

SOPHOS

Security made simple.

Sophos SafeGuard File Encryption for Mac Schnellstart-Anleitung

Produktversion: 7
Stand: Dezember 2014



Inhalt

1	Sophos SafeGuard File Encryption for Mac.....	3
2	Erstanmeldung.....	4
3	Arbeiten mit SafeGuard File Encryption for Mac.....	5
3.1	Initialverschlüsselung durchführen.....	5
4	Sophos SafeGuard File Encryption System-Menü.....	6
5	Einstellungsbereich.....	8
5.1	Registerkarte Über.....	8
5.2	Registerkarte Server.....	8
5.3	Registerkarte Benutzer.....	9
5.4	Registerkarte Schlüssel.....	9
5.5	Registerkarte Richtlinien.....	10
6	Arbeiten mit Wechselmedien.....	12
7	Allgemeine Hinweise.....	13
8	Technischer Support.....	14
9	Rechtliche Hinweise.....	15

1 Sophos SafeGuard File Encryption for Mac

Sophos SafeGuard File Encryption for Mac erweitert den Sophos SafeGuard Enterprise Datenschutz von Windows auf Mac und ermöglicht 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 austauschen.

- Neue Dateien in den relevanten Speicherorten werden automatisch verschlüsselt.
- Wenn Sie den Schlüssel für eine verschlüsselte Datei haben, können Sie den Inhalt lesen und ändern.
- Wenn Sie keinen Schlüssel für eine verschlüsselte Datei haben, können Sie die Datei nicht im Klartext lesen, sondern sehen nur den verschlüsselten Inhalt.
- Wenn Sie auf einem beliebigen Endpoint, auf dem File Encryption nicht installiert ist, auf eine verschlüsselte Datei zugreifen, wird ebenfalls der verschlüsselte Inhalt angezeigt.

2 Erstanmeldung

In diesem Handbuch wird davon ausgegangen, dass die Software bereits, wie in der *Sophos SafeGuard File Encryption for Mac Administratorhilfe* beschrieben, installiert und die Kommunikation mit dem SafeGuard Enterprise Backend erfolgreich hergestellt wurde.

1. Schalten Sie den Mac ein.
2. Melden Sie sich wie gewohnt an Ihrem Mac mit Ihrem OS X-Kennwort an.
3. Wenn Sie sich nach der Installation das erste Mal anmelden, werden Sie aufgefordert, Ihr Kennwort erneut in den folgenden Dialog einzugeben:



Abbildung 1: Dieser Anmeldedialog erscheint nur nach Installation und erster Anmeldung pro Benutzer.

4. Geben Sie das Kennwort ein und bestätigen Sie mit OK.
Wichtig: Um das Produkt ordnungsgemäß zu verwenden, benötigen Sie ein persönliches Zertifikat. Dieses Zertifikat wird pro Benutzer generiert, wenn Sie das Kennwort im Dialogfeld eingeben. Dieser Vorgang ist nur nach Produktinstallation, erster Anmeldung oder dem Kennwort-Zurücksetzen erforderlich.
5. Je nachdem, welche Sicherheitseinstellungen Ihnen zugewiesen worden sind, werden nun ein oder mehrere Laufwerke auf Ihrem Schreibtisch angezeigt.
Wichtig: Stellen Sie sicher, dass die Einstellungen "Verbundene Server" in den Finder-Einstellungen aktiviert ist. Wählen Sie dazu **Finder - Einstellungen...- Register "Allgemein"** und aktivieren Sie die Option **Verbundene Server**.

3 Arbeiten mit SafeGuard File Encryption for Mac

SafeGuard File Encryption for Mac ermöglicht Ihrem Sicherheitsadministrator festzulegen, ob Dateien in bestimmten Verzeichnissen und/oder Laufwerken verschlüsselt werden oder ob nicht. Ist das Verzeichnis oder das Laufwerk verschlüsselt, wird es als Netzwerk-Laufwerk angezeigt. Die Spotlight-Suche und permanente Versionsspeicherung ("Alle Versionen durchsuchen...") sind daher nicht verfügbar. Wenn Sie jedoch versuchen, ein solches Laufwerk auszuwerfen, wird es automatisch wieder verbunden.

Die Verschlüsselung selbst ist transparent. Nach der Initialverschlüsselung stellt das System sicher, dass die Dateien, die sich auf einem Laufwerk oder in einem Verzeichnis befinden, das für die Verschlüsselung festgelegt wurde (der "sichere Ordner"), verschlüsselt werden.

3.1 Initialverschlüsselung durchführen

Starten Sie eine Initialverschlüsselung, bevor Sie mit Ihrer Arbeit beginnen.

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



3. Wählen Sie das Register **Richtlinien**.
4. Wechseln Sie zur Ansicht **Lokal übersetzter Pfad** und klicken Sie auf **Erzwingen alle Richtlinien**, um alle Richtlinien anzuwenden.

Alle unverschlüsselten Dateien werden nun verschlüsselt.

Wenn Sie eine einzelne Richtlinie erzwingen wollen, so wählen Sie diese mit der Maus aus und klicken Sie auf **Erzwingen Richtlinie**. Um eine einzelne Richtlinie aus der Liste zu deselektieren, drücken Sie die Taste **Cmd** und klicken Sie mit der Maus auf die Richtlinie.





4 Sophos SafeGuard File Encryption System-Menü

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

1. Wenn ein sicherer Ordner oder eine Datei innerhalb des Ordners ausgewählt ist, zeigt Ihnen das Symbol in der Menüleiste automatisch den Verschlüsselungs- und Schlüsselstatus an:



Abbildung 2: Systemmenü, Fokus auf verschlüsselter Datei oder sicherem Ordner

	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. (*)
	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.

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 Verschlüsselungszustand von Dateien oder Verzeichnissen auch angezeigt wird, kann es nötig sein, den Fokus von der ausgewählten Datei oder dem Verzeichnis irgendwo auf den 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 Ordnersymbole fahren, wird der vollständige Pfad angezeigt.

- **Sophos Encryption-Systemeinstellungen öffnen...**

Öffnet den Sophos Encryption-Einstellungsbereich.

5 Einstellungsbereich

Der Einstellungsbereich ermöglicht Ihnen, Einstellungen für spezifische Anwendungen oder für das System vorzunehmen. Nachdem Sie Sophos Encryption auf einem Mac-Client installiert haben, erscheint das folgende Symbol in den **Systemeinstellungen**:



Darüber hinaus sehen Sie das Symbol für FUSE for OS X (OSXFUSE) 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-Informationenfenster zu öffnen:

5.1 Registerkarte Über

In der Registerkarte **Über** erhalten Sie Informationen zur installierten Produktversion auf Ihrem Mac und zu Copyrights und eingetragenen Warenzeichen. Wenn Sophos SafeGuard Disk Encryption oder Native Device Encryption installiert ist, sind diese ebenfalls aufgeführt.

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

Klicken Sie auf das Fragezeichen-Symbol in der unteren rechten Ecke, um die SafeGuard File Encryption-Schnellanleitung in Ihrer eingestellten Systemsprache zu öffnen.

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. Es wird zentral vom Sicherheitsbeauftragten festgelegt.
- **Zuletzt kontaktiert:** zeigt das Datum an, an dem ein Client zuletzt mit dem Server kommuniziert hat.
- **URL Primärer Server:** URL der Hauptserververbindung.
- **URL Sekundärer Server:** URL der Zweitserververbindung.
- **Server-Verifizierung:** zeigt, ob die SSL-Server-Verifizierung zur Kommunikation mit dem SafeGuard Enterprise-Server aktiviert oder deaktiviert ist.

Konfigurationsdatei hierhin ziehen

Ziehen Sie die Konfigurations-Zip-Datei in diesen Bereich, um die Konfigurationsinformation aus dem Management-Center auf dem Mac-Rechner zu übernehmen.

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:



Sollte dieses Problem weiter bestehen, wenden Sie sich an Ihren Sicherheitsadministrator.

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.

5.3 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 Computernamen angezeigt.

Hinweis:

Der Eintrag **Domäne** muss identisch sein mit dem Eintrag in **System Preferences - Users & Groups - Login Options - Network Account Server**.

- 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 6).

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.

5.4 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 eins der Überschriftenelemente **Schlüsselname** oder **Schlüssel-GUID** klicken.

Wenn ein Schlüssel in blau angezeigt wird, handelt es sich um Ihren persönlichen Schlüssel. Wird ein Schlüssel in orange angezeigt, gehört er nicht Ihnen.

5.5 Registerkarte Richtlinien

Klicken Sie auf **Richtlinien**, um die Richtlinienansicht zu öffnen. Klicken Sie auf eins 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:** mögliche Modi sind **verschlüsseln** oder **ausschließen**.

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.

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 für den Lokal übersetzten Pfad bereits beschriebenen Informationen.

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 in einem Finder-Fenster zu öffnen und dessen Inhalte anzuzeigen.
- auf **Erzwingen Richtlinie** (3) klicken, um die ausgewählte Richtlinie auf alle erlaubten Dateien 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:

Schreib- oder eigentümergegeschützte Dateien werden von der Verschlüsselung ausgenommen.

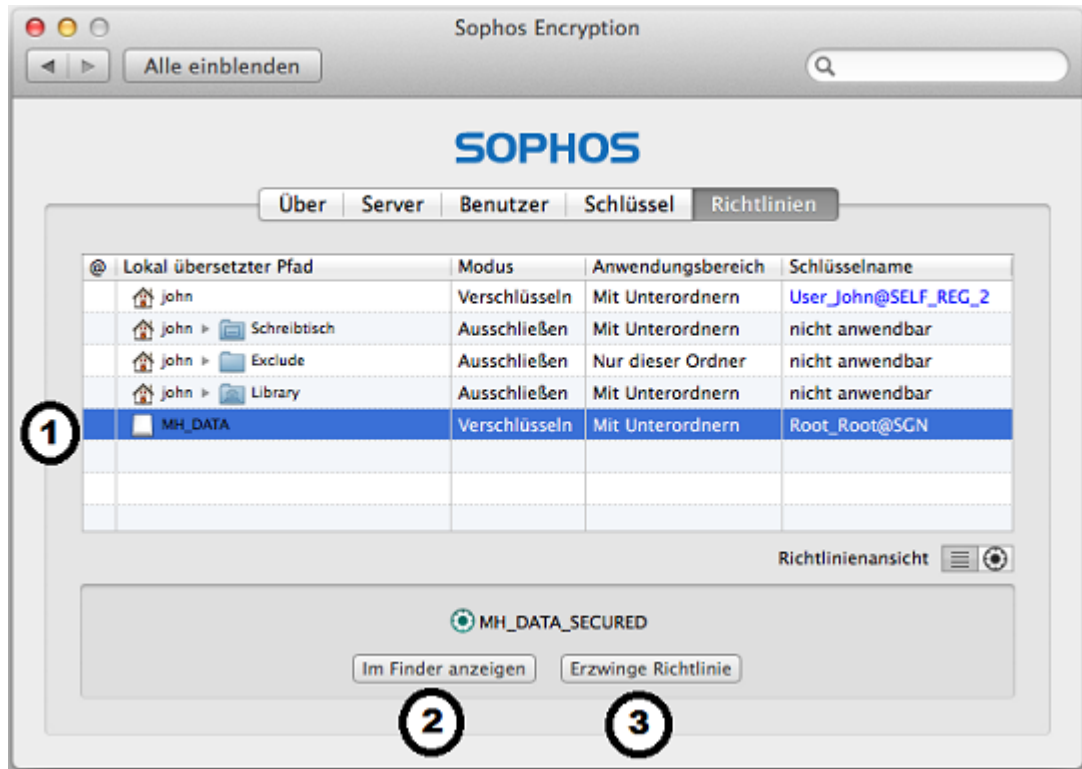


Abbildung 3: Registerkarte Richtlinien - Ansicht Lokal übersetzter Pfad

Mögliche Ergebnisse aus erzwungenen Richtlinien

Wenn Sie Richtlinien erzwungen haben:

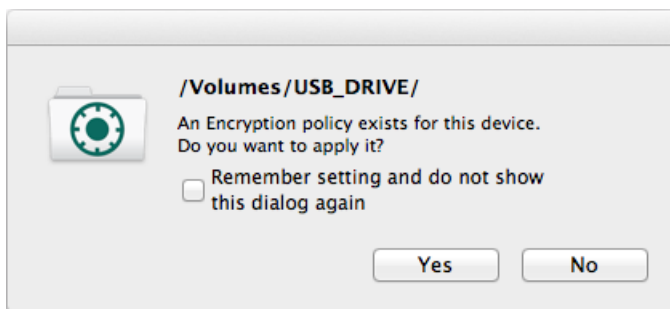
- Klartextdateien werden mit dem Schlüssel verschlüsselt, der von einer Richtlinie zugewiesen wurde.
- Bereits verschlüsselte Dateien bleiben verschlüsselt, wenn der Benutzer den entsprechenden Schlüssel an seinem Schlüsselring hat.
- Dateien, die mit einem anderen Schlüssel verschlüsselt sind,
 - bleiben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

6 Arbeiten mit Wechselmedien

Wichtig: Stellen Sie sicher, dass Ihnen eine Richtlinie und ein Schlüssel zugewiesen wurden, die Ihnen erlauben, Dateien auf Wechselmedien zu bearbeiten und zu verschlüsseln.

Um Dateien auf Wechselmedien zu verschlüsseln, gehen Sie wie folgt vor:

1. Stecken Sie das Wechselmedium in den Mac.
2. Ein Dialog erscheint in dem Sie bestätigen, dass Sie die Dateien verschlüsseln wollen.



3. Klicken Sie **Ja**, um dies zu bestätigen. Um diese Einstellung zu speichern, aktivieren Sie die zugehörige Option.
4. Die Dateien auf Ihrem Wechselmedium werden verschlüsselt. Das äußere Rad des Symbols dreht sich.
5. Sind alle Dateien auf Ihrem Medium verschlüsselt, so hört das Rad auf, sich zu drehen.
6. Werfen Sie das Wechselmedium aus. Das zugehörige Laufwerk-Symbol wird automatisch ausgeblendet.

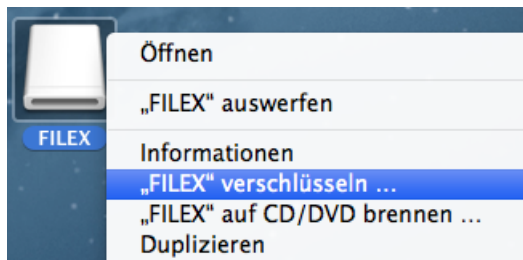
Um Daten auf Wechselmedien zwischen zwei Stellen austauschen und bearbeiten zu können, müssen beiden Stellen die zugehörige Richtlinie und der entsprechende Schlüssel zugewiesen werden.

Wichtig: Wenn Sie größere Datenmengen auf Wechsellaufwerken austauschen stellen Sie sicher, dass Sie über mehr als doppelt so viel freien Plattenplatz zur Verfügung haben, wie die größte auszutauschende Datei benötigt.

7 Allgemeine Hinweise

Wenn Sie auf die Mac OS X FileVault 2-Festplattenverschlüsselung treffen...

Wenn Sie ein Laufwerk (auf Ihrem Schreibtisch oder im Finder) wählen und rechts mit der Maus klicken, so kann ein Menübefehl "<Laufwerksname> verschlüsseln" erscheinen:



Dies ist die interne Apple OS X Festplattenverschlüsselung FileVault 2, die nicht mit unserer SafeGuard-Dateiverschlüsselung zusammenhängt.

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

Copyright © 2014 Sophos Limited. Alle Rechte vorbehalten. SafeGuard ist ein eingetragenes Warenzeichen von Sophos Limited und Sophos Group.

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

Sophos, Sophos Anti-Virus und SafeGuard sind eingetragene Warenzeichen der Sophos Limited, Sophos Group und Utimaco Safeware AG. Alle anderen erwähnten Produkt- und Unternehmensnamen sind Warenzeichen oder eingetragene Warenzeichen der jeweiligen Inhaber.

Copyright-Informationen von Drittanbietern finden Sie im Dokument *Disclaimer and Copyright for 3rd Party Software* in Ihrem Produktverzeichnis.