen Sie die Power-on Authentication von Ihrem Recovery-Medium aus starten.

1. Stecken Sie Ihr Recovery-Medium an und starten Sie Ihren Mac von diesem Medium.
2. Wenn das Festplattensymbol mit einem weißen Kreuz auf grünem Hintergrund angezeigt wird, klicken Sie auf das Symbol.
3. Die vom Recovery-Medium gestartete Power-on Authentication wird angezeigt.

4. Wählen Sie **Fehlerbehebung** und klicken Sie im **Fehlerbehebung** Menü auf **Recover**.
5. Wählen Sie im **Recovery** Menü die Option **Kernel-Partition**. Durch Auswahl der Option **Authentisierungsdaten** wird der unter **Beschädigte Anmeldedaten** beschriebene Vorgang ausgelöst.
6. Wenn Sie die erfolgreiche Durchführung des Recovery-Vorgangs bestätigt haben, wechseln Sie wieder in die Power-on Authentication und melden Sie sich wie üblich an.

3.2.2 Partition permanent entschlüsseln

Das permanente Entschlüsseln einer Partition kann z. B. notwendig sein, wenn sich das Betriebssystem nicht mehr starten lässt, Sie aber Zugriff auf verschlüsselte Daten benötigen. So lassen sich Partitionen entschlüsseln, ohne dass dazu das Betriebssystem laufen muss.

Wenn Sie diese Option auswählen, wird eine Liste von allen auf Ihrem Mac verfügbaren Partitionen angezeigt.

Um eine Partition auszuwählen, drücken Sie die Leertaste. Sie müssen die Entschlüsselung durch Eingabe Ihrer SafeGuard Admin Anmeldedaten in den Eingabefeldern autorisieren.

Wählen Sie **Entschlüsseln**, um die Entschlüsselung der ausgewählten Partition zu starten.

3.2.3 Log anzeigen

Wenn Sie diese Option auswählen, wird die Log-Datei angezeigt, die bei der Problemanalyse hilfreich ist.

Sie können den Log-Inhalt in einer Datei auf einem USB-Stick exportieren.

Verbinden Sie hierzu einen USB-Stick mit Ihrem Mac und wählen Sie **Exportieren**. Die Log-Datei wird automatisch im Stammverzeichnis des USB-Sticks gespeichert.

Hinweis: Der USB-Stick muss eine FAT-Partition aufweisen.

4 Benutzerverwaltung

Die Sophos SafeGuard Disk Encryption Benutzerverwaltung basiert auf drei verschiedenen Benutzertypen:

- Typ: **Admin**
- Typ: **Benutzer**
- Typ: **Recovery**

Diese Rollen sind von den Systemkonten unabhängig und spiegeln eine Art "kryptographischen SafeGuard-Benutzer" wider.

4.1 Admin-Benutzer

Die Rolle des Admin-Benutzers ist für folgende Vorgänge erforderlich.

- **Hinzufügen** von Benutzern eines beliebigen Typs
- **Löschen** von Benutzern eines beliebigen Typs
- **Ändern** des Verschlüsselungsstatus von Partitionen

Es muss immer ein Admin-Benutzer vorhanden sein. Der erste Benutzer, der erstellt wird, muss ein Admin-Benutzer sein. Dies wird von der SafeGuard Benutzerverwaltung durchgesetzt und ist Voraussetzung für alle Administrationsaufgaben. Sind mehrere Admin-Benutzer vorhanden, so kann beim Löschen von Benutzern der letzte Admin-Benutzer nicht gelöscht werden.

4.1.1 Erstellen des ersten Sophos SafeGuard Disk Encryption Admin-Benutzers

1. Klicken Sie auf das Sophos SafeGuard Disk Encryption Symbol und wählen Sie **Benutzerverwaltung**.
2. Geben Sie einen Namen für den Admin-Benutzer ein.
3. Geben Sie das Kennwort in den Feldern **Kennwort** und **Kennwort bestätigen** ein. Sophos SafeGuard Disk Encryption akzeptiert nur Kennwörter mit acht oder mehr Zeichen (bis zu 127). Um das eingegebene Kennwort anzuzeigen, wählen Sie die Option **Kennwort anzeigen**.
4. Klicken Sie auf **OK**.

4.2 Benutzer

Der Benutzertyp **Benutzer** steht für einen normalen Benutzer. Benutzer dieses Typs sind nicht dazu berechtigt, andere Benutzer anzulegen/zu löschen oder Disks zu verwalten. Sie können jedoch die aktuellen Einstellungen auf Ihrem Mac einsehen. Sie sind dazu berechtigt, sich an der POA anzumelden.

4.2.1 Erstellen eines SafeGuard-Benutzers

Um einen SafeGuard-Benutzer erstellen zu können, müssen Ihnen die SafeGuard Admin Anmeldedaten bekannt sein.

1. Klicken Sie auf das Sophos SafeGuard Disk Encryption Symbol und wählen Sie **Benutzerverwaltung**.
2. Geben Sie Ihre SafeGuard-Anmeldedaten (Admin, Benutzer, Recovery) ein und klicken Sie auf **OK**.
3. Wählen Sie im Verwaltungsbereich die Option **Benutzer**.
4. Klicken Sie auf die **Hinzufügen** Schaltfläche (+) unter der Liste der Benutzerkonten.
5. Wählen Sie die Option **Benutzer** aus dem **Benutzer hinzufügen** Pop-up-Menü.
6. Geben Sie einen Namen für den SafeGuard-Benutzer ein.
7. Geben Sie das Benutzer-Kennwort in den Feldern **Kennwort** und **Kennwort bestätigen** ein. Sophos SafeGuard Disk Encryption akzeptiert nur Kennwörter mit acht oder mehr Zeichen (bis zu 127). Um das eingegebene Kennwort anzuzeigen, wählen Sie die Option **Kennwort anzeigen**.
8. Geben Sie Ihre Admin-Anmeldedaten in den Feldern **Admin-Name** und **Admin-Kennwort** ein.
9. Klicken Sie auf **OK**.

Der neue SafeGuard-Benutzer wird nun in der Liste der Benutzerkonten angezeigt. Die Anmeldedaten dieses Benutzers können nun für die Anmeldung an der POA verwendet werden.

4.3 Recovery-Benutzer

Mit einem Recovery-Benutzer lässt sich ein Recovery-Vorgang für die Anmeldung durchführen, wenn ein SafeGuard-Benutzer sein Kennwort vergessen hat. Ein Recovery-Benutzer kann nicht

für Recovery-Vorgänge bei Admin-Benutzern oder anderen Recovery-Benutzern verwendet werden.

Ein Recovery-Benutzer ist als Einmal-Benutzer zu betrachten. Jeder Recovery-Benutzer ist an eine spezifischen SafeGuard-Benutzer gebunden. Mit einem Recovery-Benutzer kann also nur ein Recovery-Vorgang bei einem spezifischen SafeGuard-Benutzer durchgeführt werden. Wenn der SafeGuard-Benutzer gelöscht wird, werden auch seine Recovery-Benutzer entfernt.

Recovery-Benutzer können sich zwar an der POA anmelden, sie werden jedoch nach Ihrer Benutzung für einen Recovery-Vorgang bei einem SafeGuard-Benutzer entfernt.

Hinweis: Wir empfehlen, für jeden SafeGuard Benutzer mehrere Recovery-Benutzer anzulegen. Somit wird sichergestellt, dass immer ein Recovery-Benutzer vorhanden ist, falls der Benutzer sein Kennwort vergessen hat.

4.3.1 Erstellen eines Recovery-Benutzers

Um einen SafeGuard Recovery-Benutzer erstellen zu können, müssen Ihnen die SafeGuard Admin Anmeldedaten bekannt sein.

1. Klicken Sie auf das Sophos SafeGuard Disk Encryption Symbol und wählen Sie **Benutzerverwaltung**.
2. Geben Sie Ihre SafeGuard-Anmeldedaten (Admin, Benutzer, Recovery) ein und klicken Sie auf **OK**.
3. Wählen Sie im Verwaltungsbereich die Option **Benutzer**.
4. Klicken Sie auf die **Hinzufügen** Schaltfläche (+) unter der Liste der Benutzerkonten.
5. Wählen Sie die Option **Recovery** aus dem **Benutzer hinzufügen** Pop-up-Menü.
6. Wählen Sie einen vorhandenen Benutzer aus dem Pop-up-Menü aus. Der Recovery-Benutzer kann nur für diesen spezifischen Benutzer verwendet werden.
7. Geben Sie einen Namen für den Recovery-Benutzer ein.
8. Geben Sie das Kennwort für den Recovery-Benutzer in den Feldern **Kennwort** und **Kennwort bestätigen** ein. Sophos SafeGuard Disk Encryption akzeptiert nur Kennwörter mit acht oder mehr Zeichen. Um das eingegebene Kennwort anzuzeigen, wählen Sie die Option **Kennwort anzeigen**.
9. Geben Sie Ihre Admin-Anmeldedaten in den Feldern **Admin-Name** und **Admin-Kennwort** ein.
10. Klicken Sie auf **OK**.

Der neue Recovery-Benutzer wird nun in der Benutzerkontenliste angezeigt. Der Recovery-Benutzer kann nun für die Anmeldung an der POA und zum Wiederherstellen eines vergessenen Kennworts verwendet werden.

4.3.2 Wiederherstellen des Kennwort eines SafeGuard-Benutzers

1. Melden Sie sich mit Ihren SafeGuard Admin-Anmeldedaten oder mit den Anmeldedaten des entsprechenden Recovery-Benutzers an der POA an.
2. Klicken Sie auf das Sophos SafeGuard Disk Encryption Symbol und wählen Sie **Benutzerverwaltung**.
3. Geben Sie Ihre SafeGuard-Anmeldedaten (Admin, Benutzer, Recovery) ein und klicken Sie auf **OK**.
4. Wählen Sie im Verwaltungsbereich die Option **Benutzer**.
5. Wählen Sie rechts neben dem relevanten SafeGuard-Benutzerkonto die Option **Recover-User**.
6. Geben Sie ein neues Kennwort in den Feldern **Kennwort** und **Kennwort bestätigen** ein.
7. Geben Sie den Namen und das Kennwort des Recovery-Benutzers in den Feldern **Recovery-Name** und **Recovery-Kennwort** ein.
8. Klicken Sie auf **OK**.

Das Kennwort des SafeGuard-Benutzers wird zurückgesetzt. Es kann nun für die Anmeldung an der POA verwendet werden.

Hinweis: Der Recovery-Benutzer wird aus der Benutzerkontenliste gelöscht. Stellen Sie sicher, dass für jedes Benutzerkonto jeweils immer ein Recovery-Benutzer vorhanden ist. Falls nötig, erstellen Sie einen neuen Recovery-Benutzer. Ohne Recovery-Benutzer lassen sich Kennwörter nicht wiederherstellen.

5 Disk-Verwaltung

Mit Sophos SafeGuard Disk Encryption können Sie die Festplatte oder Partitionen auf Ihrem Mac verschlüsseln. Für alle Disk-Verwaltungsaufgaben (verschlüsseln/entschlüsseln/unterbrechen/fortsetzen) ist die Authentisierung als SafeGuard Admin-Benutzer erforderlich.

Das Sophos SafeGuard Disk Encryption Systemmenü am rechten Ende der Menüleiste zeigt den Status von laufenden Ver-/Entschlüsselungsvorgängen.

5.1 Verschlüsseln einer Partition

Bevor Sie eine Datenpartition verschlüsseln, stellen Sie sicher, dass alle Dateien auf dieser Partition geschlossen sind.

1. Klicken Sie auf das Sophos SafeGuard Disk Encryption Symbol und wählen Sie **Disk-Verwaltung**.
2. Geben Sie Ihre SafeGuard Admin Anmeldedaten ein und klicken Sie auf **OK**.
3. Wählen Sie im Verwaltungsbereich die Option **Partitionen**. Alle verfügbaren Partitionen werden angezeigt.
4. Klicken Sie neben der Partition, die Sie verschlüsseln möchten, auf **Verschlüsseln**.
5. Die Verschlüsselung der ausgewählten Partitionen wird sofort gestartet. Um die Geschwindigkeit des Verschlüsselungsvorgangs zu steigern, wählen Sie die Option **Fast Mode** in der unteren linken Ecke des Bereichs **Disk-Verwaltung**.

Während der Verschlüsselung können Sie weiterhin auf der Datenpartition arbeiten.

Hinweis: Wir empfehlen, die Installation von Updates und die initiale Verschlüsselung/ endgültige Entschlüsselung einer Maschine nicht gleichzeitig durchzuführen. Andernfalls können sich Installationsvorgänge erheblich verlangsamen.

Sie können die Ver-/Entschlüsselung unterbrechen, indem Sie auf die **Unterbrechen** Schaltfläche rechts neben der Fortschrittsanzeige klicken. Um die Verschlüsselung fortzusetzen, klicken Sie auf die **Fortsetzen** Schaltfläche. Diese wird angezeigt, wenn die Verschlüsselung unterbrochen wird. Für beide Aktionen ist eine Authentisierung als SafeGuard Admin-Benutzer erforderlich.

Wenn Sie Ihren Mac neu starten, werden unterbrochene Ver-/Entschlüsselungsvorgänge automatisch fortgesetzt.

Hinweis: Starten Sie die Verschlüsselung nicht für nicht gemountete Partitionen und machen Sie den Mountvorgang bei einer Partition nicht während der Verschlüsselung rückgängig. Beides kann zu Datenverlust führen.

5.2 Entschlüsseln einer Partition

Stellen Sie sicher, dass während der Durchführung einer Entschlüsselung alle Dateien auf der relevanten Datenpartition geschlossen sind.

1. Klicken Sie auf das Sophos SafeGuard Disk Encryption Symbol und wählen Sie **Disk-Verwaltung**.
2. Geben Sie Ihre SafeGuard Admin Anmeldedaten ein und klicken Sie auf **OK**.
3. Wählen Sie im Verwaltungsbereich die Option **Partitionen**. Alle verfügbaren Partitionen werden angezeigt.
4. Klicken Sie neben der Partition, die Sie verschlüsseln möchten, auf **Entschlüsseln**.
5. Die Entschlüsselung der ausgewählten Partitionen wird sofort gestartet.

Die Entschlüsselung von Partitionen ist auch in der Power-on Authentication möglich. Dies ist z. B. dann hilfreich, wenn sich das Betriebssystem nicht starten lässt.

Um die Partitionen auf Ihrem Mac zu entschlüsseln, wählen Sie **Fehlerbehebung > Partition permanent entschlüsseln**.

Hinweis: Starten Sie die Entschlüsselung nicht für nicht gemountete Partitionen und machen Sie den Mountvorgang bei einer Partition nicht während der Entschlüsselung rückgängig. Beides kann zu Datenverlust führen.

6 Benutzung von Sophos SafeGuard Disk Encryption über Terminal

Sie können Sophos SafeGuard Disk Encryption über Terminal (die Mac OS X Kommandozeilenschnittstelle) benutzen.

6.1 Kommandos

Die folgenden Kommandos sind über die "sgadmin" Kommandozeile verfügbar:

```
sgadmin --help | -h

sgadmin --status

sgadmin --add-user
    --type "user | admin"
    [--user "username"]
    [--password "password"]
    [--confirm-password "confirm password"]
    [--authenticate-user "admin username"]
    [--authenticate-password "admin password"]

sgadmin --add-recovery-user
    --user-to-recover "username"
    [--user "username"]
    [--password "password"]
    [--confirm-password "confirm password"]
    [--authenticate-user "admin username"]
    [--authenticate-password "admin password"]

sgadmin --add-recovery-users
    --user-to-recover "username"
    [--count "number of users"]
    [--authenticate-user "admin username"]
    [--authenticate-password "admin password"]

sgadmin --remove-user
    [--user "username"]
    [--authenticate-user "admin username"]
    [--authenticate-password "admin password"]

sgadmin --list-users
    [--authenticate-user "username"]
    [--authenticate-password "password"]

sgadmin --change-password
    [--user "username"]
    [--old-password "old password"]
    [--new-password "new password"]
    [--confirm-password "confirm password"]
```

```
sgadmin --recover-password
    [--user "username"]
    [--new-password "new password"]
    [--confirm-password "confirm password"]
    [--recovery-user "recovery username"]
    [--recovery-password "recovery password"]

sgadmin --backup-authentication
    --target "/path/to/target/folder"

sgadmin --backup-kernel
    --target "/path/to/target/folder"
    [--include-authentication]
    [--create-dmg]

sgadmin --encrypt "uuid | index | system | all"
    [--authenticate-user "admin username"]
    [--authenticate-password "admin password"]

sgadmin --decrypt "uuid | index | system | all"
    [--authenticate-user "admin username"]
    [--authenticate-password "admin password"]

sgadmin --pause "uuid | index | all"
    [--authenticate-user "admin username"]
    [--authenticate-password "admin password"]

sgadmin --resume "uuid | index | all"
    [--authenticate-user "admin username"]
    [--authenticate-password "admin password"]

sgadmin --enable-fast

sgadmin --disable-fast

sudo sgadmin --set-boot
```

6.2 Kommandobeschreibungen

Die folgende Tabelle beschreibt alle Kommandos und Optionen. Die in eckigen Klammern "[...]" stehenden Angaben sind optional. Benutzernamen und Kennwort werden interaktiv abgefragt, wenn sie nicht durch die Optionen bereitgestellt werden. Benutzernamen werden "sichtbar" eingegeben. Kennwörter werden "unsichtbar" eingegeben.

Befehl	Beschreibung
--help -h	Ruft den Hilfetext auf.

Befehl	Beschreibung
--status	Zeigt Statusinformationen an. Die mit <code>sgadmin --status</code> angezeigten Indexinformationen sind dynamisch. Das heißt, je nach Anzahl an gemounteten Partitionen können die Indexinformationen variieren.
--add-user	<p>Mit dem Kommando "add-user" lässt sich ein Benutzer zur Maschine hinzufügen. Hier ist nur der Parameter "type" erforderlich. Der Benutzername und das Kennwort sowie <code>authenticate user</code> und <code>authenticate password</code> können durch Optionen weitergegeben werden oder werden interaktiv abgefragt. Als erster Benutzer muss ein Admin-Benutzer hinzugefügt werden. Beim Hinzufügen des ersten Benutzers müssen <code>auth-user</code> und <code>auth-password</code> nicht angegeben werden. Optionen:</p> <ul style="list-style-type: none"> ■ <code>--type</code>: Benutzertyp (Admin, Benutzer) ■ <code>--user</code>: Name des Benutzers, der hinzugefügt werden soll. ■ <code>--password</code>: Kennwort des Benutzers, der hinzugefügt werden soll. ■ <code>--authenticate-user</code>: "Admin"-Benutzer, der sich authentisieren muss (wenn es sich nicht um den ersten Benutzer handelt). ■ <code>--authenticate-password</code>: "Admin"-Kennwort, das für die Authentisierung erforderlich ist (wenn es sich nicht um den ersten Benutzer handelt).
--add-recovery-user	<p>Fügt für einen spezifischen Benutzer einen Recovery-Benutzer hinzu. Optionen:</p> <ul style="list-style-type: none"> ■ <code>--user-to-recover</code>: Name des Benutzers, für den der Recovery-Benutzer hinzugefügt werden soll. ■ <code>--recovery-user</code>: Name des Recovery-Benutzers, der hinzugefügt werden soll. ■ <code>--recovery-password</code>: Kennwort des Benutzers, der hinzugefügt werden soll. ■ <code>--confirm-password</code>: Bestätigen Sie das Kennwort. ■ <code>--authenticate-user</code>: "Admin"-Benutzer, der sich authentisieren muss. ■ <code>--authenticate-password</code>: "Admin"-Kennwort, das für die Authentisierung erforderlich ist.

Befehl	Beschreibung
--add-recovery-users	<p>Der Parameter "count" gibt an, wie viele Recovery-Benutzer (beliebiger Benutzername und beliebiges Kennwort) erstellt und über "stdout" ausgegeben werden sollen. Optionen:</p> <ul style="list-style-type: none"> ■ --user-to-recover: Name des Benutzers, für den der Recovery-Benutzer hinzugefügt werden soll. ■ --count: Anzahl an Benutzern. ■ --authenticate-user: "Admin"-Benutzer, der sich authentisieren muss. ■ --authenticate-password: "Admin"-Kennwort, das für die Authentisierung erforderlich ist.
--remove-user	<p>Entfernt einen Benutzer. Optionen:</p> <ul style="list-style-type: none"> ■ --user: Name des Benutzers, der entfernt werden soll. ■ --authenticate-user: "Admin"-Benutzer, der sich authentisieren muss. ■ --authenticate-password: "Admin"-Kennwort, das für die Authentisierung erforderlich ist.
--list-users	<p>Listet alle "SafeGuard" Benutzer auf der Maschine auf. Optionen:</p> <ul style="list-style-type: none"> ■ --authenticate-user: Jeder Benutzer, der Zugriff auf die Maschine hat. ■ --authenticate-password: Kennwort des Benutzers
--change-password	<p>Ändert das Kennwort eines Benutzers. Optionen:</p> <ul style="list-style-type: none"> ■ --recover-password ■ --old-password: Altes Kennwort des Benutzers ■ --new-password: Neues Kennwort des Benutzers ■ --confirm-password: Bestätigung des neuen Kennworts

Befehl	Beschreibung
--recover-password	<p>Stellt das das Kennwort eines Benutzers wieder her. Optionen:</p> <ul style="list-style-type: none"> ■ --user: Name des Benutzers, für den das Kennwort wiederhergestellt werden soll. ■ --new-password: Neues Kennwort des Benutzers ■ --confirm-password: Bestätigung des neuen Kennworts ■ --recovery-user: Name des Recovery-Benutzers, der für den Recovery-Vorgang verwendet wird. Dieser wird nach einem erfolgreichen Recovery-Vorgang gelöscht. ■ --recovery-password: Kennwort des Recovery-Benutzers
--backup-authentication	<p>Erstellt einen Backup der Authentisierungs- und Schlüsseldaten, die zum Entsperren der Maschine verwendet werden. Optionen:</p> <ul style="list-style-type: none"> ■ --target: Vollständiger Pfad zum Zielordner (muss ein Ordner sein)
--backup-kernel	<p>Erstellt einen Backup des Pre-Boot Kernel. Optionen:</p> <ul style="list-style-type: none"> ■ --target: Vollständiger Pfad zum Zielordner (muss ein Ordner sein) ■ --include-authentication: Authentisierungs- und Schlüsseldaten werden mit einbezogen. ■ --create-dmg: Erstellt ein Disk Image (.dmg). Die Bezeichnung lautet "sgRecoveryMedia.dmg".
--encrypt	<p>Verschlüsselt eine Partition. Sie können entweder eine Partition UUID oder einen Index angeben. Beide lassen sich mit dem Kommando --status ermitteln. Sie können auch die Schlüsselwörter "system" und "all" verwenden. In diesem Fall werden entweder die Systempartition oder alle Partitionen verschlüsselt. Optionen:</p> <ul style="list-style-type: none"> ■ --authenticate-user: "Admin"-Benutzer, der sich authentisieren muss. ■ --authenticate-password: "Admin"-Kennwort, das für die Authentisierung erforderlich ist.

Befehl	Beschreibung
<p>--decrypt</p>	<p>Entschlüsselt eine Partition. Sie können entweder eine Partition UUID oder einen Index angeben. Beide lassen sich mit dem Kommando --status ermitteln. Sie können auch die Schlüsselwörter "system" und "all" verwenden. In diesem Fall werden entweder die Systempartition oder alle Partitionen entschlüsselt. Optionen:</p> <ul style="list-style-type: none"> ■ --authenticate-user: "Admin"-Benutzer, der sich authentisieren muss. ■ --authenticate-password: "Admin"-Kennwort, das für die Authentisierung erforderlich ist.
<p>--pause</p>	<p>Unterbricht einen Ver-/Entschlüsselungsvorgang. Sie können entweder eine Partition UUID oder einen Index angeben. Beide lassen sich mit dem Kommando --status ermitteln. Sie können auch das Schlüsselwort "all" verwenden. In diesem Fall werden entweder die Ver-/Entschlüsselungsvorgänge bei der Systempartition oder bei allen Partitionen unterbrochen. Optionen:</p> <ul style="list-style-type: none"> ■ --authenticate-user: "Admin"-Benutzer, der sich authentisieren muss. ■ --authenticate-password: "Admin"-Kennwort, das für die Authentisierung erforderlich ist.
<p>--resume</p>	<p>Nimmt einen Ver-/Entschlüsselungsvorgang wieder auf. Sie können entweder eine Partition UUID oder einen Index angeben. Beide lassen sich mit dem Kommando --status ermitteln. Sie können auch das Schlüsselwort "all" verwenden. In diesem Fall werden entweder die Ver-/Entschlüsselungsvorgänge bei der Systempartition oder bei allen Partitionen wieder aufgenommen. Optionen:</p> <ul style="list-style-type: none"> ■ --authenticate-user: "Admin"-Benutzer, der sich authentisieren muss. ■ --authenticate-password: "Admin"-Kennwort, das für die Authentisierung erforderlich ist.

Befehl	Beschreibung
--enable-fast	Führt alle Ver-/Entschlüsselungsvorgänge so schnell wie möglich aus. Standardmäßig ist die Geschwindigkeit für diese Vorgänge gedrosselt. Bei Ausführung dieses Kommandos werden die Vorgänge nicht gedrosselt. Dadurch sollte sich die Gesamtgeschwindigkeit um 20 bis 30 Prozent steigern lassen.
--disable-fast	Aktiviert das Standardverhalten (Drosselung) für Ver-/Entschlüsselungsvorgänge.
--set-boot	Setzt das Standard-Betriebssystem wieder auf OS X.

7 Time Machine Backups

Die folgenden Komponenten von Sophos SafeGuard Disk Encryption sollten von Time Machine Backups ausgenommen werden:

- /.com.sophos
- /System/Library/Extensions/sgbiodrv.kext
- /usr/sbin/sgd
- /usr/bin/sgadmin
- /Library/Sophos SafeGuard
- /Library/LaunchDaemons/com.sophos.sgd.plist
- /Library/LaunchAgents/com.sophos.sguimenu.plist
- /Library/LaunchAgents/com.sophos.sgsynclang.plist
- /Applications/sgui.app

8 Unterstützte Hardware und Konfigurationen

■ Hardware (nur Intel-basierend)

- MacBook
- MacBook Pro
- MacBook Air
- iMac
- Mac mini
- Mac Pro

■ EFI

- EFI32 (Firmware)
- EFI64 (Firmware)

Mit dem folgenden Terminalbefehl lässt sich die EFI Firmware überprüfen:

```
"ioreg -l -p IODeviceTree | grep firmware-abi"
```

Es sollte der Wert "firmware-abi" = <"EFI64" >oder "firmware-abi" = <"EFI32" > geliefert werden.

■ Betriebssystem

- 10.5 (Leopard) aktueller Patch Level, 32 Bit Kernel, 32 Bit/64Bit User-Modus
- 10.6 (Snow Leopard) aktueller Patch Level, 32 Bit/64 Bit Kernel, 32 Bit/64Bit User-Modus

■ Update

- Ein Update von Version 5.50 auf 5.50.1 ist ohne vorherige Entschlüsselung der Festplatte möglich.

8.1 Bootcamp-Unterstützung

Eine Bootcamp-Partition muss auf einer Maschine vor der Installation von Sophos SafeGuard Disk Encryption eingerichtet werden. Das Einrichten oder Entfernen von Bootcamp nach der Installation von Sophos SafeGuard Disk Encryption wird nicht unterstützt. Beachten Sie, dass das Ändern des Partitionslayouts sowie das Ändern der Partitionsgröße nach der Installation von Sophos SafeGuard Disk Encryption nicht unterstützt wird.

Wenn das Standard-Betriebssystem von OS X zu Windows geändert wurde, lässt es sich weder mit dem Windows Bootcamp Control Panel noch mit der OS X Startup Disk Utility wieder auf OS X einstellen. Dies muss über die von Sophos SafeGuard Disk Encryption bereitgestellte Funktionalität erfolgen.

Für das Zurücksetzen des Standard-Bootsystems auf OS X haben Sie folgende Möglichkeiten:

1. Über die Benutzeroberfläche:

- Öffnen Sie die **SafeGuard Disk-Verwaltung**.
- Öffnen Sie das **Bearbeiten** Menü und wählen Sie **Dieses Betriebssystem standardmäßig starten**. Hier ist eine Anmeldung als OS X Administrator notwendig.

2. Über Terminal:

- Öffnen Sie ein **Terminal** und geben Sie `sudo sgadmin --set-boot` ein. Hier ist eine Anmeldung als OS X Administrator notwendig.

9 Nicht unterstützte Hardware, Konfigurationen und Vorgänge

- **Hardware**
 - PowerPC-basierende Hardware
- **Betriebssystem**
 - 10.4 und frühere
- **Bootcamp und SafeGuard Enterprise/SafeGuard Easy for Windows**
 - SafeGuard Enterprise for Windows unterstützt keine Apple Hardware und kann nicht in einer Bootcamp/Windows-Umgebung installiert werden. Diese Einschränkung gilt, bis in der SafeGuard Enterprise for Windows Dokumentation explizit andere Angaben gemacht werden.
- **Für das Produkt gelten folgende EINSCHRÄNKUNGEN:**
 - Sophos SafeGuard Disk Encryption for Mac unterstützt keine Multi-Boot-Systeme. Das heißt, mehrere OS X Installationen auf einem Mac werden nicht unterstützt.
 - Installieren Sie die Software nicht auf Systemen mit mehr als 50 Partitionen.
 - Wir empfehlen, nicht mehr als fünf Partitionen gleichzeitig zu verschlüsseln.
 - **Tastatur:** Der Tastatur-Übersetzungscode setzt nur die üblichen Tasten und Tasten mit einer Umschalttaste um. Für nicht-numerische Tasten des Zahlenblocks kann nicht garantiert werden, dass eine Umsetzung in dieselbe Zeichenfolge funktioniert, wenn das Layout der Tastatur geändert wird. Benutzen Sie daher nur die Tasten "0-9" aus diesem Tastenblock. Die Ursache hierfür ist, dass EFI nur ein äquivalentes US ANSI Zeichen ausgibt, keine Modifikatortasten. Während der Umsetzung, erhält die normale Taste der Tastatur Vorrang vor der Taste des numerischen Tastenblocks. Dies hat Auswirkungen auf die nicht-numerischen Tasten des numerischen Tastenblocks ('=', '/', ', ', '-', '+'). Diese Tasten werden aufgrund des Tastaturlayouts u. U. in andere Zeichen umgesetzt. So wird z. B. auf einer deutschen Tastatur die " Taste des numerischen Tastaturblocks in das Tastatur-Zeichen '(' umgesetzt. Der Code wurde mit folgenden Tastaturen entwickelt und getestet: US, Französisch, Deutsch Für andere Tastaturen kann nicht garantiert werden, dass die Umsetzung funktioniert.
 - **Partitionierung** Nach der Installation von Sophos SafeGuard Disk Encryption for Mac kann das Partitionierungs-Layout nicht mehr geändert werden. Das heißt, Änderungen mit "gpt" oder "diskutil" sind nicht möglich. Wird Partitionierung einer Maschine verändert, muss sie neu installiert werden.

- **Formatierung:** Die Formatierung verschlüsselter Partitionierung wird nicht unterstützt. Wenn Sie alle Daten entfernen möchten, empfehlen wir, die Dateien zu löschen oder die Partition zu entschlüsseln, sie zu formatieren und sie danach wieder zu verschlüsseln. Beachten Sie, dass für die Verschlüsselung nur HFS+ Partitionen unterstützt werden.
- **Target Disk Mode:** Die Benutzung von Target Disk Mode wird nicht unterstützt, wenn sowohl die lokale Maschine als auch die Target Disk verschlüsselt sind. Target Disk Mode wird unterstützt, wenn die lokale Maschine nicht verschlüsselt ist und die Target Disk verschlüsselt ist oder umgekehrt.
- **Verwendung von diskutil von einem über Network Boot gestarteten System aus**
Verwenden Sie diskutil nicht von einem System aus, das über Network Boot gestartet wurde und bei dem lokale Partitionen verschlüsselt sind. In diesem Fall erkennt diskutil die verschlüsselten Partitionen nicht und versucht, sie zu initialisieren. Dies führt zu Datenverlust.
- **Partitionen löschen** Das Löschen von Partitionen, bei denen gerade eine initiale Verschlüsselung oder eine endgültige Entschlüsselung durchgeführt wird, wird nicht unterstützt. Das Löschen von verschlüsselten Partitionen wird auch nicht unterstützt. Partitionen müssen erst entschlüsselt werden.
- **Nicht gemountete Partitionen und Ver-/Entschlüsselung** Für nicht gemountete Partitionen kann die initiale Verschlüsselung bzw. die endgültige Entschlüsselung nicht gestartet werden. Während eine Partition ver- oder entschlüsselt wird, kann außerdem der Mount-Vorgang nicht rückgängig gemacht werden. Dies kann zu Datenverlust führen.
- **OS-Aktualisierungen (z. B. 10.5 auf 10.6) werden nicht unterstützt:** Für Aktualisierungen müssen Sie zunächst die Partitionen Ihres Mac entschlüsseln und dann Sophos SafeGuard Disk Encryption for Mac deinstallieren. Danach können Sie das Betriebssystem aktualisieren, das Produkt wieder installieren und die Partitionen wieder verschlüsseln.
- **Deep Sleep:** Wenn Sophos SafeGuard Disk Encryption for Mac installiert ist, wird das Ruhezustand-Feature "Deep Sleep" nicht unterstützt. Das Feature ist deaktiviert. Einige Anwendungen speichern Ihre Daten nicht automatisch, wenn der Sleep-Modus aktiviert ist. Wenn der Sleep-Modus für längere Zeit benutzt wird, der Mac nicht an das Stromnetz angeschlossen ist und eine solche Anwendung mit nicht gespeicherten Daten geöffnet ist, kann es zu Datenverlust kommen.
- **Aktualisierung von einer Beta3-Installation:** Das Benutzerkonto, mit dem die Aktualisierung initiiert wird, muss entweder der Administratorengruppe angehören, oder es muss vor der Installation folgender Befehl ausgeführt werden: `sudo chmod a+r / .com.sophos.`

- **Defekte Sektoren:** Wir empfehlen, die Software nicht zu installieren, wenn sich auf Ihrer Festplatte defekte Sektoren befinden. Werden defekte Sektoren gefunden, so wird die initiale Verschlüsselung zwar nicht abgebrochen, es wird jedoch im Kernel Log ein Log-Eintrag erstellt.
- **Initiale Verschlüsselung/endgültige Entschlüsselung bei Datenpartitionen:** Bevor Sie eine Datenpartition verschlüsseln, stellen Sie sicher, dass alle Dateien auf dieser Partition geschlossen sind. Stellen Sie sicher, dass während der Durchführung einer Entschlüsselung alle Dateien auf der relevanten Datenpartition geschlossen sind.

10 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.

11 Rechtlicher Hinweis

Copyright © 2010 - 2011 Sophos Group. Alle Rechte vorbehalten. SafeGuard ist ein eingetragenes Warenzeichen der Sophos Group.

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.

11.1 Disclaimer and Copyright for 3rd Party Software

Portions of this software are copyright © 2010 The FreeType Project (www.freetype.org). All rights reserved.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)

Gladman AES

Copyright (c) 1998-2007, Brian Gladman, Worcester, UK. All rights reserved.

LICENSE TERMS

The free distribution and use of this software is allowed (with or without changes) provided that:

1. source code distributions include the above copyright notice, this list of conditions and the following disclaimer;
2. binary distributions include the above copyright notice, this list of conditions and the following disclaimer in their documentation;
3. the name of the copyright holder is not used to endorse products built using this software without specific written permission.

DISCLAIMER

This software is provided 'as is' with no explicit or implied warranties in respect of its properties, including, but not limited to, correctness and/or fitness for purpose.