SOPHOS

Security made simple.

Sophos SafeGuard File Encryption for Mac

Administratorhilfe

Produktversion: 7

Stand: Dezember 2014

Inhalt

1 Über Sophos SafeGuard File Encryption for Mac

Sophos SafeGuard File Encryption für Mac erweitert den Schutz der Daten, der von Sophos SafeGuard Enterprise geboten wird, von Windows auch in die Mac-Welt. Ermöglicht wird eine dateibasierte Verschlüsselung auf lokalen Laufwerken, auf Netzlaufwerken, auf Wechsellaufwerken und in der Cloud.

Mit SafeGuard File Encryption for Mac können Sie Dateien sicher ver- und entschlüsseln und diese Dateien mit anderen Benutzern zwischen Mac-Rechnern und PCs austauschen.

Um Dateien zu lesen, die mit SafeGuard Enterprise auf mobilen Geräten verschlüsselt wurden, verwenden Sie Sophos Mobile Encryption für iOS oder Android.

Im SafeGuard Management Center definieren Sie die Regeln für die dateibasierte Verschlüsselung in File Encryption-Richtlinien. In den File Encryption-Richtlinien geben Sie die Zielordner für File Encryption, den Verschlüsselungsmodus und den Schlüssel für die Verschlüsselung an. Diese Zentralverwaltung stellt sicher, dass identische Ordner und Verschlüsselungsschlüssel auf unterschiedlichen Plattformen verarbeitet werden.

1.1 Über dieses Dokument

Dieses Dokument beschreibt, wie Sophos SafeGuard File Encryption for Mac installiert, konfiguriert und verwaltet wird.

Mehr zum Arbeiten mit dem Management Center und zu Richtlinien finden Sie in der *SafeGuard Enterprise Administratorhilfe*.

Benutzerrelevante Informationen finden Sie in der *Schnellstart-Anleitung für Sophos SafeGuard File Encryption for Mac*.

1.2 Fachbegriffe und Akronyme

Die folgenden Fachbegriffe und Akronyme werden in diesem Dokument verwendet:

Fachbegriff oder Akronym	Bedeutung oder Erläuterung
FUSE	Filesystem in Userspace (siehe http://osxfuse.github.io/)
GUID	Ein Globally Unique Identifier (GUID) ist eine global eindeutige Zahl, die in verteilten Computersystemen zum Einsatz kommt
Secured Folder	Sicherer Ordner, für den im SafeGuard Management Center eine Regel festgelegt wurde. Die Regel gibt vor, dass die Inhalte des Ordners verschlüsselt werden.

Fachbegriff oder Akronym	Bedeutung oder Erläuterung
SSL	Secure Sockets Layer: Netzwerkprotokoll zur sicheren Übertragung von Daten über das Internet.

2 Installation

Das folgende Kapitel beschreibt die Installation von SafeGuard File Encryption auf Mac OS X Client-Rechnern. Eine Beschreibung zur Installation der Administrationsumgebung (Backend) finden Sie in der *SafeGuard Enterprise Installationsanleitung*.

Zwei Installationsarten für Mac OS X Client-Rechner gibt es:

- manuelle (beaufsichtigte) Installation
- automatisierte (unbeaufsichtigte) Installation.

Hinweis: Wenn Sie SafeGuard Disk Encryption 6.01 oder älter installiert haben, müssen Sie diese Version vor der Installation von SafeGuard File Encryption für Mac Version 7 deinstallieren.

Wenn Sie SafeGuard File Encryption und SafeGuard Native Device Encryption (hieß bis Version 6.10 SafeGuard Disk Encryption) verwenden möchten, muss es sich in beiden Fällen um Version 7 handeln. Die Verwendung unterschiedlicher Versionen dieser Produkte auf demselben Mac wird nicht unterstützt.

Das Installer Package ist signiert und OS X versucht, diese Signatur zu validieren. Ist die Internetverbindung langsam oder nicht richtig konfiguriert, kann es eventuell zu Verzögerungen beim Installationsvorgang von bis zu 20 Minuten kommen.

2.1 Installationsvoraussetzungen

Stellen Sie vor dem Beginn der Installation sicher, dass das SafeGuard Enterprise-SSL-Serverzertifikat in den Systemschlüsselbund importiert wurde und für SSL auf **Immer vertrauen** gesetzt ist.

Hinweis: Es darf nicht am Anmelde-Schlüsselbund gespeichert werden.

1. Bitten Sie Ihren SafeGuard Server-Administrator, Ihnen das zertifikat (Datei <Zertifikatsname>.cer).zur Verfügung zu stellen.
2. Importieren Sie die Datei *Zertifikatsname>.cer*) in Ihre Schlüsselbundverwaltung. Wählen Sie dazu **Programme** - **Dienstprogramme** und doppelklicken Sie **Schlüsselbundverwaltung.app**.
3. Wählen Sie im linken Fensterteil **System**.
4. Öffnen Sie einen Finder und wählen Sie die Datei *<Zertifikatsname>.cer* von oben.
5. Ziehen Sie die Zertifikatsdatei in die Schlüsselbundverwaltung.
6. Sie werden aufgefordert, Ihr Mac-OS X-Kennwort einzugeben.
7. Klicken Sie nach der Kennworteingabe auf **Schlüsselbund ändern**, um den Vorgang zu bestätigen.
8. Doppelklicken Sie dann auf die Datei *<Zertifikatsname>.cer* . Klicken Sie auf den Pfeil neben **Vertrauen**, um die Vertrauenseinstellungen anzuzeigen.
9. Für **Secure Sockets Layer (SSL)** wählen Sie die Option **Immer vertrauen**.
10. Schließen Sie den Dialog. Sie werden erneut aufgefordert, Ihr Mac-OS X-Kennwort einzugeben.

11. Geben Sie das Kennwort ein und bestätigen Sie mit ein Klick auf **Einstellungen aktualisieren**. Ein blaues Plus-Zeichen in der unteren rechten Ecke des Zertifikats-Symbols zeigt Ihnen, dass dieses Zertifikat als vertrauenswürdig für alle Benutzer eingestuft ist.

12. Öffnen Sie einen Webbrowser und stellen Sie sicher, dass Ihr SafeGuard Enterprise Server unter **`https://<Servername>//SGNSRV`** verfügbar ist.

Nun können Sie mit der Installation beginnen.

Hinweis:

Das Zertifikat kann auch importiert werden, indem der folgende Befehl ausgeführt wird: **`sudo /usr/bin/security add-trusted-cert -d -k /Library/Keychains/System.keychain -r trustAsRoot -p ssl "/<Ordner>/<Zertifikatsname>.cer"`**. Dieser Befehl kann auch für eine automatisierte Installation mittels Skript verwendet werden. Ändern Sie die Namen des Ordners und des Zertifikats entsprechend Ihren Anforderungen.

Hinweis:

Wenn Sie den oben beschriebenen Vorgang umgehen möchten, können Sie den Befehl **`sudo sgfsadmin --disable-server-verify`** ausführen (siehe auch Kommandozeilen-Optionen (Seite 19)). Wir empfehlen nicht, diese Option zu verwenden, da dadurch eine Sicherheits-Schwachstelle entstehen kann.

2.2 Manuelle (beaufsichtigte) Installation

Eine manuelle (oder beaufsichtigte) Installation ermöglicht Ihnen, die Installation Schritt-für-Schritt zu steuern und zu testen. Sie wird auf Mac-Einzelplatzrechnern durchgeführt.

Hinweis:

Stellen Sie sicher, dass FUSE for OS X (OSXFUSE) Version 2.7.0 oder höher installiert ist. Mehr Information zu FUSE for OS X und zu Download-Optionen finden Sie unter http://osxfuse.github.io/.

Stellen Sie sicher, dass die Serververbindung wie unter Installationsvoraussetzungen (Seite 5) beschrieben korrekt eingerichtet wurde.

1. Öffnen Sie *Sophos SafeGuard FE.dmg*.
2. Nachdem Sie die Readme-Datei gelesen haben, doppelklicken Sie auf *Sophos SafeGuard FE.pkg* und folgen Sie den Anweisungen des Installationsassistenten. Sie werden nach Ihrem Kennwort gefragt, um die Installation neuer Software zu erlauben. Das Produkt wird im Ordner */Library/Sophos SafeGuard FS/* installiert.
3. Klicken Sie auf **Schließen**, um die Installation abzuschließen.
4. Öffnen Sie die **Systemeinstellungen** und klicken Sie auf das Sophos Encryption-Symbol, um die Produkteinstellungen anzuzeigen.

5. Klicken Sie auf die Registerkarte **Server**.
6. Werden Server und Zertifikatsdetails angezeigt, so überspringen Sie die nächsten Schritte, gehen zu Schritt 11 und klicken **Synchronisieren**. Wird keine Information angezeigt, so fahren Sie mit dem nächsten Schritt fort.
7. Wählen Sie die Konfigurations-Zip-Datei aus (nähere Informationen zum Erstellen eines Konfigurationspakets für Mac-Endpoints finden Sie unter *SafeGuard Enterprise Administrator-Hilfe*, *Arbeiten mit Konfigurationspaketen* > *Erstellen von Konfigurationspaketen für Macs*).

8. Ziehen Sie die Zip-Datei in den **Server**-Dialog und lassen Sie sie in der Dropzone los.
9. Sie werden aufgefordert, Ihr Mac-Administratorkennwort einzugeben. Geben Sie das Kennwort ein und klicken Sie zur Bestätigung auf **OK**.
10. Geben Sie Ihr Mac-Kennwort ein, um Ihr SafeGuard Benutzerzertifikat anzufordern.
11. Überprüfen Sie die Verbindung zum SafeGuard Enterprise Server. Details zum Unternehmenszertifikat werden im unteren Teil des **Server**dialogs angezeigt. Klicken Sie dann auf **Synchronisieren**. Eine erfolgreichen Verbindung erkennen Sie an einem aktualisierten Zeitstempel (Registerkarte **Server**, **Serverinfo**-Bereich, **Letzter Serverkontakt:**). Bei einer unterbrochenen Verbindung erscheint das folgende Symbol:

    

    Mehr Information finden Sie in der System-Logdatei.

    Mehr Informationen zur Synchronisation und zur Registerkarte Server (Seite 15) finden Sie auch in .

2.3 Automatisierte (unbeaufsichtigte) Installation über Remote Management Software

Eine automatisierte (unbeaufsichtigte) Installation erfordert keinen Benutzereingriff während des Installationsprozesses.

Der folgende Abschnitt beschreibt die grundsätzlichen Schritte einer automatisierten (unbeaufsichtigten) Installation von SafeGuard File Encryption. Je nach Managementsoftware-Lösung, die Sie verwenden, können die tatsächlichen Schritte von der Beschreibung abweichen. Verwenden Sie Ihre installierte Managementsoftware.

Hinweis:

Installieren Sie die Pakete in der korrekten Reihenfolge.

Um SafeGuard File Encryption for Mac auf Client-Rechnern zu installieren, gehen Sie wie folgt vor:

1. Laden Sie die Installationsdatei *Sophos SafeGuardFS.pkg* herunter.
2. Kopieren Sie die Datei auf die Zielrechner.
3. Installieren Sie die Datei auf den Zielrechnern. Wenn Sie Apple Remote Desktop verwenden, sind die Schritte 2 und 3 zu einem einzelnen Schritt zusammengefasst.
4. Wählen Sie die Konfigurations-Zipdatei (in der *SafeGuard Enterprise Administratorhilfe* Version 7.00, Abschnitt *Mit Konfigurationspaketen arbeiten* > *Erzeugen eines Konfigurationspakets für Macs* finden Sie eine Beschreibung wie Konfigurations-Zipdateien auf Macs erstellt werden) und kopieren Sie sie auf die Zielrechner.
5. Führen Sie auf den Zielrechnern das folgende Kommando aus:

    ```
    /usr/bin/sgfsadmin --import-config /Pfad/zur/Datei.zip
    ```

    Passen Sie */Pfad/zur/Datei* auf Ihre Einstellungen an. Dieses Kommando muss mit Administratorrechten ausgeführt werden. Wenn Sie Apple Remote Desktop verwenden, geben Sie **`root`** in das Feld **Benutzername** ein um festzulegen, welcher Benutzer das Kommando oben ausführt.

6. Sie können Ihrem Workflow weitere Schritte je nach Ihren spezifischen Einstellungen hinzufügen wie z.B. die Zielrechner herunterzufahren.

3 Empfehlungen und Beschränkungen

3.1 Empfehlungen

Verringern Sie den Administrationsaufwand

- Minimieren Sie die Anzahl der Mount Points (bzw. sicheren Ordner).
- **Deaktivieren Sie die Option "Bestätigung vor Erstellen mobiler Accounts einholen"**

  Wenn Sie mobile Accounts auf Mac-Rechnern erstellen oder verwenden, stellen Sie sicher, dass die Option **Bestätigung vor Erstellen mobiler Accounts einholen** deaktiviert ist. Ist die Option aktiviert, könnte der Benutzer "Nicht erstellen" auswählen. Dies würde dazu führen, dass ein unvollständiger OS X Benutzer angelegt wird, z. B. ein Benutzer, der kein lokales Basisverzeichnis hat.

  Zum Deaktivieren der Option sind folgende Schritte erforderlich:

  1. Öffnen Sie die **Systemeinstellungen** und klicken Sie auf **Benutzer & Gruppen**.
  2. Klicken Sie auf das Schloss-Symbol und geben Sie dann Ihr Kennwort ein.
  3. Wählen Sie den Benutzer.
  4. Klicken Sie auf **Anmeldeoptionen**.
  5. Wählen Sie **Netzwerkaccount-Server** und klicken Sie auf **Bearbeiten...**
  6. Wählen Sie die Active Directory-Domäne.
  7. Klicken Sie auf **Verzeichnisdienste öffnen...**
  8. Klicken Sie auf das Schloss-Symbol, geben Sie dann Ihr Kennwort ein und klicken Sie **Konfiguration ändern**.
  9. Wählen Sie Active Directory und klicken Sie auf das Bearbeiten-Symbol.
  10. Klicken Sie auf den Pfeil links neben **Erweiterte Optionen einblenden**.
  11. Wählen Sie **Mobilen Account bei Anmeldung erstellen** und deaktivieren Sie die Option **Bestätigung vor Erstellen mobiler Accounts einholen**.
  12. Bestätigen Sie Ihre Auswahl mit **Ok**.

3.2 Einschränkungen

- **Maximale Anzahl an sicheren Ordnern (Aktivierungspunkte bzw. Mount Points) auf einem Client**

  Auf jedem Mac OS X Client kann es maximal 24 sichere Ordner (Aktivierungspunkte bzw. Mount Points) geben. Sind mehrere Benutzer auf einem Rechner angemeldet, müssen Sie die Mount Points aller angemeldeten Benutzer addieren. Wenn Sie weitere Produkte auf Ihrem Mac nutzen, die ebenfalls auf FUSE für OS X zurückgreifen, müssen Sie diese Mount Points bei der insgesamt zulässigen Anzahl von 24 ebenfalls berücksichtigen.

- **Permanente Versionsspeicherung in sicheren Ordnern nicht verfügbar**

  Beim Öffnen einer Datei (die zuvor geändert wurde) von einem sicheren Ordner aus ist die Standardfunktionalität **Alle Versionen durchsuchen...** nicht verfügbar.

- **Ausgeschlossene Ordner**

Die folgenden Ordner werden von der Verschlüsselung ausgenommen:

- **Ordner werden ausgenommen, aber nicht ihre Unterordner:**
  - <Root>/
  - <Root>/Volumes/
  - <User Profile>/
- **Ordner sowie ihre Unterordner werden ausgenommen:**
  - <Desktop>/
  - <Root>/bin/
  - <Root>/sbin/
  - <Root>/usr/
  - <Root>/private/
  - <Root>/dev/
  - <Root>/Applications/
  - <Root>/System/
  - <Root>/Library/
  - <User Profile>/Library/
  - /<Removables>/SGPortable/
  - /<Removables>/System Volume Information/

Das bedeutet, dass z. B. eine Verschlüsselungsregel für das Root einer zusätzlichen Partition (<Root>/Volumes/) keine Wirkung hat, auch wenn sie als erhaltene Richtlinie angezeigt wird.

Eine Verschlüsselungsregel für <Root>/abc wirkt sich aus, aber nicht eine Verschlüsselungsregel für <Root>/private/abc.

- **Nach Dateien suchen**
  - **Spotlight-Suche**

    Die Spotlight-Suche funktioniert nicht bei verschlüsselten Dateien, daher werden bei der Suche in sicheren Ordnern keine Treffer zurückgegeben.

  - **Dateien mit Etikett**

    Die Suche nach Dateien mit Etikett funktioniert nicht in sicheren Ordnern.

- **CDs brennen**

  Es ist nicht möglich, eine verschlüsselte CD zu brennen.

- **Sichere Ordner freigeben**

  Ein sicherer Ordner kann nicht über das Netzwerk freigegeben werden. Existiert z. B. eine Regel für <Documents>, kann dieser Ordner nicht mehr freigegeben werden.

- **Dateien löschen**

  Beim Löschen von Dateien aus einem sicheren Ordner (Aktivierungspunkt bzw. Mount Point) wird eine Meldung angezeigt, mit der Sie aufgefordert werden, den Löschvorgang

zu bestätigen. Gelöschte Dateien werden nicht in den Papierkorb verschoben und können somit nicht wiederhergestellt werden.

- **SafeGuard Portable**

  SafeGuard Portable ist nicht für Mac OS X verfügbar.

- **Time Machine verwenden**

  Wenn Sie Time Machine für einen verschlüsselten Ordner verwenden, werden keine alten Versionen angezeigt. Die Sicherungen sind jedoch vorhanden – sofern Sie Time Machine aktiviert haben –, sie sind lediglich versteckt. Gehen Sie wie folgt vor:

  - Öffnen Sie Time Machine (z. B. indem Sie "Time Machine" in die Spotlight-Suche eingeben). Die Inhalte Ihres Stammverzeichnisses werden angezeigt.
  - Drücken Sie **Shift + CMD + G** (für "Gehe zu Ordner:") und geben Sie den versteckten Pfad des verschlüsselten Ordners ein, den Sie wiederherstellen möchten. Beispiel: Wenn der verschlüsselte Ordner, mit dem Sie normalerweise arbeiten, /Users/admin/Documents heißt, geben Sie /Users/admin/.sophos_safeguard_Documents/ ein.
  - Suchen Sie die Datei, die Sie wiederherstellen möchten, klicken Sie auf das Rad-Symbol in der Time Machine Menüleiste und wählen Sie **<file name> wiederherstellen nach...**. Wenn Sie von Time Machine zu Ihrem Desktop zurückkehren, ist Ihre Datei wiederhergestellt und kann entschlüsselt werden.

    Hinweis: Sie können die Inhalte der Dateien in dem versteckten Pfad nicht lesen. Die Sicherung enthält somit nur verschlüsselte Daten und Ihre Inhalte bleiben geschützt.

- **AirDrop verwenden**

  Verschlüsselte Dateien können mit AirDrop übertragen werden. Stellen Sie sicher, dass das Zielgerät verschlüsselte Dateien verarbeiten kann, da sich die Anwendungen sonst möglicherweise anders verhalten als erwartet.

- **Handoff**

  Handoff für verschlüsselte Dateien wird nicht unterstützt.

- **Netzlaufwerke mit `autofs` aktivieren**

  Netzlaufwerke, für die eine Richtlinie gilt und die beim Start automatisch aktiviert werden, werden von Sophos SafeGuard File Encryption nicht erkannt. Solche Aktivierungspunkte bzw. Mount Points können nicht verarbeitet werden, weil der ursprüngliche Mount Point nicht ersetzt werden kann.

4 Konfiguration

Sophos SafeGuard File Encryption für Mac OS X wird über das SafeGuard Management Center verwaltet. Das folgende Kapitel beschreibt ausschließlich die Mac-spezifischen Konfigurationseinstellungen. Alle Management Center-Standardfunktionen sind in der *SafeGuard Enterprise Administrator-Hilfe* beschrieben. Spezifische Informationen zu Dateiverschlüsselungsrichtlinien finden Sie im Kapitel "Richtlinieneinstellungen" und in den darauf folgenden Kapiteln in der *SafeGuard Administratorhilfe*.

Hinweis:

SafeGuard File Encryption für Mac verwendet nur Richtlinien vom Typ **Dateiverschlüsselung** und **Allgemeine Einstellungen**. Das bedeutet, dass Sie nur eine **Dateiverschlüsselungs**richtlinie für die Verwaltung der Datenverschlüsselung auf dem lokalen Dateisystem, Wechselmedien, Netzlaufwerken und Cloud-Speicher benötigen. **Geräteschutz**-Richtlinien (einschließlich der Richtlinien **Cloud-Speicher** und **Verschlüsselung von Wechselmedien**) werden für SafeGuard File Encryption für Mac OS X ignoriert. Weisen Sie den Benutzerobjekten immer **Dateiverschlüsselung** zu. Richtlinien vom Typ **Dateiverschlüsselung**, die Endpoints zugewiesen werden, haben keine Wirkung auf OS X Endpoints.

Hinweis:

Im SafeGuard Enterprise Management Center müssen Pfade mit Backslashes eingegeben werden. Sie werden Mac Client-seitig automatisch in Schrägstriche umgewandelt.

4.1 Zentral verwaltete Konfigurationsoptionen

Die folgenden Optionen werden zentral im Management Center konfiguriert:

- **Richtlinien**
- **Schlüssel**
- **Zertifikate**

  Das SafeGuard Enterprise Backend stellt ein X.509-Benutzerzertifikat zur Verfügung. Wenn Sie sich das erste Mal anmelden, wird ein Zertifikat generiert. Das Zertifikat schützt den Schlüsselring der Benutzer. Nähere Informationen darüber, wie Sie nach dem Anmelden ein Zertifikat anfordern können, finden Sie in der *Schnellstart-Anleitung*.

- **Server-Verbindungsintervall**

Hinweis: Mehr zu den oben genannten Optionen finden Sie in der *SafeGuard Enterprise Administratorhilfe*.

4.2 Lokal verwaltete Konfigurationsoptionen

Die folgenden Optionen werden lokal auf dem Mac Client-Rechner konfiguriert:

- **Datenbankinformation synchronisieren**

  Verwenden Sie den Befehl **`sgfsadmin --synchronize`**, um Datenbankinformationen vom Management Center, wie z. B. Richtlinien, Schlüssel und Zertifikate, zu synchronisieren.

- **System Menü aktivieren oder deaktivieren**

  Verwenden Sie den Befehl **`sgfsadmin --enable-systemmenu`**, um das System-Menü in der rechten oberen Bildschirmecke zu aktivieren.

  Verwenden Sie den Befehl **`sgfsadmin --disable-systemmenu`**, um das System-Menü in der rechten oberen Bildschirmecke zu deaktivieren.

  Informationen zu beiden Optionen finden Sie auch unter Sophos SafeGuard File Encryption System-Menü (Seite 18).

Eine vollständige Übersicht aller Kommandozeilen-Optionen (Seite 19) finden Sie in .

5 Arbeiten mit File Encryption for Mac

In der separaten Schnellstart-Anleitung für File Encryption werden die benutzerrelevanten Aspekte der Anwendung erklärt. Sie finden die aktuelle Version der Produktdokumentation auf unserer Dokumentations-Webseite unter http://www.sophos.com/de-de/support/documentation.aspx.

In den folgenden Abschnitten finden Sie Informationen zum Arbeiten mit File Encryption for Mac aus der Sicht eines Administrators.

5.1 Wie funktioniert Verschlüsselung?

Jede verschlüsselte Datei ist mit einem zufallsgenerierten Schlüssel namens Data Encryption Key (DEK) unter Verwendung des AES-256-Algorithmus verschlüsselt. Dieser zufällig generierte und eindeutige DEK wird verschlüsselt und als Datei-Header zusammen mit der verschlüsselten Datei gespeichert. Dadurch erhöht sich die ursprüngliche Dateigröße um 4 KB.

Der DEK wird mit einem Key Encryption Key (KEK) verschlüsselt. Der KEK wird in der zentralen SafeGuard Enterprise-Datenbank gespeichert. Der Sicherheitsbeauftragte ordnet diesen KEK einem einzelnen Benutzer, einer Benutzergruppe oder einer Organisationseinheit zu.

Um eine verschlüsselte Datei zu entschlüsseln, muss der Benutzer den KEK speziell für diese Datei an seinem Schlüsselring haben.

5.2 Initialverschlüsselung

Gehen Sie auf Client-Seite wie folgt vor:

1. Öffnen Sie die **Systemeinstellungen**.
2. Klicken Sie auf das Sophos Encryption-Symbol.

   

3. Wählen Sie das Register **Richtlinien**.
4. Wechseln Sie in die Ansicht **Lokal übersetzter Pfad** sofern diese nicht bereits geöffnet ist. Nun können Sie

   a) alle Richtlinien erzwingen. Klicken Sie dazu auf die Schaltfläche **Erzwinge alle Richtlinien** im unteren Fensterteil.

   oder

   b) eine einzelne Richtlinie auswählen und auf **Erzwinge Richtlinie** klicken.

   Hinweis: Trennen Sie keine Geräte, auf denen gerade die Initialverschlüsselung ausgeführt wird.

   Hinweis: Wenn Sie Details und Inhalte des lokal übersetzten Pfads sehen wollen, wählen Sie den Pfad aus der Liste und klicken Sie auf **Im Finder anzeigen**. Das Finder-Fenster öffnet sich und zeigt den ausgewählten Pfad und dessen Inhalte (sofern verfügbar) an.

5.3 Umgang mit Passwörtern

Der Sophos SafeGuard Schlüsselring ist mit einem Benutzerzertifikat gesichert. Der entsprechende private Schlüssel ist mit dem OS X Kennwort geschützt.

Das Kennwort wird benötigt, damit das Zertifikat erzeugt werden kann, wenn der Benutzer nicht in SafeGuard Enterprise angelegt wurde.

Lokales Ändern des Kennworts

Benutzer können ihre Kennwörter lokal unter **Systemeinstellungen > Benutzer & Gruppen** ändern. Es sind keine weiteren Schritte erforderlich.

Kennwort wurde auf einem anderen Endpoint geändert

Hinweis: Kennwörter können auf Windows und Mac Endpoints geändert werden.

Da das Kennwort auf diesem Endpoint nicht mehr bekannt ist, müssen die folgenden Schritte ausgeführt werden:

1. Melden Sie sich mit Ihrem neuen Kennwort bei OS X an.
2. **Das System konnte Ihren Schlüsselbund nicht entsperren** wird angezeigt.
3. Wählen Sie **Schlüsselbundkennwort aktualisieren**.
4. Geben Sie das alte Kennwort ein.

Nähere Informationen darüber, wie Sie Ihr Kennwort zurücksetzen können, falls Sie es vergessen haben, finden Sie unter Mac OS X-Anmeldekennwort vergessen (Seite 23).

5.4 Schneller Benutzerwechsel

SafeGuard File Encryption für Mac unterstützt auch den schnellen Benutzerwechsel. Sie können so zwischen Benutzerkonten auf einem Endpoint wechseln, ohne Anwendung beenden oder sich von dem Rechner abmelden zu müssen.

Hinweis: OS X FUSE erlaubt eine maximale Anzahl von 24 Aktivierungspunkten (Secured Folders) Siehe auch Empfehlungen und Beschränkungen (Seite 8).

5.5 Einstellungsbereich

Im Einstellungsbereich können Sie Einstellungen für eine bestimmte Anwendung oder das System festlegen. Nachdem Sie Sophos SafeGuard File Encryption (oder Sophos SafeGuard native Device Encryption) auf einem Mac-Client installiert haben, erscheint das folgende Symbol in den **Systemeinstellungen**:

Klicken Sie auf das Symbol um den Einstellungsbereich zu öffnen. Der Inhalt der Registerkarte **Über** wird angezeigt.

Die Menüleiste ermöglicht Ihnen die folgenden Menü-Informationsfenster zu öffnen:

5.5.1 Registerkarte Über

Die Registerkarte **Über** enthält Informationen über die auf Ihrem Mac OS X installierte Produktversion sowie das Copyright und eingetragene Marken. Wenn SafeGuard Disk Encryption oder Native Device Encryption installiert ist, wird es ebenfalls aufgelistet.

Klicken Sie auf den Link im unteren Fensterbereich, um die Sophos-Webseite zu öffnen.

5.5.2 Registerkarte Server

Klicken Sie auf **Server**, um ein Fenster mit den folgenden Informationen und Funktionalitäten zu öffnen:

Serverinfo

- **Kontaktintervall:** zeigt das Intervall an, in dem die Synchronisation gestartet wird. Informationen darüber, wie dieses Intervall festgelegt wird, finden Sie unter *SafeGuard Enterprise Administrator-Hilfe > Richtlinieneinstellungen > Allgemeine Einstellungen*.
- **Letzter Serverkontakt:** zeigt Datum und Uhrzeit, an dem der Client zuletzt mit dem Server kommuniziert hat.
- **URL Primärer Server:** URL der Haupt-Serververbindung.
- **URL Sekundärer Server:** URL der sekundären Serververbindung.
- **Server-Verifizierung:** zeigt, ob die SSL-Server-Verifizierung zur Kommunikation mit dem SafeGuard Enterprise-Server aktiviert oder deaktiviert ist. Eine Beschreibung, wie Sie diese Option ändern können, finden Sie unter Kommandozeilen-Optionen (Seite 19).

Konfigurationsdatei hierhin ziehen

Ziehen Sie die Konfigurations-Zip-Datei in diesen Bereich, um die Konfigurationsinformation aus dem SafeGuard Management-Center auf dem Mac-Rechner zu übernehmen. Siehe auch Manuelle (beaufsichtigte) Installation (Seite 6).

Synchronisieren

Klicken Sie diese Schaltfläche, um Datenbankinformationen wie z.B. Richtlinien und/oder Schlüssel manuell zu synchronisieren. Dies kann z.B. erforderlich sein, wenn Änderungen im SafeGuard Management-Center vorgenommen wurden.

Ist die Netzwerkverbindung unterbrochen, so erscheint das folgende Symbol:

Besteht das Problem weiter, überprüfen Sie mithilfe der URL des Haupt- und Zweitservers die Serververbindung. Informationen zu den allgemeinen Voraussetzungen finden Sie unter Installation (Seite 5). Hat das Synchronisieren vorher funktioniert, könnte das Problem in einem abgelaufenen SSL-Zertifikat liegen. Nähere Informationen über mögliche Ursachen finden Sie auch im Systemprotokoll.

Unternehmenszertifikat

- **Gültig ab:** ist das Datum, an dem das Zertifikat gültig wurde.
- **Gültig bis:** ist das Datum, an dem das Zertifikat ungültig wird.
- **Herausgeber:** ist die Instanz, die das Zertifikat herausgegeben hat.
- **Seriennummer:** zeigt die Seriennummer des Unternehmenszertifikats an.

5.5.3 Registerkarte Benutzer

Klicken Sie auf **Benutzer**, um sich Information zu folgenden Punkten anzeigen zu lassen:

- Den **Benutzernamen** des momentan angemeldeten Benutzers.
- Die **Domäne**, die das Domänenverzeichnis auflistet, zu dem der Client gehört. Für lokale Benutzer wird hier der lokale Computername angezeigt.
- Die **SafeGuard Benutzer-GUID**, die die GUID wiedergibt, die für den Benutzer nach dem ersten Anmelden generiert wurde.

Im zweiten Fensterteil können Sie die folgende Option aktivieren oder deaktivieren:

- **System Menü für File Encryption anzeigen**: Wenn aktiviert, wird das Sophos SafeGuard File Encryption Symbol in der Menüleiste angezeigt. Siehe auch Sophos SafeGuard File Encryption System-Menü (Seite 18).

Im dritten Fensterteil wird Information über das **Benutzerzertifikat** angezeigt:

- **Gültig ab:** ist das Datum, an dem das Zertifikat gültig wurde.
- **Gültig bis:** ist das Datum, an dem das Zertifikat ungültig wird.
- **Herausgeber:** ist die Instanz, die das Zertifikat herausgegeben hat.
- **Seriennummer:** zeigt die Seriennummer des Zertifikats an.

5.5.4 Registerkarte Schlüssel

Klicken Sie auf **Schlüssel**, um alle existierenden Schlüsselnamen in einer Listendarstellung anzuzeigen.

Klicken Sie auf das Listensymbol unten rechts in der Ecke neben **Anzahl Schlüssel**, um die GUID-Informationen des oder der betreffenden Schlüssel aus- oder einzublenden.

Sie können Schlüssel anzeigen und sortieren, indem Sie auf eines der Überschriftenelemente **Schlüsselname** oder **Schlüssel-GUID** klicken.

Wenn ein Schlüssel in blau angezeigt wird, handelt es sich um den persönlichen Schlüssel des Benutzers.

5.5.5 Registerkarte Richtlinien

Klicken Sie auf **Richtlinien**, um die Richtlinienansicht zu öffnen. Klicken Sie auf eines der Symbole in der unteren rechten Ecke, um zwischen der Ansicht **Lokal übersetzter Pfad** und **Empfangene Richtlinien** hin- und herzuschalten:

- Der **Lokal übersetzte Pfad** zeigt nur diejenigen Richtlinien an, die dem zu diesem Zeitpunkt angemeldeten Benutzer an einem spezifischen Mac zugewiesen sind. Die Spalten in der Tabelle enthalten folgende Informationen:
  - **@-Symbol**: während der Initialverschlüsselung oder wenn größere Dateien verschlüsselt werden sehen Sie ein sich drehendes Rad in der ersten Spalte mit der Überschrift @, bis die Verschlüsselung abgeschlossen ist.
  - **Modus**: Es wird entweder **verschlüsseln** oder **ausschließen** angezeigt.

    Hinweis:

    In der *SafeGuard Enterprise Administratorhilfe* finden Sie detaillierte Information zu diesen Modi.

- **Anwendungsbereich**: legt fest, ob Unterordner verschlüsselt werden sollen
- **Schlüsselname**: Name des Schlüssels, der dem angegebenen Ablageort zugewiesen ist.

  Wenn ein Schlüssel in blau angezeigt wird, handelt es sich um den persönlichen Schlüssel des Benutzers.

  Ein orangefarbener Schlüssel wurde in einer Richtlinie konfiguriert, die dem Benutzer zugewiesen wurde. Der Benutzer besitzt den Schlüssel jedoch nicht, weil er nicht seinem Schlüsselring zugewiesen wurde. Dies kann zu Problemen beim Datenzugriff führen (siehe auch Probleme beim Zugriff auf Daten (Seite 23)).

Um zur Ansicht 'Empfangene Richtlinien' zu wechseln, klicken Sie in der rechten unteren Ecke auf das rechte Symbol für **Richtlinienansicht**:

- Die Ansicht **Empfangene Richtlinien** zeigt alle Richtlinien an, die vom Server empfangen wurden. Diese Ansicht ist identisch zur Ansicht im SafeGuard Management-Center. Die Übersicht enthält folgende Informationen:
  - **Erhaltene Richtlinien**: legt fest, welche Dateien oder Ordner verschlüsselt werden sollen.
  - Alle anderen Spalten enthalten die oben beschriebenen Informationen für die Ansicht **Lokal übersetzter Pfad**.

Sichere Ordner anzeigen und Richtlinien in der Ansicht "Lokal übersetzter Pfad" anzeigen

Ist eine Richtlinie in der Tabelle **Lokal übersetzter Pfad** ausgewählt, so können Sie

- Klicken Sie auf die Schaltfläche **In Finder anzeigen** (2), um den ausgewählten sicheren Ordner (Aktivierungspunkt bzw. Mount Point) in einem Finder-Fenster zu öffnen und dessen Inhalte anzuzeigen.
- Klicken Sie auf **Richtlinie durchsetzen** (3), um die ausgewählte Richtlinie auf alle Dateien an dem angegebenen Speicherort anzuwenden. Ein Fortschrittsbalken erscheint. Warten Sie, bis das System die Anwendung der Richtlinie abgeschlossen hat, oder brechen Sie den Vorgang ab, indem Sie auf das Kreuz neben dem Balken klicken.

  Hinweis:

  Um eine einzelne Richtlinie aus der Liste zu deselektieren, drücken Sie die Taste **Cmd** und klicken Sie mit der Maus auf die Richtlinie.

  Hinweis:

  Dateien, die schreibgeschützt oder aufgrund fehlender Berechtigungen nicht zugänglich sind, werden von der Verschlüsselung ausgenommen.

Abbildung 1: Registerkarte Richtlinien - Ansicht Lokal übersetzter Pfad

Mögliche Folgen einer Durchsetzung von Richtlinien

Bei einer Richtliniendurchsetzung geschieht Folgendes:

- Klartextdateien werden mit dem Verschlüsselungsschlüssel verschlüsselt, der von einer Richtlinie zugewiesen wurde.
- Dateien, die bereits mit dem in der Richtlinie vorgegebenen Verschlüsselungsschlüssel verschlüsselt sind, bleiben verschlüsselt.
- Dateien, die mit einem anderen Verschlüsselungsschlüssel verschlüsselt sind,
  - bleiben unverändert, wenn der Benutzer nicht den entsprechenden Verschlüsselungsschlüssel an seinem Schlüsselring hat.
  - werden mit dem per Richtlinie zugewiesenen Verschlüsselungsschlüssel neu verschlüsselt, wenn der Benutzer diesen Verschlüsselungsschlüssel an seinem Schlüsselring hat.
- Dateien, die mehrmals verschlüsselt waren, werden einmal mit dem per Richtlinie zugewiesenen Schlüssel verschlüsselt. Wenn einer der erforderlichen Schlüssel nicht verfügbar ist, werden diese Dateien so weit wie möglich entschlüsselt.

5.6 Sophos SafeGuard File Encryption System-Menü

Das System-Menü stellt Ihnen die folgenden Informationen zur Verfügung:

1. Wird eine Datei ausgewählt, zeigt das Symbol automatisch den Verschlüsselungsstatus und den Schlüsselnamen an:

	Grünes Symbol: Die Datei ist verschlüsselt, und Sie besitzen den zugehörigen Schlüssel.
	Rotes Symbol: Die Datei ist verschlüsselt, aber Sie besitzen den zugehörigen Schlüssel nicht.
	Graues Symbol: Die Datei sollte verschlüsselt werden, ist es aber noch nicht. (*)
	Schwarzes Symbol: Die Datei wird ignoriert oder ist von der Verschlüsselung ausgeschlossen.

(*) Mögliches Szenario: Wenn Sie eine unverschlüsselte Datei auswählen, die sich in einem Verzeichnis befindet, auf das eine Verschlüsselungsregel angewendet wird, so wird das Symbol grau. Öffnen Sie das Register **Richtlinien**, wählen Sie die zu diesem Verzeichnis zugehörige Richtlinie und klicken Sie **Erzwinge Richtlinie**, um diese Datei initial zu verschlüsseln. Siehe auch Registerkarte Richtlinien (Seite 16).

2. Wird eine Datei verarbeitet, so dreht sich das äußere Rad des Symbols. Dieses Verhalten ist unabhängig vom aktuellen Verschlüsselungsstatus.
3. Abhängig davon, ob Dateien oder Laufwerke ausgewählt sind, stehen folgende Menübefehle zur Verfügung:

   - Aktueller Verschlüsselungs- und Schlüsselstatus:

     Ist eine Datei, ein Verzeichnis oder ein Laufwerk ausgewählt, so erscheinen ein entsprechender Informationstext zum aktuellen Verschlüsselungsstatus, der Name des erforderlichen Schlüssels und eine Information, ob der Benutzer diesen Schlüssel besitzt.

     Hinweis:

     Um sicherzustellen, dass der aktuelle Verschlüsselungsstatus und Schlüsselname von Dateien oder Verzeichnissen auch angezeigt wird, kann es nötig sein, den Fokus von der ausgewählten Datei oder dem Verzeichnis auf eine beliebige Stelle auf dem Desktop zu legen und danach wieder die ausgewählte Datei/das ausgewählte Verzeichnis zu markieren.

   - List der verfügbaren SafeGuard Secured Folders (Aktivierungspunkte oder mount points)

     Hinweis:

     Wenn Sie mit der Maus über eines der Symbole für sichere Ordner fahren, wird der vollständige Pfad des Ordners angezeigt.

   - **Sophos Encryption-Systemeinstellungen öffnen…**

     Öffnet den Sophos Encryption-Einstellungsbereich. Siehe auch Einstellungsbereich (Seite 14).

5.7 Kommandozeilen-Optionen

Terminal erlaubt Ihnen, Kommandos und Kommandozeilen-Optionen einzugeben. Folgende Kommandozeilen-Optionen stehen zur Verfügung:

Kommando-Name	Definition	Zusätzliche Parameter (optional)
sgfsadmin	Listet die verfügbaren Kommandos zusammen mit einer Kurzhilfe auf.	**--help**
sgfsadmin --version	Zeigt Version und Copyright des installierten Produkts an.	
sgfsadmin --status	Zeigt Systemstatusinformationen wie Versions-, Server- und Zertifikatsinformation an.	
sgfsadmin --list-user-details	Zeigt Informationen zum momentan angemeldeten Benutzer an.	**--all** zeigt Information für alle Benutzer an (sudo erforderlich). **--xml** zeigt Ausgabe im xml-Format an.
sgfsadmin --list-keys	Listet existierende GUIDS und Schlüsselnamen aller Schlüssel im Schlüsselbund auf	**--all** zeigt Information für alle Benutzer an (sudo erforderlich). **--xml** zeigt Ausgabe im xml-Format an.
sgfsadmin --list-policies	Zeigt Richtlinien-spezifische Informationen an. Schlüssel-GUIDS werden wenn möglich in Schlüsselnamen aufgelöst. Fett ausgezeichnete Elemente zeigen einen persönlichen Schlüssel an.	**--all** zeigt Information für alle Benutzer an (sudo erforderlich). **--xml** zeigt Ausgabe im xml-Format an. **--raw** zeigt Richtlinien in Originalansicht an, d.h. so wie sie auf SafeGuard Management Center-Serverseite aufgesetzt sind.
sgfsadmin --enforce-policies	Wendet die Verschlüsselungs-Richtlinie an	**--all** wendet die Richtlinie auf alle Verzeichnisse an, wo Richtlinien gelten **"directoryname"** wendet die Richtlinie auf das angegebene Verzeichnis an.
sgfsadmin --file-status "filename1" ["filename2"..."filenameN"]	Zeigt Verschlüsselungsinformation für eine Datei oder Dateilisten an. Die Verwendung von Platzhaltern ist erlaubt.	**--xml** zeigt Ausgabe im xml-Format an.

Kommando-Name	Definition	Zusätzliche Parameter (optional)
sgfsadmin --import-config "/Pfad/zur/Datei"	Importiert die angegebene Konfigurations-Zipdatei Siehe auch Manuelle (beaufsichtigte) Installation (Seite 6). Das Kommando braucht Administrator-Rechte (sudo). **Hinweis:** Ziehen Sie komplette Pfade mit der Maus z.B. aus dem Finder in die Terminal-Anwendung.	
sgfsadmin --enable-server-verify	Schaltet die SSL-Serververifizierung für die Kommunikation mit dem SafeGuard Enterprise-Server ein. Nach der Installation ist die SSL-Serververifizierung standardmäßig aktiviert. Das Kommando braucht Administrator-Rechte (sudo).	
sgfsadmin --disable-server-verify	Schaltet die SSL-Serververifizierung für die Kommunikation mit dem SafeGuard Enterprise-Server aus. Das Kommando braucht Administrator-Rechte (sudo). **Hinweis:** Wir empfehlen nicht, diese Option zu verwenden, da dadurch eine Sicherheits-Schwachstelle entstehen kann.	
sgdeadmin --update-machine-info [--domain "domain"]	Aktualisiert die aktuell gespeicherten Computerinformationen, die verwendet werden, um diesen Client auf dem SafeGuard Enterprise Server zu registrieren. Das Kommando braucht Administrator-Rechte (sudo). **Hinweis:** Verwenden Sie diesen Befehl erst nach dem Ändern der Domain oder Arbeitsgruppe, zu welcher der Computer gehört. Gehört der Computer zu mehreren Domains oder Arbeitsgruppen und führen Sie diesen Befehl aus, kann dies zu einer Änderung der Domain-Registrierung und	**--domain "domain"** Die Domain, die der Client für die Registrierung auf dem SafeGuard Enterprise Server verwenden sollte. Dieser Parameter ist nur erforderlich, wenn der Rechner zu mehreren Domains gehört. Der Computer muss dieser Domain hinzugefügt werden, ansonsten schlägt der Befehl fehl.

Kommando-Name	Definition	Zusätzliche Parameter (optional)
	Entfernung von persönlichen Schlüsseln und/oder FileVault 2 Benutzern führen.	

Die folgenden Befehle sind ausführlich in Abschnitt Lokal verwaltete Konfigurationsoptionen (Seite 11) beschrieben:

- **`sgfsadmin --enable-systemmenu`**
- **`sgfsadmin --disable-systemmenu`**
- **`sgfsadmin --synchronize`**

5.8 Arbeiten mit Wechselmedien

Hinweis:

Stellen Sie vor dem Arbeiten mit Wechselmedien sicher, dass Ihnen eine Richtlinie und ein Schlüssel zugewiesen wurden, die es Ihnen erlauben, Dateien auf Wechselmedien zu verschlüsseln.

1. Schließen Sie das Wechselmedium an.
2. Es öffnet sich ein Dialog, in dem Sie gefragt werden, ob Sie Klartextdateien auf dem Gerät verschlüsseln möchten. Nach dem Klicken auf **Ja** startet die Verschlüsselung. Wenn Sie auf **NEIN** klicken, bleiben diese Dateien unverschlüsselt, aber Sie haben Zugriff auf Dateien auf dem Gerät, die bereits verschlüsselt sind. Unabhängig von Ihrer Auswahl werden neue Dateien auf dem Gerät immer gemäß der Richtlinie verschlüsselt.
3. Die Dateien auf Ihrem Wechselmedium werden automatisch verschlüsselt. Dies wird durch das System-Menü-Symbol des sich drehenden Rads angezeigt
4. Sind alle Dateien auf Ihrem Medium verschlüsselt, so hört das Rad auf, sich zu drehen.
5. Werfen Sie das Wechselmedium aus. Das zugehörige Symbol für den sicheren Ordner wird automatisch ausgeblendet.

   Hinweis:

   Um Daten auf Wechselmedien zwischen zwei Stellen austauschen und bearbeiten zu können, müssen beiden Stellen die zugehörige Richtlinie und der entsprechende Schlüssel zugewiesen werden. Für den Austausch zwischen Windows- und Mac OS X-Clients muss das Gerät mit FAT32 formatiert sein und es können keine persönlichen Schlüssel verwendet werden. Für den Windows-Client ist eine Datenaustausch-Richtlinie erforderlich. Die Medien-Passphrase-Funktionalität steht nur für Windows zur Verfügung. Der Zugriff auf die Daten von einem Mac OS X-Client aus ist nur möglich, wenn entsprechende Richtlinien vom Typ **Dateiverschlüsselung** definiert werden.

6 Fehlerbehebung

6.1 Mac OS X-Anmeldekennwort vergessen

Hat ein Benutzer sein Mac OS X Anmeldekennwort vergessen, so gehen Sie wie folgt vor:

1. Der Benutzer wird Sie bitten, ein neues Benutzerkennwort zu erstellen.
2. Setzen Sie dazu das alte Kennwort in der Benutzerverwaltung zurück und generieren Sie ein neues Kennwort. Wählen Sie die entsprechende Option um den Benutzer zu zwingen, sein Kennwort nach der ersten Anmeldung zu ändern.
3. Wechseln Sie in die SafeGuard Management Center-Anwendung und löschen Sie das Zertifikat für den Benutzer.
4. Kontaktieren Sie den Benutzer und übergeben Sie das neue Kennwort.
5. Fordern Sie den Benutzer auf, sich mit dem neuen Kennwort anzumelden.
6. Nach dem Anmelden erscheint der Dialog **Kennwort zurücksetzen**.
7. Bitten Sie den Benutzer, ein neues Kennwort festzulegen und dieses neue Kennwort einzugeben und zu bestätigen und eine Sicherheitsabfrage für das Kennwort festzulegen. Abschließend muss der Benutzer auf **Kennwort zurücksetzen** klicken, um die Änderungen zu bestätigen.
8. Nach dem Zurücksetzen des Kennworts erscheint auf Benutzerseite die folgende Meldung:

   Das System konnte Ihren Anmeldeschlüsselbund nicht freigeben
9. Fordern Sie den Benutzer auf, die Option **Neuen Schlüsselbund erstellen** auszuwählen.
10. Es wird ein neuer Schlüsselbund für diesen Benutzer erstellt.
11. Nun wird der Benutzer aufgefordert, sein neues OS X-Kennwort aus Schritt 7 einzugeben, um ein SafeGuard-Benutzerzertifikat zu erstellen.

Die Schlüssel des Benutzers werden automatisch in den neuen Schlüsselbund geladen, so dass alle Dokumente wie bisher zugänglich sind.

6.2 Probleme beim Zugriff auf Daten

Hat ein Benutzer Probleme mit dem Zugriff auf Daten, kann dies daran liegen, dass er nicht den entsprechenden Schlüssel an seinem Schlüsselring an:

- Überprüfen Sie die Einstellungen in der Management Center-Umgebung und korrigieren Sie sie gegebenenfalls. Unter Sophos SafeGuard File Encryption System-Menü (Seite 18) finden Sie Informationen darüber, wie Sie überprüfen können, ob der aktuell angemeldete Benutzer bereits den entsprechenden Schlüssel hat.

  Dateien, die mit einem Schlüssel verschlüsselt wurden, der sich nicht im Schlüsselbund des Benutzers befindet, können nicht entschlüsselt werden. Sollte der Benutzer versuchen, Dateien in einen sicheren Ordner zu kopieren (wodurch die Initialverschlüsselung dieser Dateien ausgelöst wird) und der entsprechende Schlüssel nicht verfügbar sein, zeigt Mac OS X einen Dialog an, in dem der Benutzer nach einem Administratornamen und -kennwort gefragt wird. In diesem Fall sollte der Benutzer auf **Abbrechen** klicken (selbst mit Kennwort könnte er nicht auf die verschlüsselten Dateien zugreifen).

6.3 Ordner "SafeGuard Recovered Files"

Unter bestimmten Umständen kann es sein, dass sich ein Ordner namens **Sophos SafeGuard Recovered Files** in einem Ordner befindet. Dies ist dann der Fall, wenn SafeGuard File Encryption versucht, einen neuen sicheren Ordner (Aktivierungspunkt bzw. Mount Point) zu erstellen, aber der versteckte Ordner, der zum Speichern der verschlüsselten Inhalte erstellt werden muss (z. B. /Users/admin/.sophos_safeguard_Documents/) bereits existiert und nicht leer ist. Dann wird der Inhalt des ursprünglichen Ordners (z. B. /Users/admin/Documents) zu **Sophos SafeGuard Recovered Files** verschoben und es wird wie sonst auch nur der Inhalt des versteckten Ordners angezeigt.

7 Deinstallation auf dem Client-Rechner

Wenn Sie die Software von einem Client deinstallieren müssen, gehen Sie wie folgt vor:

1. Wechseln Sie auf dem Mac Client zu */Library*.
2. Öffnen Sie den Ordner *Sophos SafeGuard FS*.
3. Wählen und doppelklicken Sie die Datei *Sophos SafeGuard FS Uninstaller.pkg.*
4. Ein Assistent führt Sie durch die Deinstallation.
5. Starten Sie das System neu, bevor Sie mit Ihrer Arbeit am Mac fortfahren.

   Hinweis: Das Uninstaller Package ist signiert und OS X versucht, diese Signatur zu validieren. Ist die Internetverbindung langsam oder nicht richtig konfiguriert, kann es eventuell zu Verzögerungen beim Deinstallationsvorgang von bis zu 20 Minuten kommen.

8 Technischer Support

Technischen Support zu Sophos Produkten können Sie wie folgt abrufen:

- Rufen Sie die SophosTalk-Community unter community.sophos.com/ auf und suchen Sie nach Benutzern mit dem gleichen Problem.
- Durchsuchen Sie die Sophos Support-Knowledgebase unter www.sophos.com/de-de/support.aspx.
- Laden Sie die Produktdokumentation unter www.sophos.com/de-de/support/documentation/ herunter.
- Öffnen Sie ein Ticket bei unserem Support-Team unter https://secure2.sophos.com/support/contact-support/support-query.aspx.

9 Rechtliche Hinweise