SOPHOS

simple + secure

Sophos Anti-Virus für Mac OS X

Hilfe

Für Einzelplatzrechner oder Netzwerkcomputer unter Mac OS X, Version 10.4 oder höher

Produktversion: 8
Stand: April 2012

Inhalt

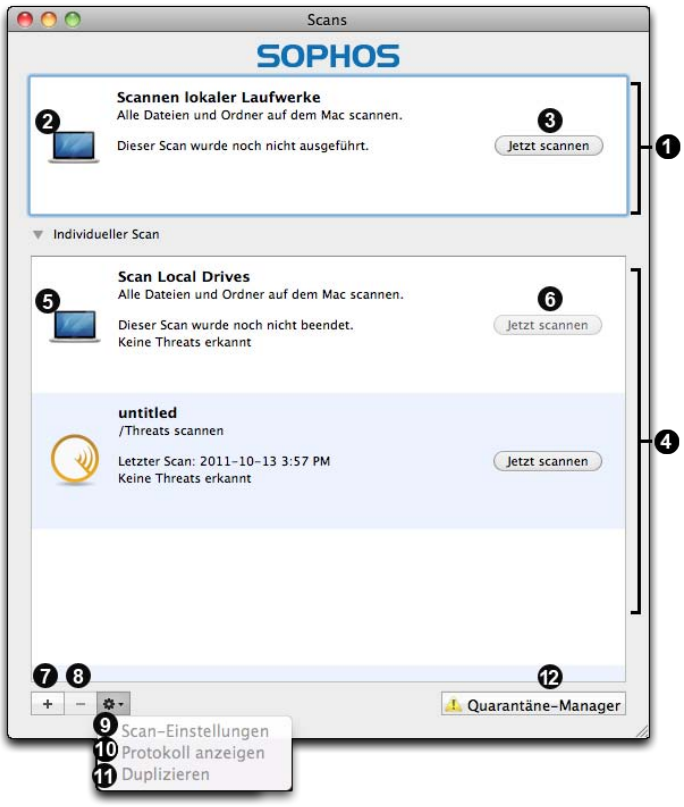
1 Über Sophos Anti-Virus

Sophos Anti-Virus für Mac OS X, Version 8, erkennt und bereinigt Threats (Viren, Würmer und Trojaner) auf Computern und im Netzwerk. Es werden nicht nur Mac OS X-Threats, sondern auch Windows-Threats erkannt, die sich unter Umständen auf dem Mac oder im Netzwerk befinden und auf Windows-Computer übertragen wurden.

Sophos Anti-Virus wird mit den empfohlenen Schutzeinstellungen konfiguriert. Es empfiehlt sich, dass Sie die Einstellungen nur zur Problembehebung oder aus bestimmten Gründen ändern.

1.1 Das Fenster „Scans“

Die Bestandteile des Fensters **Scans** werden unten angezeigt:



1	Der standardmäßig von Sophos bereitgestellte Scan lokaler Laufwerke. Nähere Informationen finden Sie unter *Scannen lokaler Laufwerke* (Seite 15).
2	Doppelklicken Sie darauf, um die Einstellungen aufzurufen. Nähere Informationen finden Sie unter *Konfigurieren von Scans lokaler Laufwerke* (Seite 16).
3	Klicken Sie darauf, um lokale Laufwerke zu scannen. Nähere Informationen finden Sie unter *Scannen lokaler Laufwerke* (Seite 16).

❹	Die Liste der von Ihnen hinzugefügten Scans. Nähere Informationen finden Sie unter *Individuelle Scans* (Seite 19). Wenn Sie das Fenster zum ersten Mal öffnen, klicken Sie zum Einblenden der Liste auf das Dreieck neben **Individuelle Scans**.
❺	Doppelklicken Sie darauf, um den individuellen Scan zu konfigurieren. Nähere Informationen finden Sie unter *Konfigurieren eines individuellen Scans* (Seite 21).
❻	Klicken Sie darauf, um den individuellen Scan auszuführen.
❼	Klicken Sie darauf, um einen individuellen Scan hinzuzufügen. Nähere Informationen finden Sie unter *Hinzufügen von individuellen Scans* (Seite 19).
❽	Klicken Sie darauf, um einen individuellen Scan zu löschen.
❾	Wählen Sie **Scan-Einstellungen**, um den ausgewählten individuellen Scan zu konfigurieren. Nähere Informationen finden Sie unter *Konfigurieren eines individuellen Scans* (Seite 21).
❿	Wählen Sie **Scanprotokoll anzeigen**, um das Protokoll des ausgewählten individuellen Scans aufzurufen.
⓫	Sie können **Duplizieren** auswählen und den benutzerdefinierten Scan als Grundlage für einen neuen Scan verwenden. Nähere Informationen finden Sie unter *Kopieren von individuellen Scans* (Seite 21).
⓬	Klicken Sie zum Öffnen des **Quarantäne-Managers** auf die Option **Quarantäne-Manager**. Nähere Informationen finden Sie unter *Über den Quarantäne-Manager* (Seite 33).

2 Scannen auf Threats

Die **On-Access-Scanfunktion** ist der Hauptmechanismus zum Schutz vor Viren und sonstigen Threats. Beim Versuch, auf eine Datei (d.h. Kopieren, Speichern, Verschieben oder Öffnen der Datei) zuzugreifen, scannt Sophos Anti-Virus die Datei. Der Zugriff wird nur erlaubt, wenn die Datei threatfrei ist. Standardmäßig sind On-Access-Scans aktiviert, und die empfohlenen Schutzeinstellungen sind vorkonfiguriert. Es empfiehlt sich, dass Sie die Einstellungen nur zur Problembehebung oder aus bestimmten Gründen ändern.

On-Demand-Scans bieten zusätzlichen Schutz. On-Demand-Scans werden vom Benutzer eingeleitet. Sie können alle Objekte scannen, auf die Sie zugreifen können – der Scanumfang reicht von einzelnen Dateien bis hin zum gesamten Mac:

Scan-Typ	Scan-Umfang	Einsatz
Lokale Laufwerke	Alle Dateien, auf die Sie auf lokalen Volumes zugreifen können. Wenn Sie sich als Administrator authentifizieren, werden auch Dateien gescannt, auf die Sie nicht zugreifen	■ Sie möchten einen von Sophos Anti-Virus erkannten Threat verarbeiten. ■ Es werden keine On-Access-Scans auf dem

Scan-Typ	Scan-Umfang	Einsatz
	können. Hierzu zählen auch angeschlossene Wechselmedien.	Mac ausgeführt, weil es sich um einen Server handelt. ■ Sie möchten infizierte Dateien *vor dem Verwenden* auffinden.
Individuell	Scan ausgewählter Dateien, Ordner oder Volumes.	■ Sie möchten nur verdächtige Festplattenabschnitte scannen. ■ Sie möchten infizierte Dateien *vor dem Verwenden* auffinden.
Finder-Objekt	Im Finder ausgewählte Dateien, Ordner oder Volumes.	■ Sie möchten die Inhalte von Archiven oder komprimierten Dateien *vor* dem Öffnen scannen. ■ Sie möchten etwas vor dem Versand per E-Mail scannen. ■ Sie möchten eine CD oder DVD scannen.

2.1 Informationen zum Scannen auf Threats

Die **On-Access-Scanfunktion** ist der Hauptmechanismus zum Schutz vor Viren und sonstigen Threats. Beim Versuch, auf eine Datei (d.h. Kopieren, Speichern, Verschieben oder Öffnen der Datei) zuzugreifen, scannt Sophos Anti-Virus die Datei. Der Zugriff wird nur erlaubt, wenn die Datei threatfrei ist. Standardmäßig sind On-Access-Scans aktiviert, und die empfohlenen Schutzeinstellungen sind vorkonfiguriert. Es empfiehlt sich, dass Sie die Einstellungen nur zur Problembehebung oder aus bestimmten Gründen ändern.

On-Demand-Scans bieten zusätzlichen Schutz. On-Demand-Scans werden vom Benutzer eingeleitet. Sie können alle Objekte scannen, auf die Sie zugreifen können – der Scanumfang reicht von einzelnen Dateien bis hin zum gesamten Mac:

- **Scannen lokaler Laufwerke**

  Alle Dateien, auf die Sie auf lokalen Volumes zugreifen können, werden gescannt. Wenn Sie sich als Administrator authentifizieren, werden auch Dateien gescannt, auf die Sie nicht zugreifen können. Hierzu zählen auch angeschlossene Wechselmedien.

  Scans lokaler Laufwerke bieten sich in folgenden Fällen an: Sie möchten einen von Sophos Anti-Virus erkannten Threat verarbeiten, es werden keine On-Access-Scans auf dem Mac

ausgeführt, weil es sich um einen Server handelt, oder Sie möchten infizierte Dateien *vor* dem Verwenden auffinden.

- **Individuelle Scans**

  Scan ausgewählter Dateien, Ordner oder Volumes.

  Individuelle Scans bieten sich an, wenn Sie nur verdächtige Festplattenabschnitte scannen oder infizierte Dateien *vor* dem Verwenden auffinden möchten.

- **Objekt-Scans im Finder**

  Scannen von im Finder ausgewählten Dateien, Ordnern oder Volumes.

  Objekt-Scans im Finder bieten sich in folgenden Fällen an: Sie möchten die Inhalte von Archiven oder komprimierten Dateien *vor* dem Öffnen scannen, etwas vor dem Versand per E-Mail scannen oder eine CD oder DVD scannen.

Sie können sich auch mittels **E-Mail-Benachrichtigungen** bei allen Scan-Arten über Threats oder schwerwiegende Fehler benachrichtigen lassen.

Sie können auch Scans mit **Terminal** über die Befehlszeile ausführen.

2.2 On-Access-Scans

Die **On-Access-Scanfunktion** ist der Hauptmechanismus zum Schutz vor Viren und sonstigen Threats. Beim Versuch, auf eine Datei (d.h. Kopieren, Speichern, Verschieben oder Öffnen der Datei) zuzugreifen, scannt Sophos Anti-Virus die Datei. Der Zugriff wird nur erlaubt, wenn die Datei threatfrei ist. Standardmäßig sind On-Access-Scans aktiviert, und die empfohlenen Schutzeinstellungen sind vorkonfiguriert. Es empfiehlt sich, dass Sie die Einstellungen nur zur Problembehebung oder aus bestimmten Gründen ändern.

2.2.1 Aktivieren/Deaktivieren der On-Access-Scans

Wichtig: Wenn Sie in Ihrem Unternehmen Standardeinstellungen festgelegt haben, haben diese möglicherweise Vorrang vor hier vorgenommenen Änderungen.

On-Access-Scans werden standardmäßig beim Hochfahren des Computers aktiviert.

So aktivieren/deaktivieren Sie On-Access-Scans:

1. Wählen Sie **Sophos Anti-Virus** > **Einstellungen** .
2. Klicken Sie auf **On-Access-Scans**.
3. Wenn bestimmte Einstellungen nicht hervorgehoben sind, klicken Sie auf das Schlosssymbol und geben Sie einen Administratorennamen und ein Kennwort ein.
4. Ändern Sie die Einstellungen wie folgt:

   - Klicken Sie zum *Aktivieren* von On-Access-Scans auf **Scan-Vorgang starten**. Der Status ändert sich zu **Ein** und das Sophos Anti-Virus Symbol in der Menüleiste wird schwarz.

- Klicken Sie zum *Deaktivieren* von On-Access-Scans auf **Scan-Vorgang anhalten**. Der Status ändert sich zu **Aus** und das Sophos Anti-Virus Symbol in der Menüleiste wird schwarz.

Wichtig: Wenn Sie On-Access-Scans deaktivieren, sucht Sophos Anti-Virus in aufgerufenen Dateien nicht nach Threats. Ihr Macintosh-Computer ist somit nicht hinreichend geschützt.

2.2.2 Konfigurieren von On-Access-Scans

2.2.2.1 Hinzufügen von On-Access-Scan-Ausschlüssen

Wichtig: Wenn Sie in Ihrem Unternehmen Standardeinstellungen festgelegt haben, haben diese möglicherweise Vorrang vor hier vorgenommenen Änderungen.

Sie können Dateien, Ordner und Volumes von On-Access-Scans ausschließen. Unter Umständen kann sich anbieten, folgende Elemente auszuschließen:

- Große Dateien, deren Scan viel Zeit in Anspruch nehmen kann
- Dateien, die einen Scan-Fehler auslösen können
- Dateien, die einen Fehlalarm auslösen können
- Backup-Volumes, weil die darauf gespeicherten Dateien beim Sichern ohnehin gescannt werden

Wichtig: Wenn Sie Dateien, Ordner oder Volumes vom Scan ausschließen, verringert sich der Schutz vor Threats.

Verfahren Sie dazu wie folgt:

1. Wählen Sie **Sophos Anti-Virus** > **Einstellungen** .
2. Klicken Sie auf **On-Access-Scans**.
3. Wenn bestimmte Einstellungen nicht hervorgehoben sind, klicken Sie auf das Schlosssymbol und geben Sie einen Administratorennamen und ein Kennwort ein.
4. Klicken Sie auf **Ausgeschlossene Objekte**.
5. Führen Sie einen der folgenden Schritte aus:
   - Ziehen Sie das gewünschte Objekt/die gewünschten Objekte in die Ausschlussliste.
   - Klicken Sie auf **Hinzufügen** (+) und wählen Sie die auszuschließenden Objekte aus.

   Näheres zur Bestimmung der auszuschließenden Objekte finden Sie unter *Ausschlussregeln* (Seite 9).

2.2.2.2 Bearbeiten von On-Access-Scan-Ausschlüssen

Wichtig: Wenn Sie in Ihrem Unternehmen Standardeinstellungen festgelegt haben, haben diese möglicherweise Vorrang vor hier vorgenommenen Änderungen.

Verfahren Sie dazu wie folgt:

1. Wählen Sie **Sophos Anti-Virus** > **Einstellungen** .
2. Klicken Sie auf **On-Access-Scans**.
3. Wenn bestimmte Einstellungen nicht hervorgehoben sind, klicken Sie auf das Schlosssymbol und geben Sie einen Administratorennamen und ein Kennwort ein.
4. Klicken Sie auf **Ausgeschlossene Objekte**.
5. Doppelklicken Sie in der Ausschlussliste auf das gewünschte Objekt und bearbeiten Sie es.

   Näheres zur Bestimmung der auszuschließenden Objekte finden Sie unter *Ausschlussregeln* (Seite 9).

2.2.2.3 Ausschlussregeln

Sie können beim Hinzufügen oder Bearbeiten von auszuschließenden Objekten jeden gewünschten POSIX-Pfad eingeben, egal ob es sich dabei um ein Volume, einen Ordner oder eine Datei handelt. Folgende Regeln gilt es bei der Auswahl der auszuschließenden Objekte zu beachten.

Auszuschließende Objekte	Syntax
Ordner inklusive Unterordner	Hängen Sie einen Schrägstrich an das auszuschließende Objekt an.
Ordner ohne Unterordner	Hängen Sie einen doppelten Schrägstrich an das auszuschließende Objekt an.
Datei	Hängen Sie *keinen* Schrägstrich/doppelten Schrägstrich an das auszuschließende Objekt an.
Ordner/Datei an einem bestimmten Speicherort	Setzen Sie einen Schrägstrich vor das auszuschließende Objekt.
Lokaler Ordner/lokale Datei oder Ordner/Datei im Netzwerk	Setzen Sie *keinen* Schrägstrich vor das auszuschließende Objekt.
Datei mit bestimmter Dateierweiterung	Ersetzen Sie den Stamm des Dateinamens durch ein Sternchen (*).

Beispiele

Pfad	Ausgeschlossene Objekte
/Mein Ordner/Meine Programme	Die Datei "Meine Programme" an einem bestimmten Speicherort
/Mein Ordner/	Alle Dateien im Ordner "Mein Ordner" an einem bestimmten Speicherort inklusive Unterordner

Pfad	Ausgeschlossene Objekte
/Mein Ordner//	Alle Dateien im Ordner "Mein Ordner" an einem bestimmten Speicherort ohne Unterordner
Mein Ordner/Meine Programme	Die Datei "Meine Programme" in einem beliebigen Ordner mit der Bezeichnung "Mein Ordner", lokal oder auf dem Netzwerk
Mein Ordner/	Alle Dateien in einem beliebigen Ordner mit der Bezeichnung "Mein Ordner", lokal oder im Netzwerk, inklusive Unterordner
Mein Ordner//	Alle Dateien in einem beliebigen Ordner mit der Bezeichnung "Mein Ordner", lokal oder im Netzwerk, ohne Unterordner
Meine Programme	Die Datei "Meine Programme" an einem beliebigen Ort, lokal oder im Netzwerk
*.mov	Alle Dateien mit der Erweiterung ".mov" an einem beliebigen Ort, lokal oder im Netzwerk
/Mein Ordner/*.mov	Alle Dateien mit der Erweiterung ".mov" an einem bestimmten Speicherort

2.2.2.4 Löschen von On-Access-Ausschlüssen

Wichtig: Wenn Sie in Ihrem Unternehmen Standardeinstellungen festgelegt haben, haben diese möglicherweise Vorrang vor hier vorgenommenen Änderungen.

Verfahren Sie dazu wie folgt:

1. Wählen Sie **Sophos Anti-Virus** > **Einstellungen** .
2. Klicken Sie auf **On-Access-Scans**.
3. Wenn bestimmte Einstellungen nicht hervorgehoben sind, klicken Sie auf das Schlosssymbol und geben Sie einen Administratorennamen und ein Kennwort ein.
4. Klicken Sie auf **Ausgeschlossene Objekte**.
5. Wählen Sie den zu löschenden Ausschluss in der Ausschlussliste aus und klicken Sie auf **Löschen** (-).

2.2.2.5 Aktivieren von On-Access-Scans in Archiven und komprimierten Dateien

Wichtig: Wenn Sie in Ihrem Unternehmen Standardeinstellungen festgelegt haben, haben diese möglicherweise Vorrang vor hier vorgenommenen Änderungen.

Standardmäßig sind On-Access-Scans in Archiven und komprimierten Dateien deaktiviert. Wenn Sie jedoch mehrere Dateien gleichzeitig bearbeiten, ist die Gefahr, dass ein Threat nicht erkannt wird, groß. Dann bietet sich an, die Option zu aktivieren. Dies kann etwa der Fall sein, wenn Sie Archive oder komprimierte Dateien an einen wichtigen Kunden schicken.

Hinweis: Aus folgenden Gründen empfiehlt sich die Auswahl dieser Option nicht:

- Das Scannen in Archivdateien und komprimierten Dateien wird erheblich verlangsamt.
- Auch wenn diese Option nicht aktiviert ist, wird eine aus einem Archiv extrahierte Datei beim Öffnen gescannt.
- Auch wenn diese Option nicht aktiviert ist, werden Dateien gescannt, die mit dynamischen Komprimierungsprogrammen (PKLite, LZEXE und Diet) gepackt wurden.

So aktivieren Sie On-Access-Scans in Archiven und komprimierten Dateien:

1. Wählen Sie **Sophos Anti-Virus** > **Einstellungen** .
2. Klicken Sie auf **On-Access-Scans**.
3. Wenn bestimmte Einstellungen nicht hervorgehoben sind, klicken Sie auf das Schlosssymbol und geben Sie einen Administratorennamen und ein Kennwort ein.
4. Klicken Sie auf **Optionen**.
5. Wählen Sie **In Archiven und komprimierten Dateien scannen**.

2.2.2.6 Aktivieren von On-Access-Scans in Netzwerkvolumes

Wichtig: Wenn Sie in Ihrem Unternehmen Standardeinstellungen festgelegt haben, haben diese möglicherweise Vorrang vor hier vorgenommenen Änderungen.

Standardmäßig werden Dateien in Netzwerkvolumes nicht bei Zugriff gescannt, da dies den Dateizugriff verlangsamen kann.

So aktivieren Sie On-Access-Scans in Netzwerkvolumes:

1. Wählen Sie **Sophos Anti-Virus** > **Einstellungen** .
2. Klicken Sie auf **On-Access-Scans**.
3. Wenn bestimmte Einstellungen nicht hervorgehoben sind, klicken Sie auf das Schlosssymbol und geben Sie einen Administratorennamen und ein Kennwort ein.
4. Klicken Sie auf **Optionen**.
5. Wählen Sie **Dateien auf Netzwerk-Volumes**.

Hinweis: Dateien in Netzwerk-Volumes, auf die über einen anderen Namen zugegriffen wird, werden nicht gescannt.

2.2.2.7 Konfigurieren von On-Access-Scans zum automatischen Bereinigen von Threats

Wichtig: Wenn Sie in Ihrem Unternehmen Standardeinstellungen festgelegt haben, haben diese möglicherweise Vorrang vor hier vorgenommenen Änderungen.

Es empfiehlt sich, Threats über den Quarantäne-Manager zu bereinigen (Details finden Sie unter *Vorgehensweise bei Threaterkennung* (Seite 33)). Sie können On-Access-Scans so konfigurieren, dass erkannte Threats automatisch bereinigt werden.

Wichtig: Sophos Anti-Virus fordert den Benutzer vor dem Löschen eines Threats nicht zur Bestätigung auf.

So konfigurieren Sie On-Access-Scans zum automatischen Bereinigen von Threats:

1. Wählen Sie **Sophos Anti-Virus** > **Einstellungen** .
2. Klicken Sie auf **On-Access-Scans**.

3. Wenn bestimmte Einstellungen nicht hervorgehoben sind, klicken Sie auf das Schlosssymbol und geben Sie einen Administratorennamen und ein Kennwort ein.
4. Wählen Sie die Option **Threat bereinigen** aus dem Einblendmenü **Bei Erkennung eines Threats** aus.
5. Wählen Sie im Einblendmenü **Bei fehlgeschlagener Bereinigung** die Maßnahme aus, die Sophos Anti-Virus bei fehlgeschlagener Bereinigung ergreifen soll:
   - Wenn Sie den Zugriff auf den Threat verweigern möchten, wählen Sie **Zugriff verweigern**.
   - Wählen Sie zum Löschen eines Threats **Threat löschen** aus.
   - Wenn Sie Threats verschieben möchten, damit diese nicht ausgeführt werden können, aktivieren Sie das Kontrollkästchen **Zugriff verweigern und Threat verschieben**.

     Standardmäßig werden die Threats in den Ordner /Benutzer/Für alle Benutzer/Infected/ verschoben. Sie können jedoch auch auf **Ordnerauswahl** klicken und einen anderen Ordner angeben.

Im Protokoll von Sophos Anti-Virus werden alle Maßnahmen, die Sophos Anti-Virus bei infizierten Objekten vorgenommen hat, festgehalten.

Wichtig: Durch die Bereinigung werden unter Umständen nicht alle vom Threat vorgenommenen Maßnahmen nicht rückgängig gemacht. Wenn der Threat beispielsweise eine Einstellung modifiziert hat, ist bei der Bereinigung unter Umständen die Originaleinstellung nicht mehr bekannt. Sie müssen möglicherweise die Konfiguration des Macs überprüfen. Durch die Bereinigung werden vom Threat am Dokument vorgenommene Änderungen nicht rückgängig gemacht.

2.2.2.8 Konfigurieren von On-Access-Scans zum automatischen Verschieben von Threats

Wichtig: Wenn Sie in Ihrem Unternehmen Standardeinstellungen festgelegt haben, haben diese möglicherweise Vorrang vor hier vorgenommenen Änderungen.

Es empfiehlt sich, Threats über den Quarantäne-Manager zu bereinigen (Details finden Sie unter *Vorgehensweise bei Threaterkennung* (Seite 33)). Sie können On-Access-Scans auch so konfigurieren, dass erkannte Threats automatisch in einen anderen Ordner verschoben werden. Das Verschieben eines infizierten Programms senkt das Risiko, dass das Programm gestartet wird. Hinweis: Sofern On-Access-Scans aktiviert sind, verweigert Sophos Anti-Virus den Zugriff auf verschobene Dateien.

Wichtig: Diese Option sollten Sie nur nach Rücksprache mit dem technischen Support von Sophos verwenden. Sophos Anti-Virus fordert den Benutzer vor dem Löschen eines Threats nicht zur Bestätigung auf.

So können Sie On-Access-Scans zum automatischen Verschieben von Threats konfigurieren:

1. Wählen Sie **Sophos Anti-Virus** > **Einstellungen** .
2. Klicken Sie auf **On-Access-Scans**.
3. Wenn bestimmte Einstellungen nicht hervorgehoben sind, klicken Sie auf das Schlosssymbol und geben Sie einen Administratorennamen und ein Kennwort ein.

4. Wählen Sie die Option **Zugriff verweigern und Threat verschieben** aus dem Einblendmenü **Bei Erkennung eines Threats** aus.

   Standardmäßig werden die Threats in den Ordner /Benutzer/Für alle Benutzer/Infected/ verschoben. Sie können jedoch auch auf **Ordnerauswahl** klicken und einen anderen Ordner angeben.

Im Protokoll von Sophos Anti-Virus werden alle Maßnahmen, die Sophos Anti-Virus bei infizierten Objekten vorgenommen hat, festgehalten.

2.2.2.9 Konfigurieren von On-Access-Scans zum automatischen Löschen von Threats

Wichtig: Wenn Sie in Ihrem Unternehmen Standardeinstellungen festgelegt haben, haben diese möglicherweise Vorrang vor hier vorgenommenen Änderungen.

Es empfiehlt sich, Threats über den Quarantäne-Manager zu bereinigen (Details finden Sie unter *Vorgehensweise bei Threaterkennung* (Seite 33)). Sie können On-Access-Scans so konfigurieren, dass erkannte Threats automatisch gelöscht werden.

Wichtig: Diese Option sollten Sie nur nach Rücksprache mit dem technischen Support von Sophos verwenden. Sophos Anti-Virus fordert den Benutzer vor dem Löschen eines Threats nicht zur Bestätigung auf.

So können Sie On-Access-Scans zum automatischen Löschen von Threats konfigurieren:

1. Wählen Sie **Sophos Anti-Virus** > **Einstellungen** .
2. Klicken Sie auf **On-Access-Scans**.
3. Wenn bestimmte Einstellungen nicht hervorgehoben sind, klicken Sie auf das Schlosssymbol und geben Sie einen Administratorennamen und ein Kennwort ein.
4. Wählen Sie die Option **Threat löschen** aus dem Einblendmenü **Bei Erkennung eines Threats** aus.

Im Protokoll von Sophos Anti-Virus werden alle Maßnahmen, die Sophos Anti-Virus bei infizierten Objekten vorgenommen hat, festgehalten.

Wichtig: Durch das Löschen werden vom Threat vorgenommene Maßnahmen nicht rückgängig gemacht.

2.2.2.10 Wiederherstellen der On-Access-Scan-Voreinstellungen

Sie können die Voreinstellungen zu On-Access-Scans wiederherstellen. Wenn Sie in Ihrem Unternehmen Standardeinstellungen für On-Access-Scans festgelegt haben, werden diese Einstellungen wiederhergestellt. Andernfalls werden die von Sophos empfohlenen Standardwerte übernommen.

So stellen Sie die On-Access-Scan-Voreinstellungen wieder her:

1. Wählen Sie **Sophos Anti-Virus** > **Einstellungen** .
2. Klicken Sie auf **On-Access-Scans**.
3. Wenn bestimmte Einstellungen nicht hervorgehoben sind, klicken Sie auf das Schlosssymbol und geben Sie einen Administratorennamen und ein Kennwort ein.
4. Klicken Sie auf **Voreinstellungen wiederherstellen**.

2.2.2.11 Konfigurieren von Bildschirm-Alerts

Wichtig: Wenn Sie in Ihrem Unternehmen Standardeinstellungen festgelegt haben, haben diese möglicherweise Vorrang vor hier vorgenommenen Änderungen.

Sophos Anti-Virus zeigt einen Bildschirm-Alert an, wenn bei On-Access-Scans Fehler auftreten. Standardmäßig werden auch Bildschirm-Alerts angezeigt, wenn das Programm bei On-Access-Scans Threats erkennt. Sie können die Bildschirm-Alerts, die bei Threat-Erkennung angezeigt werden, konfigurieren.

So konfigurieren Sie Bildschirm-Alerts:

1. Wählen Sie **Sophos Anti-Virus** > **Einstellungen** .
2. Klicken Sie auf **Benachrichtigung**.
3. Wenn bestimmte Einstellungen nicht hervorgehoben sind, klicken Sie auf das Schlosssymbol und geben Sie einen Administratorennamen und ein Kennwort ein.
4. Ändern Sie die Einstellungen wie folgt:
   - Wenn Sie den Text von Bildschirm-Alerts zu Threats ergänzen möchten, geben Sie die Meldung in das Feld **Benutzerdefinierte Nachricht hinzufügen** ein.
   - Deaktivieren Sie zum Deaktivieren von Bildschirm-Alerts die Option **Anzeigen einer Desktop-Benachrichtigung bei Threat-Erkennung bei Zugriff**.

2.2.2.12 Wiederherstellen der Alert-Einstellungen

Sie können die Voreinstellungen für Alerts wiederherstellen. Wenn Sie in Ihrem Unternehmen Standard-Alert-Einstellungen festgelegt haben, werden diese Einstellungen wiederhergestellt. Andernfalls werden die von Sophos empfohlenen Standardwerte übernommen.

So stellen Sie die Alert-Einstellungen wieder her:

1. Wählen Sie **Sophos Anti-Virus** > **Einstellungen** .
2. Klicken Sie auf **Benachrichtigung**.
3. Wenn bestimmte Einstellungen nicht hervorgehoben sind, klicken Sie auf das Schlosssymbol und geben Sie einen Administratorennamen und ein Kennwort ein.
4. Klicken Sie auf **Voreinstellungen wiederherstellen**.

2.2.2.13 Ändern der Protokolleinstellungen

Wichtig: Wenn Sie in Ihrem Unternehmen Standardeinstellungen festgelegt haben, haben diese möglicherweise Vorrang vor hier vorgenommenen Änderungen.

Alle Aktivitäten von On-Access-Scans (einschließlich Threat-Erkennungen) werden im Sophos On-Access-Scan-Protokoll und im Update-Protokoll verzeichnet. Sophos Anti-Virus kann solche Aktivitäten auch im Mac OS X-Systemprotokoll festhalten.

Verfahren Sie wie folgt, um die Protokolleinstellungen von On-Access-Scans und Updates zu ändern:

1. Wählen Sie **Sophos Anti-Virus** > **Einstellungen** .
2. Klicken Sie auf **Protokoll**.
3. Wenn bestimmte Einstellungen nicht hervorgehoben sind, klicken Sie auf das Schlosssymbol und geben Sie einen Administratorennamen und ein Kennwort ein.

4. Ändern Sie die Einstellungen wie folgt:
   - Sie können den Dateinamen und den Speicherort des Protokolls ändern: Klicken Sie auf **Protokolldatei wählen** und geben Sie den neuen Dateinamen bzw. Speicherort ein.
   - Klicken Sie zum Löschen aller Protokolleinträge auf **Protokoll löschen**.
   - Aktivieren Sie die Option **Systemprotokoll erstellen**, wenn alle Aktivitäten und Ergebnisse von On-Access-Scans und Updates im Systemprotokoll festgehalten werden sollen.

2.2.2.14 Wiederherstellen der Protokolleinstellungen

Sie können die Voreinstellungen der Protokolle zu On-Access-Scans und Updates wiederherstellen. Wenn Sie in Ihrem Unternehmen Standardprotokolleinstellungen festgelegt haben, werden diese Einstellungen wiederhergestellt. Andernfalls werden die von Sophos empfohlenen Standardwerte übernommen.

So stellen Sie die Protokolleinstellungen wieder her:

1. Wählen Sie **Sophos Anti-Virus** > **Einstellungen** .
2. Klicken Sie auf **Protokoll**.
3. Wenn bestimmte Einstellungen nicht hervorgehoben sind, klicken Sie auf das Schlosssymbol und geben Sie einen Administratorennamen und ein Kennwort ein.
4. Klicken Sie auf **Voreinstellungen wiederherstellen**.

2.2.3 Aufrufen von On-Access-Scan- und Update-Protokollen

Verfahren Sie wie folgt, um ein Protokoll aller Aktivitäten von On-Access-Scans (auch erkannte Threats) und Updates aufzurufen:

1. Wählen Sie **Sophos Anti-Virus** > **Einstellungen** .
2. Klicken Sie im **Protokollfenster** auf **Protokoll anzeigen**.

Das Protokoll wird in der Konsole angezeigt. Am Anfang des Protokolleintrags wird jeweils angezeigt, ob es sich um einen Eintrag des On-Access-Scanners (com.sophos.intercheck) oder von AutoUpdate (com.sophos.autoupdate) handelt.

2.3 Scannen lokaler Laufwerke

Scans lokaler Laufwerke werden vom Benutzer eingeleitet. Hierbei werden alle Dateien gescannt, auf die auf lokalen Volumes zugegriffen werden kann. Wenn Sie sich als Administrator authentifizieren, werden auch Dateien gescannt, auf die Sie nicht zugreifen können. Hierzu zählen auch angeschlossene Wechselmedien.

Scans lokaler Laufwerke bieten sich in folgenden Fällen an: Sie möchten einen von Sophos Anti-Virus erkannten Threat verarbeiten, es werden keine On-Access-Scans auf dem Mac ausgeführt, weil es sich um einen Server handelt, oder Sie möchten infizierte Dateien *vor dem Verwenden* auffinden.

2.3.1 Scannen lokaler Laufwerke

Sie können alle Dateien auf dem Mac scannen, auf die Sie Zugriff haben. Wenn Sie als Administrator angemeldet sind, können auch alle Dateien einbezogen werden, auf die Sie für gewöhnlich *nicht* zugreifen können.

❖ Wenn Sie alle lokalen Volumes, für die Sie Schreibzugriff besitzen, scannen möchten, wählen Sie **Scan** > **Scannen lokaler Laufwerke** .

Sophos Anti-Virus zeigt den Scan-Fortschritt im Fenster **Scans** an.

Hinweis: Sie können den Scan jedoch auch wie folgt ausführen:

- Klicken Sie im Fenster **Scans** im Feld **Scannen lokaler Laufwerke** auf die Wiedergabeschaltfläche.
- Klicken Sie auf das Symbol von Sophos Anti-Virus auf der rechten Seite der Menüleiste und wählen Sie anschließend die Option **Lokale Laufwerke scannen** aus dem Kurzbefehlmenü aus.
- Drücken Sie auf die „ctrl"-Taste und klicken Sie mit der Maustaste auf das Symbol von Sophos Anti-Virus im Dock. Wählen Sie dann im Kurzbefehlmenü die Option **Scannen lokaler Laufwerke** aus.

2.3.2 Konfigurieren von Scans lokaler Laufwerke

2.3.2.1 Deaktivieren des Scannens in Archiven und komprimierten Dateien bei Scans lokaler Laufwerke

Hinweis: Die genannte Einstellung gilt für Scans lokaler Laufwerke und Objekt-Scans im Finder.

Standardmäßig ist das Scannen in Archiven und komprimierten Dateien bei Scans lokaler Laufwerke aktiviert.

So deaktivieren Sie das Scannen in Archiven und komprimierten Dateien bei Scans lokaler Laufwerke:

1. Wählen Sie **Sophos Anti-Virus** > **Einstellungen** .

   Hinweis: Sie können jedoch auch im Fenster **Scans** im Feld **Scannen lokaler Laufwerke** auf Bearbeiten klicken.

2. Deaktivieren Sie im Feld **Scannen lokaler Laufwerke** das Kontrollkästchen **In Archiven und komprimierten Dateien scannen**.

2.3.2.2 Konfigurieren des Scans lokaler Laufwerke zum automatischen Bereinigen von Threats

Hinweis: Die genannte Einstellung gilt für Scans lokaler Laufwerke und Objekt-Scans im Finder.

Es empfiehlt sich, Threats über den Quarantäne-Manager zu bereinigen (Details finden Sie unter *Vorgehensweise bei Threaterkennung* (Seite 33)). Sie können Scans lokaler Laufwerke so konfigurieren, dass erkannte Threats automatisch bereinigt werden.

Wichtig: Sophos Anti-Virus fordert den Benutzer vor dem Löschen eines Threats nicht zur Bestätigung auf.

So konfigurieren Sie Scans lokaler Laufwerke zum automatischen Bereinigen von Threats:

1. Wählen Sie **Sophos Anti-Virus** > **Einstellungen** .

   Hinweis: Sie können jedoch auch im Fenster **Scans** im Feld **Scannen lokaler Laufwerke** auf Bearbeiten klicken.

2. Wählen Sie im Feld **Scannen lokaler Laufwerke** die Option **Threat bereinigen** aus dem Einblendmenü **Bei Erkennung eines Threats** aus.
3. Wählen Sie im Einblendmenü **Bei fehlgeschlagener Bereinigung** die Maßnahme aus, die Sophos Anti-Virus bei fehlgeschlagener Bereinigung ergreifen soll:

   - Wenn keine Maßnahme ergriffen werden soll, wählen Sie **Nur protokollieren** aus. Wenn Sie jedoch E-Mail-Benachrichtigungen aktiviert haben, sendet Sophos Anti-Virus auch eine E-Mail-Benachrichtigung.
   - Wählen Sie zum Löschen eines Threats **Threat löschen** aus.
   - Wenn Sie Threats verschieben möchten, damit diese nicht ausgeführt werden können, aktivieren Sie das Kontrollkästchen **Threat verschieben**.

     Standardmäßig werden die Threats in den Ordner /Benutzer/Für alle Benutzer/Infected/ verschoben. Sie können jedoch auch auf **Ordnerauswahl** klicken und einen anderen Ordner angeben.

Im Protokoll des Scans lokaler Laufwerke werden alle Maßnahmen, die Sophos Anti-Virus bei Threats vorgenommen hat, festgehalten.

Wichtig: Durch die Bereinigung werden unter Umständen nicht alle vom Threat vorgenommenen Maßnahmen nicht rückgängig gemacht. Wenn der Threat beispielsweise eine Einstellung modifiziert hat, ist bei der Bereinigung unter Umständen die Originaleinstellung nicht mehr bekannt. Sie müssen möglicherweise die Konfiguration des Macs überprüfen. Durch die Bereinigung werden vom Threat am Dokument vorgenommene Änderungen nicht rückgängig gemacht.

2.3.2.3 Konfigurieren des Scans lokaler Laufwerke zum automatischen Verschieben von Threats

Hinweis: Die genannte Einstellung gilt für Scans lokaler Laufwerke und Objekt-Scans im Finder.

Es empfiehlt sich, Threats über den Quarantäne-Manager zu bereinigen (Details finden Sie unter *Vorgehensweise bei Threaterkennung* (Seite 33)). Sie können Scans lokaler Laufwerke auch so konfigurieren, dass erkannte Threats automatisch in einen anderen Ordner verschoben werden. Das Verschieben eines infizierten Programms senkt das Risiko, dass das Programm gestartet wird.

Wichtig: Diese Option sollten Sie nur nach Rücksprache mit dem technischen Support von Sophos verwenden. Sophos Anti-Virus fordert den Benutzer vor dem Löschen eines Threats nicht zur Bestätigung auf.

So können Sie den Scan lokaler Laufwerke zum automatischen Verschieben von Threats konfigurieren:

1. Wählen Sie **Sophos Anti-Virus** > **Einstellungen** .

   Hinweis: Sie können jedoch auch im Fenster **Scans** im Feld **Scannen lokaler Laufwerke** auf Bearbeiten klicken.

2. Wählen Sie im Feld **Scannen lokaler Laufwerke** die Option **Threat löschen** aus dem Einblendmenü **Bei Erkennung eines Threats** aus.

   Standardmäßig werden die Threats in den Ordner /Benutzer/Für alle Benutzer/Infected/ verschoben. Sie können jedoch auch auf **Ordnerauswahl** klicken und einen anderen Ordner angeben.

Im Protokoll des Scans lokaler Laufwerke werden alle Maßnahmen, die Sophos Anti-Virus bei Threats vorgenommen hat, festgehalten.

2.3.2.4 Konfigurieren des Scans lokaler Laufwerke zum automatischen Löschen von Threats

Hinweis: Die genannte Einstellung gilt für Scans lokaler Laufwerke und Objekt-Scans im Finder.

Es empfiehlt sich, Threats über den Quarantäne-Manager zu bereinigen (Details finden Sie unter *Vorgehensweise bei Threaterkennung* (Seite 33)). Sie können Scans lokaler Laufwerke so konfigurieren, dass erkannte Threats automatisch gelöscht werden.

Wichtig: Diese Option sollten Sie nur nach Rücksprache mit dem technischen Support von Sophos verwenden. Sophos Anti-Virus fordert den Benutzer vor dem Löschen eines Threats nicht zur Bestätigung auf.

So können Sie den Scan lokaler Laufwerke zum automatischen Löschen von Threats konfigurieren:

1. Wählen Sie **Sophos Anti-Virus** > **Einstellungen** .

   Hinweis: Sie können jedoch auch im Fenster **Scans** im Feld **Scannen lokaler Laufwerke** auf Bearbeiten klicken.

2. Wählen Sie im Feld **Scannen lokaler Laufwerke** die Option **Threat löschen** aus dem Einblendmenü **Bei Erkennung eines Threats** aus.

Im Protokoll des Scans lokaler Laufwerke werden alle Maßnahmen, die Sophos Anti-Virus bei Threats vorgenommen hat, festgehalten.

Wichtig: Durch das Löschen werden vom Threat vorgenommene Maßnahmen nicht rückgängig gemacht.

2.3.2.5 Wiederherstellen der Voreinstellungen bei Scans lokaler Laufwerke

Hinweis: Die genannte Einstellung gilt für Scans lokaler Laufwerke und Objekt-Scans im Finder.

So können Sie die von Sophos empfohlenen Standardeinstellungen für Scans lokaler Laufwerke wiederherstellen:

1. Wählen Sie **Sophos Anti-Virus** > **Einstellungen** .

   Hinweis: Sie können jedoch auch im Fenster **Scans** im Feld **Scannen lokaler Laufwerke** auf Bearbeiten klicken.

2. Klicken Sie im Feld **Scannen lokaler Laufwerke** auf **Voreinstellungen wiederherstellen**.

2.3.3 Aufrufen des Protokolls zu Scans lokaler Laufwerke

❖ Wählen Sie **Scan** > **Protokoll anzeigen** .

Das Protokoll wird in der Konsole angezeigt.

2.4 Individuelle Scans

Individuelle Scans werden vom Benutzer eingeleitet. Hierbei werden bestimmte Dateien, Ordner oder Volumes gescannt.

Individuelle Scans bieten sich an, wenn Sie nur verdächtige Festplattenabschnitte scannen oder infizierte Dateien *vor dem Verwenden* auffinden möchten.

Wichtig: Wenn Sie eine Management-Konsole einsetzen, werden möglichweise noch weitere geplante Scans angezeigt. Sie können diese Scans nicht bearbeiten oder deaktivieren. Administratoren können über die Management-Konsole geplante Scans jedoch löschen.

2.4.1 Ausführen eines individuellen Scans

1. Öffnen Sie das Fenster **Scans** ggf. über die Option **Fenster** > **Scans** .
2. Wenn die Liste der **individuellen Scans** nicht angezeigt wird, klicken Sie auf das Dreieck neben **Individuelle Scans**.
3. Wählen Sie den gewünschten Scan aus der Liste **Individuelle Scans** aus.
4. Klicken Sie auf die Schaltfläche **Jetzt scannen**.

   Der Scan-Fortschritt wird im Fenster **Sophos Anti-Virus** angezeigt.

2.4.2 Hinzufügen von individuellen Scans

1. Wählen Sie **Datei** > **Neu** .
2. Der Scaneditor wird angezeigt. Bearbeiten Sie den Scan darin wie folgt:
   - Wenn Sie den Scan umbenennen möchten, geben Sie einen neuen Namen in das Feld **Scan-Name** ein.
   - Sie können den Scan-Inhalt anhand der Anweisungen unter *Festlegen des Scan-Inhalts* (Seite 22) festlegen.

- Sie können Objekte vom Scan ausschließen. Informationen hierzu finden Sie unter *Hinzufügen von Ausschlüssen bei individuellen Scans* (Seite 22), *Bearbeiten von Ausschlüssen bei individuellen Scans* (Seite 23) und *Löschen von Ausschlüssen bei individuellen Scans* (Seite 24).
- Wenn Sie Archive und komprimierte Dateien scannen möchten, verfahren Sie anhand der Anweisungen unter *Deaktivieren des Scannens in Archiven und komprimierten Dateien bei individuellen Scans* (Seite 25).

Der Scan wird in die Liste der **individuellen Scans** im Fenster **Scans** angezeigt.

Hinweis:

Sie können den Scan jedoch auch wie folgt hinzufügen:

- Klicken Sie auf **Hinzufügen** (+) im unteren Bereich des Fensters **Scans**.
- Ziehen Sie im Finder die zu scannenden Objekte an eine freie Stelle in der Liste **Individuelle Scans**.

2.4.3 Hinzufügen eines individuellen Scans eines Threats

Wenn ein Threat im Quarantäne-Manager aufgeführt wird, können Sie einen individuellen Scan hierzu hinzufügen.

1. Öffnen Sie das Fenster **Scans** ggf. über die Option **Fenster** > **Scans** .
2. Wenn die Liste der **individuellen Scans** nicht angezeigt wird, klicken Sie auf das Dreieck neben **Individuelle Scans**.
3. Wenn das Fenster **Quarantäne-Manager** nicht geöffnet ist, wählen Sie **Fenster** > **Quarantäne-Manager** , um es zu öffnen.
4. Führen Sie im Quarantäne-Manager eine der folgenden Aktionen durch:
   - Wählen Sie aus der Threat-Liste die Threats aus, die zum individuellen Scan hinzugefügt werden sollen.

     Ziehen Sie die ausgewählten Threats an eine freie Stelle in der Liste **Individuelle Scans**.
   - Wählen Sie im Feld **Threat-Details** die Dateien aus, die zum individuellen Scan hinzugefügt werden sollen.

     Ziehen Sie die ausgewählten Dateien an eine freie Stelle in der Liste **Individuelle Scans**.
   - Klicken Sie im Feld **Threat-Details** auf **Pfad und Dateiname** und wählen Sie **Inidviduellen Scan aus den Dateien erstellen** im Einblendmenü aus.
5. Geben Sie zum Umbenennen des Scans im Scaneditor den neuen Namen in das Feld **Scan-Name** ein.
6. Wählen Sie im Feld **Optionen** die Option **Threat löschen** aus dem Einblendmenü **Bei Erkennung eines Threats** aus.

Der Scan wird zur Liste der **individuellen Scans** hinzugefügt.

2.4.4 Kopieren von individuellen Scans

1. Öffnen Sie das Fenster **Scans** ggf. über die Option **Fenster** > **Scans** .
2. Wenn die Liste der **individuellen Scans** nicht angezeigt wird, klicken Sie auf das Dreieck neben **Individuelle Scans**.
3. Wählen Sie den gewünschten Scan aus der Liste **Individuelle Scans** aus.
4. Wählen Sie **Datei** > **Duplizieren** .
5. Doppelklicken Sie auf den neuen Scan und bearbeiten Sie ihn wie folgt:
   - Wenn Sie den Scan umbenennen möchten, geben Sie einen neuen Namen in das Feld **Scan-Name** ein.
   - Sie können den Scan-Inhalt anhand der Anweisungen unter *Festlegen des Scan-Inhalts* (Seite 22) festlegen.
   - Sie können Objekte vom Scan ausschließen. Informationen hierzu finden Sie unter *Hinzufügen von Ausschlüssen bei individuellen Scans* (Seite 22), *Bearbeiten von Ausschlüssen bei individuellen Scans* (Seite 23) und *Löschen von Ausschlüssen bei individuellen Scans* (Seite 24).
   - Wenn Sie Archive und komprimierte Dateien scannen möchten, verfahren Sie anhand der Anweisungen unter *Deaktivieren des Scannens in Archiven und komprimierten Dateien bei individuellen Scans* (Seite 25).

Der Scan wird in die Liste der **individuellen Scans** im Fenster **Scans** angezeigt.

Hinweis: Sie können außerdem einen ausgewählten Scan im Fenster **Scans** anhand einer der folgenden Methoden kopieren:

- Drücken Sie Befehlstaste-D.
- Wählen Sie im unteren Fensterbereich die Option **Duplizieren** aus dem Einblendmenü „Maßnahme“ aus.

2.4.5 Konfigurieren eines individuellen Scans

2.4.5.1 Öffnen des Editors für individuelle Scans

1. Öffnen Sie das Fenster **Scans** ggf. über die Option **Fenster** > **Scans** .
2. Wenn die Liste der **individuellen Scans** nicht angezeigt wird, klicken Sie auf das Dreieck neben **Individuelle Scans**.
3. Doppelklicken Sie im Fenster **Individuelle Scans** auf den zu bearbeitenden Scan.

Hinweis: Sie können den Editor jedoch auch wie folgt öffnen:

- Wählen Sie den gewünschten Scan aus und klicken Sie auf „Bearbeiten“.
- Wählen Sie den gewünschten Scan aus und klicken Sie im Einblendmenü „Maßnahme“ auf die Option **Scan bearbeiten**.

2.4.5.2 Umbenennen eines individuellen Scans

1. Öffnen Sie den Scaneditor. Nähere Anweisungen hierzu finden Sie unter *Öffnen des Editors für individuelle Scans* (Seite 21).
2. Geben Sie im Scaneditor den neuen Namen in das Feld **Scan-Name** ein.

2.4.5.3 Festlegen des Scan-Inhalts

❖ Führen Sie einen der folgenden Schritte aus:

- Ziehen Sie im Finder die zum individuellen Scan im Fenster **Scans**.
- Klicken Sie im Scan-Editor auf **Hinzufügen** (+) und wählen Sie die zu scannenden Objekte aus.

  Anweisungen zum Öffnen des Scan-Editors finden Sie unter *Öffnen des Editors für individuelle Scans* (Seite 21).

Hinweis: Wenn Sie nicht über die erforderlichen Zugriffsrechte zum Anzeigen des Ordnerinhalts verfügen, weist Sophos Anti-Virus durch ein entsprechendes Ordnersymbol ("Kein Zugriff") darauf hin. Der Ordner wird nicht gescannt.

2.4.5.4 Hinzufügen eines Threats zu einem individuellen Scan

Wenn ein Threat im Quarantäne-Manager aufgeführt wird, können Sie ihn zu einem vorhandenen individuellen Scan hinzufügen.

1. Öffnen Sie das Fenster **Scans** ggf. über die Option **Fenster** > **Scans** .
2. Wenn die Liste der **individuellen Scans** nicht angezeigt wird, klicken Sie auf das Dreieck neben **Individuelle Scans**.
3. Wenn das Fenster **Quarantäne-Manager** nicht geöffnet ist, wählen Sie **Fenster** > **Quarantäne-Manager** , um es zu öffnen.
4. Führen Sie im Quarantäne-Manager eine der folgenden Aktionen durch:

   - Wählen Sie aus der Threat-Liste die Threats aus, die zu einem vorhandenen individuellen Scan hinzugefügt werden sollen.

     Ziehen Sie die ausgewählten Threats zum gewählten Scan in der Liste **Individuelle Scans**.
   - Wählen Sie im Feld **Threat-Details** die Dateien aus, die zu einem vorhandenen individuellen Scan hinzugefügt werden sollen.

     Ziehen Sie die ausgewählten Dateien zum gewählten Scan in der Liste **Individuelle Scans**.

   Hinweis: Wenn der Editor für den gewünschten Scan bereits geöffnet ist, können Sie die gewählten Threats bzw. Dateien auch hierhin ziehen.

2.4.5.5 Hinzufügen von Ausschlüssen bei individuellen Scans

Sie können Dateien, Ordner und Volumes von einem individuellen Scan ausschließen. Unter Umständen kann sich anbieten, folgende Elemente auszuschließen:

- Große Dateien, deren Scan viel Zeit in Anspruch nehmen kann

- Dateien, die einen Scan-Fehler auslösen können
- Dateien, die einen Fehlalarm auslösen können
- Backup-Volumes, weil die darauf gespeicherten Dateien beim Sichern ohnehin gescannt werden.

Wichtig: Wenn Sie Dateien, Ordner oder Volumes vom Scan ausschließen, verringert sich der Schutz vor Threats.

So können Sie einen Ausschluss zu einem individuellen Scan hinzufügen:

1. Öffnen Sie den Scaneditor. Nähere Anweisungen hierzu finden Sie unter *Öffnen des Editors für individuelle Scans* (Seite 21).
2. Führen Sie im Fenster **Ausgeschlossene Objekte** einen der folgenden Schritte durch:
   - Ziehen Sie das gewünschte Objekt/die gewünschten Objekte in die Ausschlussliste.
   - Klicken Sie auf **Hinzufügen** (+) und wählen Sie die auszuschließenden Objekte aus.

   Näheres zur Bestimmung der auszuschließenden Objekte finden Sie unter *Ausschlussregeln* (Seite 23).

2.4.5.6 Bearbeiten von Ausschlüssen bei individuellen Scans

1. Öffnen Sie den Scaneditor. Nähere Anweisungen hierzu finden Sie unter *Öffnen des Editors für individuelle Scans* (Seite 21).
2. Doppelklicken Sie im Feld **Ausgeschlossene Objekte** auf das gewünschte Objekt und bearbeiten Sie dieses.

   Näheres zur Bestimmung der auszuschließenden Objekte finden Sie unter *Ausschlussregeln* (Seite 23).

2.4.5.7 Ausschlussregeln

Sie können beim Hinzufügen oder Bearbeiten von auszuschließenden Objekten jeden gewünschten POSIX-Pfad eingeben, egal ob es sich dabei um ein Volume, einen Ordner oder eine Datei handelt. Folgende Regeln gilt es bei der Auswahl der auszuschließenden Objekte zu beachten.

Auszuschließende Objekte	Syntax
Ordner inklusive Unterordner	Hängen Sie einen Schrägstrich an das auszuschließende Objekt an.
Ordner ohne Unterordner	Hängen Sie einen doppelten Schrägstrich an das auszuschließende Objekt an.
Datei	Hängen Sie *keinen* Schrägstrich/doppelten Schrägstrich an das auszuschließende Objekt an.
Ordner/Datei an einem bestimmten Speicherort	Setzen Sie einen Schrägstrich vor das auszuschließende Objekt.

Auszuschließende Objekte	Syntax
Lokaler Ordner/lokale Datei oder Ordner/Datei im Netzwerk	Setzen Sie *keinen* Schrägstrich vor das auszuschließende Objekt.
Datei mit bestimmter Dateierweiterung	Ersetzen Sie den Stamm des Dateinamens durch ein Sternchen (*).

Beispiele

Pfad	Ausgeschlossene Objekte
/Mein Ordner/Meine Programme	Die Datei "Meine Programme" an einem bestimmten Speicherort
/Mein Ordner/	Alle Dateien im Ordner "Mein Ordner" an einem bestimmten Speicherort inklusive Unterordner
/Mein Ordner//	Alle Dateien im Ordner "Mein Ordner" an einem bestimmten Speicherort ohne Unterordner
Mein Ordner/Meine Programme	Die Datei "Meine Programme" in einem beliebigen Ordner mit der Bezeichnung "Mein Ordner", lokal oder auf dem Netzwerk
Mein Ordner/	Alle Dateien in einem beliebigen Ordner mit der Bezeichnung "Mein Ordner", lokal oder im Netzwerk, inklusive Unterordner
Mein Ordner//	Alle Dateien in einem beliebigen Ordner mit der Bezeichnung "Mein Ordner", lokal oder im Netzwerk, ohne Unterordner
Meine Programme	Die Datei "Meine Programme" an einem beliebigen Ort, lokal oder im Netzwerk
*.mov	Alle Dateien mit der Erweiterung ".mov" an einem beliebigen Ort, lokal oder im Netzwerk
/Mein Ordner/*.mov	Alle Dateien mit der Erweiterung ".mov" an einem bestimmten Speicherort

2.4.5.8 Löschen von Ausschlüssen bei individuellen Scans

1. Öffnen Sie den Scaneditor. Nähere Anweisungen hierzu finden Sie unter *Öffnen des Editors für individuelle Scans* (Seite 21).
2. Wählen Sie im Fenster **Ausgeschlossene Objekte** das zu löschende Objekt aus und klicken Sie auf **Löschen** (-).

2.4.5.9 Deaktivieren des Scannens in Archiven und komprimierten Dateien bei individuellen Scans

Archive und komprimierte Dateien werden standardmäßig gescannt.

So deaktivieren Sie das Scannen in Archiven und komprimierten Dateien bei individuellen Scans:

1. Öffnen Sie den Scaneditor. Nähere Anweisungen hierzu finden Sie unter *Öffnen des Editors für individuelle Scans* (Seite 21).
2. Deaktivieren Sie im Feld **Optionen** das Kontrollkästchen **In Archiven und komprimierten Dateien scannen**.

2.4.5.10 Zeitliche Planung von individuellen Scans

Administratoren können individuelle Scans so konfigurieren, dass sie zu bestimmten Zeiten automatisch ausgeführt werden. Scans können an bestimmten Wochentagen und zu bestimmten Zeiten ausgeführt werden.

1. Öffnen Sie den Scaneditor. Nähere Anweisungen hierzu finden Sie unter *Öffnen des Editors für individuelle Scans* (Seite 21).
2. Wählen Sie im Feld **Zeitplan** das Kontrollkästchen „**Zeitplan aktivieren**“ aus.
3. Geben Sie an, an welchen Tagen der individuelle Scan ausgeführt werden soll.
4. Klicken Sie auf **Hinzufügen** (+), um eine neue Uhrzeit hinzuzufügen.
5. Legen Sie die gewünschte Uhrzeit fest.

Hinweis: Per Klick auf **Hinzufügen** (+) bzw. **Entfernen** (-) können Sie weitere Uhrzeiten hinzufügen/entfernen.

2.4.5.11 Konfigurieren eines individuellen Scans zum automatischen Bereinigen von Threats

Es empfiehlt sich, Threats über den Quarantäne-Manager zu bereinigen (Details finden Sie unter *Vorgehensweise bei Threaterkennung* (Seite 33)). Sie können individuelle Scans so konfigurieren, dass erkannte Threats automatisch bereinigt werden.

Wichtig: Sophos Anti-Virus fordert den Benutzer vor dem Löschen eines Threats nicht zur Bestätigung auf.

So konfigurieren Sie einen individuellen Scan zum automatischen Bereinigen von Threats:

1. Öffnen Sie den Scaneditor. Nähere Anweisungen hierzu finden Sie unter *Öffnen des Editors für individuelle Scans* (Seite 21).
2. Wählen Sie im Feld **Optionen** die Option **Threat bereinigen** aus dem Einblendmenü **Bei Erkennung eines Threats** aus.
3. Wählen Sie im Einblendmenü **Bei fehlgeschlagener Bereinigung** die Maßnahme aus, die Sophos Anti-Virus bei fehlgeschlagener Bereinigung ergreifen soll:
   - Wenn keine Maßnahme ergriffen werden soll, wählen Sie **Nur protokollieren** aus. Wenn Sie jedoch E-Mail-Benachrichtigungen aktiviert haben, sendet Sophos Anti-Virus auch eine E-Mail-Benachrichtigung.
   - Wählen Sie zum Löschen eines Threats **Threat löschen** aus.

- Wenn Sie Threats verschieben möchten, damit diese nicht ausgeführt werden können, aktivieren Sie das Kontrollkästchen **Threat verschieben**.

  Standardmäßig werden die Threats in den Ordner /Benutzer/Für alle Benutzer/Infected/ verschoben. Sie können jedoch auch auf **Ordnerauswahl** klicken und einen anderen Ordner angeben.

Im Protokoll des individuellen Scans werden alle Maßnahmen, die Sophos Anti-Virus bei Threats vorgenommen hat, festgehalten.

Wichtig: Durch die Bereinigung werden unter Umständen nicht alle vom Threat vorgenommenen Maßnahmen nicht rückgängig gemacht. Wenn der Threat beispielsweise eine Einstellung modifiziert hat, ist bei der Bereinigung unter Umständen die Originaleinstellung nicht mehr bekannt. Sie müssen möglicherweise die Konfiguration des Macs überprüfen. Durch die Bereinigung werden vom Threat am Dokument vorgenommene Änderungen nicht rückgängig gemacht.

2.4.5.12 Konfigurieren eines individuellen Scans zum automatischen Verschieben von Threats

Es empfiehlt sich, Threats über den Quarantäne-Manager zu bereinigen (Details finden Sie unter *Vorgehensweise bei Threaterkennung* (Seite 33)). Sie können einen individuellen Scan auch so konfigurieren, dass erkannte Threats automatisch in einen anderen Ordner verschoben werden. Das Verschieben eines infizierten Programms senkt das Risiko, dass das Programm gestartet wird.

Wichtig: Diese Option sollten Sie nur nach Rücksprache mit dem technischen Support von Sophos verwenden. Sophos Anti-Virus fordert den Benutzer vor dem Löschen eines Threats nicht zur Bestätigung auf.

So können Sie einen individuellen Scan zum automatischen Verschieben von Threats konfigurieren:

1. Öffnen Sie den Scaneditor. Nähere Anweisungen hierzu finden Sie unter *Öffnen des Editors für individuelle Scans* (Seite 21).
2. Wählen Sie im Feld **Optionen** die Option **Threat verschieben** aus dem Einblendmenü **Bei Erkennung eines Threats** aus.

   Standardmäßig werden die Threats in den Ordner /Benutzer/Für alle Benutzer/Infected/ verschoben. Sie können jedoch auch auf **Ordnerauswahl** klicken und einen anderen Ordner angeben.

Im Protokoll des individuellen Scans werden alle Maßnahmen, die Sophos Anti-Virus bei Threats vorgenommen hat, festgehalten.

2.4.5.13 Konfigurieren eines individuellen Scans zum automatischen Löschen von Threats

Es empfiehlt sich, Threats über den Quarantäne-Manager zu bereinigen (Details finden Sie unter *Vorgehensweise bei Threaterkennung* (Seite 33)). Sie können individuelle Scans so konfigurieren, dass erkannte Threats automatisch gelöscht werden.

Wichtig: Diese Option sollten Sie nur nach Rücksprache mit dem technischen Support von Sophos verwenden. Sophos Anti-Virus fordert den Benutzer vor dem Löschen eines Threats nicht zur Bestätigung auf.

So können Sie einen individuellen Scan zum automatischen Löschen von Threats konfigurieren:

1. Öffnen Sie den Scaneditor. Nähere Anweisungen hierzu finden Sie unter *Öffnen des Editors für individuelle Scans* (Seite 21).
2. Wählen Sie im Feld **Optionen** die Option **Threat löschen** aus dem Einblendmenü **Bei Erkennung eines Threats** aus.

Im Protokoll des individuellen Scans werden alle Maßnahmen, die Sophos Anti-Virus bei Threats vorgenommen hat, festgehalten.

Wichtig: Durch das Löschen werden vom Threat vorgenommene Maßnahmen nicht rückgängig gemacht.

2.4.6 Löschen eines individuellen Scans

1. Öffnen Sie das Fenster **Scans** ggf. über die Option **Fenster** > **Scans** .
2. Wenn die Liste der **individuellen Scans** nicht angezeigt wird, klicken Sie auf das Dreieck neben **Individuelle Scans**.
3. Wählen Sie den gewünschten Scan aus der Liste **Individuelle Scans** aus.
4. Klicken Sie auf **Löschen** (-).

2.4.7 Aufrufen eines Protokolls eines individuellen Scans

1. Öffnen Sie das Fenster **Scans** ggf. über die Option **Fenster** > **Scans** .
2. Wenn die Liste der **individuellen Scans** nicht angezeigt wird, klicken Sie auf das Dreieck neben **Individuelle Scans**.
3. Wählen Sie im Fenster **Individuelle Scans** den Scan aus, dessen Protokoll Sie anzeigen möchten.
4. Wählen Sie im unteren Fensterbereich die Option **Scanprotokoll anzeigen** aus dem Einblendmenü „Maßnahme“ aus.

Das Protokoll wird in der Konsole angezeigt.

2.5 Objekt-Scans im Finder

Objekt-Scans im Finder werden vom Benutzer eingeleitet. Hierbei werden im Finder ausgewählte Dateien, Ordner oder Volumes gescannt.

Objekt-Scans im Finder bieten sich in folgenden Fällen an: Sie möchten die Inhalte von Archiven oder komprimierten Dateien *vor* dem Öffnen scannen, etwas vor dem Versand per E-Mail scannen oder eine CD oder DVD scannen.

2.5.1 Starten eines Objekt-Scans im Finder über ein Kurzbefehlmenü

1. Wählen Sie die Datei, den Ordner oder das Volume, das Sie scannen möchten, im Finder aus.

   Mehrfachauswahl ist möglich.

2. Drücken Sie auf die „ctrl“-Taste und klicken Sie mit der Maustaste auf die Auswahl und verfahren Sie wie folgt:
   - Wählen Sie unter Mac OS X, Version 10.5, **Mehr** > **Scannen mit Sophos Anti-Virus** aus dem Kurzbefehlmenü aus.
   - Wählen Sie bei anderen Mac OS X-Versionen **Jetzt mit Sophos Anti-Virus scannen** aus dem Kurzbefehlmenü aus.

   Sophos Anti-Virus zeigt den Scanfortschritt in einem Fenster an.

2.5.2 Starten von Objekt-Scans im Finder durch Ziehen von Objekten ins Dock

1. Wählen Sie die Datei, den Ordner oder das Volume, das Sie scannen möchten, im Finder aus.

   Mehrfachauswahl ist möglich.
2. Ziehen Sie die Auswahl in das Programm Sophos Anti-Virus im Dock.

   Sophos Anti-Virus zeigt den Scanfortschritt in einem Fenster an.

2.5.3 Ausführen eines Objekt-Scans im Finder über das Untermenü „Dienste“

1. Wählen Sie unter Mac OS X, Version 10.6, die Datei, den Ordner oder das Volume, das Sie scannen möchten, im Finder aus.

   Mehrfachauswahl ist möglich.
2. Wählen Sie **Finder** > **Dienste** > **Scannen mit Sophos Anti-Virus** .

   Sophos Anti-Virus zeigt den Scanfortschritt in einem Fenster an.

2.5.4 Konfigurieren von Objekt-Scans im Finder

2.5.4.1 Deaktivieren des Scannens in Archiven und komprimierten Dateien bei Objekt-Scans im Finder

Hinweis: Die genannte Einstellung gilt für Scans lokaler Laufwerke und Objekt-Scans im Finder.

Standardmäßig ist das Scannen in Archiven und komprimierten Dateien bei Objekt-Scans im Finder aktiviert.

So deaktivieren Sie das Scannen in Archiven und komprimierten Dateien bei Objekt-Scans im Finder:

1. Wählen Sie **Sophos Anti-Virus** > **Einstellungen** .
2. Deaktivieren Sie im Feld **Scannen lokaler Laufwerke** das Kontrollkästchen **In Archiven und komprimierten Dateien scannen**.

2.5.4.2 Konfigurieren von Objekt-Scans im Finder zum automatischen Bereinigen von Threats

Hinweis: Die genannte Einstellung gilt für Scans lokaler Laufwerke und Objekt-Scans im Finder.

Es empfiehlt sich, Threats über den Quarantäne-Manager zu bereinigen (Details finden Sie unter *Vorgehensweise bei Threaterkennung* (Seite 33)). Sie können Objekt-Scans im Finder so konfigurieren, dass erkannte Threats automatisch bereinigt werden.

Wichtig: Sophos Anti-Virus fordert den Benutzer vor dem Löschen eines Threats nicht zur Bestätigung auf.

So konfigurieren Sie Objekt-Scans im Finder zum automatischen Bereinigen von Threats:

1. Wählen Sie **Sophos Anti-Virus** > **Einstellungen** .
2. Wählen Sie im Feld **Scannen lokaler Laufwerke** die Option **Threat bereinigen** aus dem Einblendmenü **Bei Erkennung eines Threats** aus.
3. Wählen Sie im Einblendmenü **Bei fehlgeschlagener Bereinigung** die Maßnahme aus, die Sophos Anti-Virus bei fehlgeschlagener Bereinigung ergreifen soll:

   - Wenn keine Maßnahme ergriffen werden soll, wählen Sie **Nur protokollieren** aus. Wenn Sie jedoch E-Mail-Benachrichtigungen aktiviert haben, sendet Sophos Anti-Virus auch eine E-Mail-Benachrichtigung.
   - Wählen Sie zum Löschen eines Threats **Threat löschen** aus.
   - Wenn Sie Threats verschieben möchten, damit diese nicht ausgeführt werden können, aktivieren Sie das Kontrollkästchen **Threat verschieben**.

     Standardmäßig werden die Threats in den Ordner /Benutzer/Für alle Benutzer/Infected/ verschoben. Sie können jedoch auch auf **Ordnerauswahl** klicken und einen anderen Ordner angeben.

Im Protokoll des Objekt-Scans im Finder werden alle Maßnahmen, die Sophos Anti-Virus bei Threats vorgenommen hat, festgehalten.

Wichtig: Durch die Bereinigung werden unter Umständen nicht alle vom Threat vorgenommenen Maßnahmen nicht rückgängig gemacht. Wenn der Threat beispielsweise eine Einstellung modifiziert hat, ist bei der Bereinigung unter Umständen die Originaleinstellung nicht mehr bekannt. Sie müssen möglicherweise die Konfiguration des Macs überprüfen. Durch die Bereinigung werden vom Threat am Dokument vorgenommene Änderungen nicht rückgängig gemacht.

2.5.4.3 Konfigurieren von Objekt-Scans im Finder zum automatischen Verschieben von Threats

Hinweis: Die genannte Einstellung gilt für Scans lokaler Laufwerke und Objekt-Scans im Finder.

Es empfiehlt sich, Threats über den Quarantäne-Manager zu bereinigen (Details finden Sie unter *Vorgehensweise bei Threaterkennung* (Seite 33)). Sie können Objekt-Scans im Finder auch so konfigurieren, dass erkannte Threats automatisch in einen anderen Ordner verschoben werden. Das Verschieben eines infizierten Programms senkt das Risiko, dass das Programm gestartet wird.

Wichtig: Diese Option sollten Sie nur nach Rücksprache mit dem technischen Support von Sophos verwenden. Sophos Anti-Virus fordert den Benutzer vor dem Löschen eines Threats nicht zur Bestätigung auf.

So können Sie Objekt-Scans im Finder zum automatischen Verschieben von Threats konfigurieren:

1. Wählen Sie **Sophos Anti-Virus** > **Einstellungen** .
2. Wählen Sie im Feld **Scannen lokaler Laufwerke** die Option **Threat löschen** aus dem Einblendmenü **Bei Erkennung eines Threats** aus.

   Standardmäßig werden die Threats in den Ordner /Benutzer/Für alle Benutzer/Infected/ verschoben. Sie können jedoch auch auf **Ordnerauswahl** klicken und einen anderen Ordner angeben.

Im Protokoll des Objekt-Scans im Finder werden alle Maßnahmen, die Sophos Anti-Virus bei Threats vorgenommen hat, festgehalten.

2.5.4.4 Konfigurieren von Objekt-Scans im Finder zum automatischen Löschen von Threats

Hinweis: Die genannte Einstellung gilt für Scans lokaler Laufwerke und Objekt-Scans im Finder.

Es empfiehlt sich, Threats über den Quarantäne-Manager zu bereinigen (Details finden Sie unter *Vorgehensweise bei Threaterkennung* (Seite 33)). Sie können Objekt-Scans im Finder so konfigurieren, dass erkannte Threats automatisch gelöscht werden.

Wichtig: Diese Option sollten Sie nur nach Rücksprache mit dem technischen Support von Sophos verwenden. Sophos Anti-Virus fordert den Benutzer vor dem Löschen eines Threats nicht zur Bestätigung auf.

So können Sie Objekt-Scans im Finder zum automatischen Löschen von Threats konfigurieren:

1. Wählen Sie **Sophos Anti-Virus** > **Einstellungen** .
2. Wählen Sie im Feld **Scannen lokaler Laufwerke** die Option **Threat löschen** aus dem Einblendmenü **Bei Erkennung eines Threats** aus.

Im Protokoll des Objekt-Scans im Finder werden alle Maßnahmen, die Sophos Anti-Virus bei Threats vorgenommen hat, festgehalten.

Wichtig: Durch das Löschen werden vom Threat vorgenommene Maßnahmen nicht rückgängig gemacht.

2.5.4.5 Wiederherstellen der Voreinstellungen bei Objekt-Scans im Finder

Hinweis: Die genannte Einstellung gilt für Scans lokaler Laufwerke und Objekt-Scans im Finder.

So können Sie die von Sophos empfohlenen Standardeinstellungen für Objekt-Scans im Finder wiederherstellen:

1. Wählen Sie **Sophos Anti-Virus** > **Einstellungen** .
2. Klicken Sie im Feld **Scannen lokaler Laufwerke** auf **Voreinstellungen wiederherstellen**.

2.5.5 Aufrufen eines Protokolls zu Objekt-Scans im Finder

❖ Klicken Sie in der Fortschrittsanzeige, die bei einem Objekt-Scan im Finder angezeigt wird, auf **Scan-Protokoll anzeigen**.

Das Protokoll wird in der Konsole angezeigt.

2.6 Konfigurieren von E-Mail-Benachrichtigungen

Wichtig: Wenn Sie in Ihrem Unternehmen Standardeinstellungen festgelegt haben, haben diese möglicherweise Vorrang vor hier vorgenommenen Änderungen.

Sophos Anti-Virus kann Benutzer per E-Mail über erkannte Bedrohungen oder schwerwiegende Fehler informieren. Diese Optionen werden für On-Access-Scans, Scans lokaler Laufwerke, individuelle Scans und Objektscans im Finder angeboten. Standardmäßig sind E-Mail-Benachrichtigungen deaktiviert.

So konfigurieren Sie E-Mail-Benachrichtigungen:

1. Wählen Sie **Sophos Anti-Virus** > **Einstellungen** .
2. Klicken Sie auf **Benachrichtigung**.
3. Wenn bestimmte Einstellungen nicht hervorgehoben sind, klicken Sie auf das Schlosssymbol und geben Sie einen Administratorennamen und ein Kennwort ein.
4. Wählen Sie die Option „**Senden eines E-Mail-Alerts bei Threat-Erkennung oder Fehlern**“ aus.
5. Ändern Sie die Einstellungen wie folgt:
   - Wenn Sie möchten, dass Sie Sophos Anti-Virus ausschließlich über erkannte Bedrohungen per E-Mail in Kenntnis setzt, wählen Sie die Option **Threats**.
   - Wenn Sie von Sophos Anti-Virus per E-Mail über erkannte Bedrohungen und schwerwiegende Fehler informiert werden möchten, wählen Sie die Option **Threats und Fehler melden**.
   - Geben Sie zur Angabe der *Empfängeradresse* für die E-Mail-Benachrichtigungen die gewünschte E-Mail-Adresse in das Feld **Empfänger** ein.
   - Geben Sie die Adresse des E-Mail-Servers für die E-Mail-Benachrichtigungen in das Feld **Server für ausgehende E-Mails** ein.
   - Geben Sie die gewünschte *Absenderadresse* für die E-Mail-Benachrichtigungen in das Feld **Absender** ein.

2.7 Wiederherstellen der Alert-Einstellungen

Sie können die Voreinstellungen für Alerts wiederherstellen. Wenn Sie in Ihrem Unternehmen Standard-Alert-Einstellungen festgelegt haben, werden diese Einstellungen wiederhergestellt. Andernfalls werden die von Sophos empfohlenen Standardwerte übernommen.

So stellen Sie die Alert-Einstellungen wieder her:

1. Wählen Sie **Sophos Anti-Virus** > **Einstellungen** .

2. Klicken Sie auf **Benachrichtigung**.
3. Wenn bestimmte Einstellungen nicht hervorgehoben sind, klicken Sie auf das Schlosssymbol und geben Sie einen Administratorennamen und ein Kennwort ein.
4. Klicken Sie auf **Voreinstellungen wiederherstellen**.

2.8 Live-Schutz

Der Live-Schutz basiert auf einem Online-Abgleich mit der Datenbank potenzieller Threats. Wenn die Funktion aktiviert ist, vergleicht Sophos Anti-Virus verdächtige Dateien mit der Datenbank in der Cloud ab. So wird festgelegt, ob eine Datei blockiert oder zugelassen werden soll. So konfigurieren Sie den Live-Schutz:

1. Wählen Sie **Sophos Anti-Virus** > **Einstellungen** .
2. Klicken Sie auf **Benachrichtigung**.
3. Wenn bestimmte Einstellungen nicht hervorgehoben sind, klicken Sie auf das Schlosssymbol und geben Sie einen Administratorennamen und ein Kennwort ein.
4. Wählen Sie „**Live-Schutz aktivieren**“, um den Live-Schutz zu aktivieren.

2.9 Wiederherstellen der Standardeinstellungen des Live-Schutzes

Sie können die Standardeinstellung des Live-Schutzes wiederherstellen. Wenn Sie eine Standardeinstellung zum Live-Schutz vorgenommen haben, wird diese übernommen. Andernfalls werden die von Sophos empfohlenen Standardwerte übernommen.

So stellen Sie die Standardeinstellungen des Live-Schutzes wieder her:

1. Wählen Sie **Sophos Anti-Virus** > **Einstellungen** .
2. Klicken Sie auf **Live-Schutz**.
3. Wenn bestimmte Einstellungen nicht hervorgehoben sind, klicken Sie auf das Schlosssymbol und geben Sie einen Administratorennamen und ein Kennwort ein.
4. Klicken Sie auf **Voreinstellungen wiederherstellen**.

2.10 Aufrufen von Sophos Anti-Virus über Terminal

Sie können einen Scan über Terminal, die Befehlszeilenoberfläche von Mac OS X, durchführen. So können Sie die Hilfe zur Befehlszeile anzeigen:

1. Öffnen Sie Terminal.
   Suchen Sie den Ordner /Programme/Dienstprogramme und doppelklicken Sie auf Terminal.
2. Geben Sie Folgendes in die Befehlszeile ein:

```
sweep -h
```

3 Vorgehensweise bei Threaterkennung

Wenn ein Threat auf dem Mac erkannt wird, wird er im sogenannten Quarantäne-Manager aufgeführt. Öffnen Sie den Quarantäne-Manager und verarbeiten Sie den Threat dort.

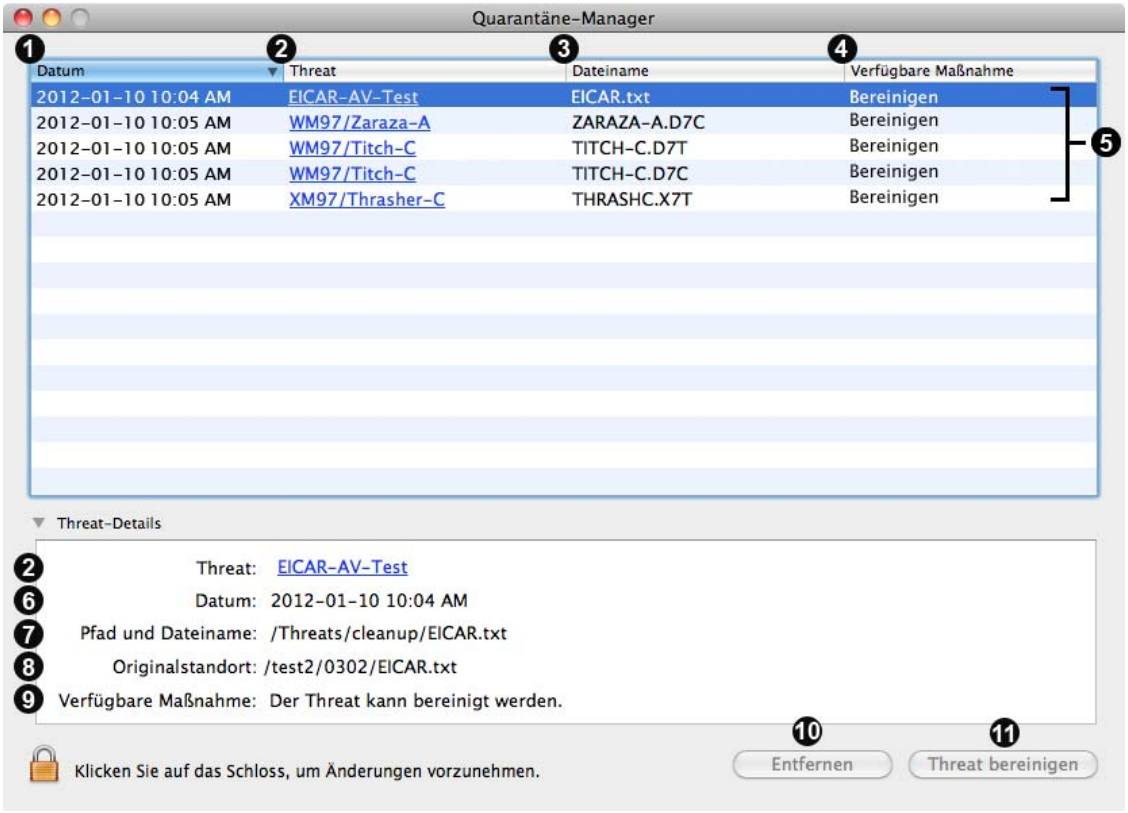
3.1 Öffnen des Quarantäne-Managers

Sie können den Quarantäne-Manager anhand einer der folgenden Methoden öffnen:

- Wählen Sie **Fenster** > **Quarantäne-Manager** .
- Klicken Sie auf das Symbol von Sophos Anti-Virus auf der rechten Seite der Menüleiste und wählen Sie anschließend die Option **Quarantäne-Manager öffnen** aus dem Kurzbefehlmenü aus.
- Klicken Sie im Fenster von **Scans** auf **Quarantäne-Manager**.

3.2 Über den Quarantäne-Manager

Im Quarantäne-Manager werden alle beim Scan erkannten Threats aufgeführt, so dass Sie sie verarbeiten können. Die Bestandteile des **Quarantäne-Manager**-Fensters werden unten angezeigt:



1. Datum und Uhrzeit der Erkennung. Wenn ein Threat mehrmals erkannt wurde, wird hier nur die erste Erkennung aufgeführt.

2. Name des Threats sowie ein Link zur Analyse auf der Sophos Website.
3. Die mit dem Threat in Verbindung stehende Hauptdatei.
4. Die zur Verfügung stehenden Maßnahmen.
5. Eine Liste aller erkannten Threats. Sie können die Threats durch Klicken auf die Spaltenüberschriften sortieren. Sie können jeweils einen oder mehrere Threats gleichzeitig zur weiteren Verarbeitung auswählen. Es können maximal 200 Threats aufgelistet werden. Wird diese Grenze erreicht, werden die ältesten durch die neuesten Threats ersetzt.
6. Datum und Uhrzeit der Erkennung. Wenn ein Threat mehrmals erkannt wurde, wird hier nur die erste und letzte Erkennung aufgeführt.
7. Speicherort und Namen aller Dateien, die den Threat umfassen.
8. Wenn der Threat beim Scannen verschoben oder teilweise entfernt wurde, wird dieses Element angezeigt. Alle Original-Dateien, die den Threat umfassen, werden aufgeführt.
9. Die zur Verfügung stehenden Maßnahmen sowie ggf. eine Zusammenfassung aller bisher ergriffenen Maßnahmen.
10. Klicken Sie auf **Aus der Liste entfernen**, um einen ausgewählten Threat aus dem Quarantäne-Manager zu entfernen, ohne den Threat selbst zu verarbeiten. Weitere Informationen finden Sie unter *Löschen eines Threats aus dem Quarantäne-Manager* (Seite 36).
11. Klicken Sie auf **Threat bereinigen**, um einen ausgewählten Threat zu bereinigen. Weitere Informationen finden Sie unter *Verarbeiten von Threats im Quarantäne-Manager* (Seite 34).

3.3 Anzeige der Threat-Details im Quarantäne-Manager

Aus dem Quarantäne-Manager geht hervor, wie sich ein Threat auf den Mac auswirkt. Sie können beispielsweise sehen, welche Dateien den Threat enthalten.

Zur Anzeige bestimmter Daten müssen Sie sich zunächst authentifizieren. Klicken Sie hierzu auf das Schlosssymbol im unteren Bereich des **Quarantäne-Manager**-Fensters.

So können Sie Threat-Details im Quarantäne-Manager aufrufen:

1. Wählen Sie im Quarantäne-Manager den gewünschten Threat aus.

   Sie können mehrere Threats auswählen. Bei Mehrfachauswahl sind die angezeigten Informationen jedoch weniger ausführlich.

2. Klicken Sie auf das Dreieck neben **Threat-Details**.

   Die Informationen werden im Fenster **Threat-Details** angezeigt. Beschreibungen zu den jeweiligen Feldern finden Sie unter *Über den Quarantäne-Manager* (Seite 33).

Wenn lange Dateipfade zur Anzeige gekürzt werden, können Sie sie in die Zwischenablage kopieren und in einen Texteditor einfügen. Klicken Sie im Feld **Threat-Details** auf **Pfad und Dateiname** und wählen Sie **Pfade der Dateien kopieren** im Einblendmenü aus.

3.4 Verarbeiten von Threats im Quarantäne-Manager

1. Klicken Sie im Quarantäne-Manager auf die Spaltenüberschrift **Verfügbare Maßnahme**, um die Threats anhand der verfügbaren Maßnahmen zu gruppieren.

2. Wählen Sie alle Threats aus, bei denen die verfügbare Maßnahme **Bereinigen** lautet.
3. Klicken Sie auf **Threat bereinigen**.

   Sie müssen sich zunächst authentifizieren. Klicken Sie hierzu auf das Schlosssymbol im unteren Bereich des **Quarantäne-Manager**-Fensters.

   Bereinigte Threats werden aus der Liste gelöscht.

4. Klicken Sie auf die Spaltenüberschrift **Verfügbare Maßnahme**, um die Threatliste zu sortieren.
5. Wenn die Maßnahme für bestimmte Threats **Neu starten** lautet, wird die Bereinigung erst nach einem Neustart des Macs abgeschlossen.
6. Klicken Sie auf die Spaltenüberschrift **Verfügbare Maßnahme**, um die Threatliste zu sortieren.
7. Wenn Threats vorhanden sind, bei denen die verfügbare Maßnahme **Scannen lokaler Laufwerke**, scannen Sie die lokalen Laufwerke (Details hierzu finden Sie unter *Scannen lokaler Laufwerke* (Seite 16)).
8. Klicken Sie auf die Spaltenüberschrift **Verfügbare Maßnahme**, um die Threatliste zu sortieren.
9. Wenn Threats vorhanden sind, bei denen die Maßnahmen **Bereinigen** lautet, gehen Sie wieder zu Schritt 3 zurück.
10. Wenn Threats vorhanden sind, bei denen die Maßnahmen **Manuell bereinigen** lautet:

    a) Fügen Sie einen neuen individuellen Scan der Threats hinzu (entsprechende Anweisungen entnehmen Sie bitte dem Abschnitt *Hinzufügen eines individuellen Scans eines Threats* (Seite 20).

    b) Führen Sie den Scan anhand der Anweisungen im Abschnitt *Ausführen eines individuellen Scans* (Seite 19).

Wichtig: Durch die Bereinigung werden unter Umständen nicht alle vom Threat vorgenommenen Maßnahmen nicht rückgängig gemacht. Wenn der Threat beispielsweise eine Einstellung modifiziert hat, ist bei der Bereinigung unter Umständen die Originaleinstellung nicht mehr bekannt. Sie müssen möglicherweise die Konfiguration des Macs überprüfen. Durch die Bereinigung werden vom Threat am Dokument vorgenommene Änderungen nicht rückgängig gemacht.

3.5 Deaktivieren von Warnhinweisen zur Bereinigung

Standardmäßig zeigt Sophos Anti-Virus vor dem Bereinigen von Threats einen Warnhinweis im Quarantäne-Manager an.

So deaktivieren Sie den Warnhinweis:

1. Wählen Sie **Sophos Anti-Virus** > **Einstellungen** .
2. Klicken Sie auf **Benachrichtigung**.
3. Wenn bestimmte Einstellungen nicht hervorgehoben sind, klicken Sie auf das Schlosssymbol und geben Sie einen Administratorennamen und ein Kennwort ein.
4. Deaktivieren Sie die Option **Anzeigen einer Warnung vor der Bereinigung von Threats im Quarantäne-Manager**.

Hinweis: Sie können jedoch auch die Option **Diese Meldung nicht mehr anzeigen** im Warnhinweis auswählen.

3.6 Löschen eines Threats aus dem Quarantäne-Manager

Zum Bereinigen eines Threats müssen Sie sich zunächst authentifizieren. Klicken Sie hierzu auf das Schlosssymbol im unteren Bereich des **Quarantäne-Manager**-Fensters.

In folgenden Fällen kann es sich anbieten, einen Threat zu löschen:

- Es handelt sich um einen Fehlalarm
- Sie sind sich sicher, dass Sie den Threat manuell bereinigt haben
- Sie haben das infizierte Wechselmedium entfernt
- Vor dem Scannen lokaler Laufwerke möchten Sie die Liste leeren

So löschen Sie einen Threat aus dem Quarantäne-Manager:

1. Wählen Sie aus dem Quarantäne-Manager den Threat aus, den Sie löschen möchten. Mehrfachauswahl ist möglich.
2. Klicken Sie auf **Aus der Liste entfernen**.

Dadurch werden keine Dateien gelöscht.

4 Updates

4.1 Sofort-Update von Sophos Anti-Virus

Sophos Anti-Virus führt standardmäßig ein Update pro Stunde durch. Sie können jedoch auch ein Sofort-Update durchführen.

Verfahren Sie wie folgt, um ein Sofort-Update von Sophos Anti-Virus einzuleiten:

- Wählen Sie **Sophos Anti-Virus** > **Jetzt aktualisieren** .
- Klicken Sie auf das Sophos Anti-Virus Symbol auf der rechten Seite der Menüleiste und wählen Sie anschließend die Option **Jetzt aktualisieren** aus dem Kurzbefehlmenü aus.
- Drücken Sie auf die „ctrl"-Taste und klicken Sie mit der Maustaste auf das Symbol von Sophos Anti-Virus im Dock. Wählen Sie dann im Kurzbefehlmenü die Option **Jetzt aktualisieren** aus.

Ein dynamischer Pfeil beim Sophos Anti-Virus Symbol auf der rechten Seite der Menüleiste weist darauf hin, dass ein Update durchgeführt wird.

4.2 Konfigurieren der Updates

4.2.1 Auswahl der Update-Quelle

Wichtig: Wenn Sie in Ihrem Unternehmen Standardeinstellungen festgelegt haben, haben diese möglicherweise Vorrang vor hier vorgenommenen Änderungen.

So können Sie die Update-Quelle für Sophos Anti-Virus festlegen:

1. Wählen Sie **Sophos Anti-Virus** > **Einstellungen** .
2. Klicken Sie auf **AutoUpdate**.
3. Wenn bestimmte Einstellungen nicht hervorgehoben sind, klicken Sie auf das Schlosssymbol und geben Sie einen Administratorennamen und ein Kennwort ein.
4. Ändern Sie die Einstellungen wie folgt:
   - Wenn Sophos Anti-Virus Updates direkt von Sophos beziehen soll, wählen Sie im Einblendmenü **Update vom Primärserver** die Option **Sophos** aus. Geben Sie Ihre Sophos Zugangsdaten in die Felder **Benutzername** und **Kennwort** ein.
   - Wenn Sophos Anti-Virus Updates direkt von Ihrem Unternehmens-Webserver beziehen soll, wählen Sie aus dem Einblendmenü **Update vom Primärserver** die Option **Unternehmens-Webserver** aus. Geben Sie in das **Adressfeld** die Internetadresse der Update-Quelle an. Geben Sie die Zugangsdaten des Servers in die Felder **Benutzername** und **Kennwort** ein.
   - Wenn Sophos Anti-Virus Updates aus einem Netzwerkvolume beziehen soll, wählen Sie im Einblendmenü **Update vom Primärserver** die Option **Netzwerkvolume** aus. Geben Sie in das **Adressfeld** die Netzwerkadresse der Update-Quelle an. Geben Sie in die Felder **Benutzername** und **Kennwort** die Zugangsdaten des Volumes ein.

   Die Adresse lautet etwa wie folgt: Der Text in Klammern muss angepasst werden:

http://<Server>/<Internetfreigabe>/Sophos Anti-Virus/ESCOSX

smb://<Server>/<Samba-Freigabe>/Sophos Anti-Virus/ESCOSX

afp://<Server>/<Apple-Freigabe>/Sophos Anti-Virus/ESCOSX

Anstatt des Domänen- oder Hostnamens können Sie auch die IP-Adresse oder den NetBIOS-Namen angeben. Die Eingabe der IP-Adresse empfiehlt sich insbesondere bei DNS-Problemen.

Wenn Sophos Anti-Virus über einen in den Systemeinstellungen festgelegten Proxyserver auf die Update-Quelle zugreift, finden Sie unter *Aktivieren von Updates über den Systemproxyserver* (Seite 39) nähere Anweisungen. Wenn Sophos Anti-Virus über einen anderen Proxyserver auf die Update-Quelle zugreifen soll, lesen Sie bitte *Aktivieren von Updates über einen benutzerdefinierten Proxyserver* (Seite 39).

4.2.2 Festlegen einer zweiten Update-Quelle

Wichtig: Wenn Sie in Ihrem Unternehmen Standardeinstellungen festgelegt haben, haben diese möglicherweise Vorrang vor hier vorgenommenen Änderungen.

So legen Sie eine zweite Update-Quelle für Sophos Anti-Virus fest:

1. Wählen Sie **Sophos Anti-Virus** > **Einstellungen** .
2. Klicken Sie auf **AutoUpdate**.
3. Wenn bestimmte Einstellungen nicht hervorgehoben sind, klicken Sie auf das Schlosssymbol und geben Sie einen Administratorennamen und ein Kennwort ein.
4. Wählen Sie **Sekundärserver verwenden**. Ändern Sie die Einstellungen wie folgt:

   - Wenn Sophos Anti-Virus Updates direkt von Sophos beziehen soll, wählen Sie im Einblendmenü **Update vom Sekundärserver** die Option **Sophos** aus. Geben Sie Ihre Sophos Zugangsdaten in die Felder **Benutzername** und **Kennwort** ein.
   - Wenn Sophos Anti-Virus Updates direkt von Ihrem Unternehmens-Webserver beziehen soll, wählen Sie aus dem Einblendmenü **Update vom Sekundärserver** die Option **Unternehmens-Webserver** aus. Geben Sie in das **Adressfeld** die Internetadresse der Update-Quelle an. Geben Sie die Zugangsdaten des Servers in die Felder **Benutzername** und **Kennwort** ein.
   - Wenn Sophos Anti-Virus Updates aus einem Netzwerkvolume beziehen soll, wählen Sie im Einblendmenü **Update vom Sekundärserver** die Option **Netzwerkvolume** aus. Geben Sie in das **Adressfeld** die Netzwerkadresse der Update-Quelle an. Geben Sie in die Felder **Benutzername** und **Kennwort** die Zugangsdaten des Volumes ein.

   Die Adresse lautet etwa wie folgt: Der Text in Klammern muss angepasst werden:

   http://<Server>/<Internetfreigabe>/Sophos Anti-Virus/ESCOSX

   smb://<Server>/<Samba-Freigabe>/Sophos Anti-Virus/ESCOSX

   afp://<Server>/<Apple-Freigabe>/Sophos Anti-Virus/ESCOSX

   Anstatt des Domänen- oder Hostnamens können Sie auch die IP-Adresse oder den NetBIOS-Namen angeben. Die Eingabe der IP-Adresse empfiehlt sich insbesondere bei DNS-Problemen.

Wenn Sophos Anti-Virus über einen in den Systemeinstellungen festgelegten Proxyserver auf die Update-Quelle zugreift, finden Sie unter *Aktivieren von Updates über den Systemproxyserver* (Seite 39) nähere Anweisungen. Wenn Sophos Anti-Virus über einen anderen Proxyserver auf die Update-Quelle zugreifen soll, lesen Sie bitte *Aktivieren von Updates über einen benutzerdefinierten Proxyserver* (Seite 39).

4.2.3 Aktivieren von Updates über den Systemproxyserver

Wichtig: Wenn Sie in Ihrem Unternehmen Standardeinstellungen festgelegt haben, haben diese möglicherweise Vorrang vor hier vorgenommenen Änderungen.

Sie können Sophos Anti-Virus so konfigurieren, dass es Updates über den in den Systemeinstellungen festgelegten Proxyserver bezieht.

So aktivieren Sie Updates über den Systemproxyserver:

1. Wählen Sie **Sophos Anti-Virus** > **Einstellungen** .
2. Klicken Sie auf **AutoUpdate**.
3. Wenn bestimmte Einstellungen nicht hervorgehoben sind, klicken Sie auf das Schlosssymbol und geben Sie einen Administratorennamen und ein Kennwort ein.
4. Wählen Sie die Option **Systemeinstellungen des Proxyservers** aus dem Einblendmenü unter **Primärserver** bzw. **Sekundärserver** (je nach Bedarf) aus.

4.2.4 Aktivieren von Updates über einen benutzerdefinierten Proxyserver

Wichtig: Wenn Sie in Ihrem Unternehmen Standardeinstellungen festgelegt haben, haben diese möglicherweise Vorrang vor hier vorgenommenen Änderungen.

Sie können einen Proxyserver angeben, über den Sophos Anti-Virus upgedatet werden soll.

So aktivieren Sie Updates über einen benutzerdefinierten Proxyserver:

1. Wählen Sie **Sophos Anti-Virus** > **Einstellungen** .
2. Klicken Sie auf **AutoUpdate**.
3. Wenn bestimmte Einstellungen nicht hervorgehoben sind, klicken Sie auf das Schlosssymbol und geben Sie einen Administratorennamen und ein Kennwort ein.
4. Wählen Sie die Option **Kundenspezifische Proxyeinstellungen** aus dem Einblendmenü unter **Primärserver** bzw. **Sekundärserver** (je nach Bedarf) aus.
5. Ein Dialogfeld wird geöffnet. Geben Sie die Adresse und Portzahl des Proxyservers in die **Adressfelder** ein. Geben Sie in die Felder **Benutzername** und **Kennwort** die Zugangsdaten des Proxyservers ein.

4.2.5 Update-Zeitpläne

Wichtig: Wenn Sie in Ihrem Unternehmen Standardeinstellungen festgelegt haben, haben diese möglicherweise Vorrang vor hier vorgenommenen Änderungen.

Sophos Anti-Virus führt standardmäßig ein Update pro Stunde durch. Sie können jedoch den Zeitpunkt und die Häufigkeit von Updates ändern.

So planen Sie Updates:

1. Wählen Sie **Sophos Anti-Virus** > **Einstellungen** .
2. Klicken Sie auf **AutoUpdate**.
3. Wenn bestimmte Einstellungen nicht hervorgehoben sind, klicken Sie auf das Schlosssymbol und geben Sie einen Administratorennamen und ein Kennwort ein.
4. Ändern Sie die Einstellungen wie folgt:
   - Wenn Sophos Anti-Virus in bestimmten Zeitintervallen Updates durchführen soll, wählen Sie **Nach Updates suchen alle** und geben Sie den gewünschten Zeitraum ein.
   - Wenn Sophos Anti-Virus bei jeder Verbindung zum Netzwerk updaten soll, wählen Sie **Bei Verbindung zum Netzwerk oder Internet nach Updates suchen**.

4.2.6 Wiederherstellen der Update-Einstellungen

Sie können die Voreinstellungen für Updates wiederherstellen. Wenn Sie in Ihrem Unternehmen Standard-Update-Einstellungen festgelegt haben, werden diese Einstellungen wiederhergestellt. Andernfalls werden die von Sophos empfohlenen Standardwerte übernommen.

So stellen Sie die Update-Einstellungen wieder her:

1. Wählen Sie **Sophos Anti-Virus** > **Einstellungen** .
2. Klicken Sie auf **AutoUpdate**.
3. Wenn bestimmte Einstellungen nicht hervorgehoben sind, klicken Sie auf das Schlosssymbol und geben Sie einen Administratorennamen und ein Kennwort ein.
4. Klicken Sie auf **Voreinstellungen wiederherstellen**.

4.2.7 Ändern der Protokolleinstellungen

Wichtig: Wenn Sie in Ihrem Unternehmen Standardeinstellungen festgelegt haben, haben diese möglicherweise Vorrang vor hier vorgenommenen Änderungen.

Alle Aktivitäten von On-Access-Scans (einschließlich Threat-Erkennungen) werden im Sophos On-Access-Scan-Protokoll und im Update-Protokoll verzeichnet. Sophos Anti-Virus kann solche Aktivitäten auch im Mac OS X-Systemprotokoll festhalten.

Verfahren Sie wie folgt, um die Protokolleinstellungen von On-Access-Scans und Updates zu ändern:

1. Wählen Sie **Sophos Anti-Virus** > **Einstellungen** .
2. Klicken Sie auf **Protokoll**.
3. Wenn bestimmte Einstellungen nicht hervorgehoben sind, klicken Sie auf das Schlosssymbol und geben Sie einen Administratorennamen und ein Kennwort ein.
4. Ändern Sie die Einstellungen wie folgt:
   - Sie können den Dateinamen und den Speicherort des Protokolls ändern: Klicken Sie auf **Protokolldatei wählen** und geben Sie den neuen Dateinamen bzw. Speicherort ein.
   - Klicken Sie zum Löschen aller Protokolleinträge auf **Protokoll löschen**.

- Aktivieren Sie die Option **Systemprotokoll erstellen**, wenn alle Aktivitäten und Ergebnisse von On-Access-Scans und Updates im Systemprotokoll festgehalten werden sollen.

4.2.8 Wiederherstellen der Protokolleinstellungen

Sie können die Voreinstellungen der Protokolle zu On-Access-Scans und Updates wiederherstellen. Wenn Sie in Ihrem Unternehmen Standardprotokolleinstellungen festgelegt haben, werden diese Einstellungen wiederhergestellt. Andernfalls werden die von Sophos empfohlenen Standardwerte übernommen.

So stellen Sie die Protokolleinstellungen wieder her:

1. Wählen Sie **Sophos Anti-Virus** > **Einstellungen** .
2. Klicken Sie auf **Protokoll**.
3. Wenn bestimmte Einstellungen nicht hervorgehoben sind, klicken Sie auf das Schlosssymbol und geben Sie einen Administratorennamen und ein Kennwort ein.
4. Klicken Sie auf **Voreinstellungen wiederherstellen**.

4.3 Überprüfen des Update-Fortschritts

❖ Ein dynamischer Pfeil beim Sophos Anti-Virus Symbol auf der rechten Seite der Menüleiste weist darauf hin, dass ein Update durchgeführt wird. Sie können jedoch auch auf das Sophos Anti-Virus Symbol rechts in der Menüleiste klicken und **AutoUpdate-Fenster einblenden** aus dem Kurzbefehlmenü auswählen.

Hinweis: Anweisungen zur Anzeige eines Protokolls der gesamten Update-Aktivitäten finden Sie unter *Aufrufen von On-Access-Scan- und Update-Protokollen* (Seite 41).

4.4 Aufrufen von On-Access-Scan- und Update-Protokollen

Verfahren Sie wie folgt, um ein Protokoll aller Aktivitäten von On-Access-Scans (auch erkannte Threats) und Updates aufzurufen:

1. Wählen Sie **Sophos Anti-Virus** > **Einstellungen** .
2. Klicken Sie im **Protokollfenster** auf **Protokoll anzeigen**.

Das Protokoll wird in der Konsole angezeigt. Am Anfang des Protokolleintrags wird jeweils angezeigt, ob es sich um einen Eintrag des On-Access-Scanners (com.sophos.intercheck) oder von AutoUpdate (com.sophos.autoupdate) handelt.

5 Problembehebung

5.1 Keine Updates durch Sophos Anti-Virus

Symptome

Sophos Anti-Virus kann nicht aktualisiert werden oder startet keine Update-Versuche. Wenn Updates nicht möglich sind, erscheint ein weißes Kreuz auf dem Sophos Anti-Virus Symbol im rechten Bereich der Menüleiste.

Ursachen

Das Update-Protokoll kann Aufschluss über die Ursachen geben. (Siehe *Aufrufen von On-Access-Scan- und Update-Protokollen* (Seite 41).)

Problemlösung

- Wenn Sophos Anti-Virus nicht auf die richtige Update-Quelle zugreift, ziehen Sie *Auswahl der Update-Quelle* (Seite 37) zu Rate. Überprüfen Sie die Einstellungen auf ihre Richtigkeit.
- Wenn Sophos Anti-Virus nicht auf Ihren Proxyserver zugreifen kann, finden Sie nähere Anweisungen in den Abschnitten *Aktivieren von Updates über den Systemproxyserver* (Seite 39) und *Aktivieren von Updates über einen benutzerdefinierten Proxyserver* (Seite 39) (je nach Proxyserver). Überprüfen Sie die Einstellungen auf ihre Richtigkeit.
- Wenn Sophos Anti-Virus keine Updates startet, befolgen Sie die Anweisungen im Abschnitt *Update-Zeitpläne* (Seite 39). Überprüfen Sie die Einstellungen auf ihre Richtigkeit.

5.2 Der Menüeintrag "Jetzt aktualisieren" ist nicht hervorgehoben

Symptome

Der Menüeintrag **Jetzt aktualisieren** ist im Menü von **Sophos Anti-Virus**, dem Kurzbefehlmenü der Menüleiste oder dem über das Dock-Symbol aufrufbare Kurzbefehlmenü nicht hinterlegt.

Mögliche Ursachen

Updates wurden nicht konfiguriert.

Problemlösung

Mehr dazu erfahren Sie unter *Konfigurieren der Updates* (Seite 37).

5.3 Graues Schildsymbol von Sophos Anti-Virus

Symptome

Das Sophos Anti-Virus Symbol im rechten Bereich der Menüleiste ist grau.

Ursachen

On-Access-Scans sind deaktiviert.

Problemlösung

Aktivieren Sie On-Access-Scans. Nähere Informationen hierzu finden Sie unter *Aktivieren/Deaktivieren der On-Access-Scans* (Seite 7).

5.4 Die Option zum Scannen mit Sophos Anti-Virus wird nicht angezeigt

Symptome

Sie möchten ein Objekt im Finder scannen, doch im Kontextmenü wird die Option **Mit Sophos Anti-Virus scannen** nicht angezeigt.

Mögliche Ursachen

Der Befehl ist unmittelbar nach der Installation von Sophos Anti-Virus noch nicht vorhanden.

Problemlösung

Melden Sie sich erneut am System an.

5.5 Manuelle Bereinigung erforderlich

Symptome

Im Quarantäne-Manager wird ein Threat angezeigt. Die verfügbare Maßnahme lautet **Manuell bereinigen**.

Ursachen

Folgende Ursachen sind möglich:

- Sophos Anti-Virus verfügt nicht über Threat-Daten zum Bereinigen des Threats.
- Der Threat befindet sich auf einem schreibgeschützten Volume.

Problemlösung

Wenn Sie die Ursache ermittelt haben, verfahren Sie anhand einer der entsprechenden Anweisungen:

- Wenn Sophos Anti-Virus nicht über Threat-Daten zum Bereinigen des Threats verfügt, muss der Threat manuell bereinigt werden:

  1. Fügen Sie einen neuen individuellen Scan der Threats hinzu (entsprechende Anweisungen entnehmen Sie bitte dem Abschnitt *Hinzufügen eines individuellen Scans eines Threats* (Seite 20).
  2. Führen Sie den Scan anhand der Anweisungen im Abschnitt *Ausführen eines individuellen Scans* (Seite 19).

  Wichtig: Durch die Bereinigung werden unter Umständen nicht alle vom Threat vorgenommenen Maßnahmen nicht rückgängig gemacht. Wenn der Threat beispielsweise eine Einstellung modifiziert hat, ist bei der Bereinigung unter Umständen die Originaleinstellung nicht mehr bekannt. Sie müssen möglicherweise die Konfiguration des Macs überprüfen.

- Wenn Sie Schreibzugriff auf das Volume einstellen können:

  1. Bereinigen Sie den Threat aus dem Quarantäne-Manager (entsprechende Anweisungen finden Sie hier: *Löschen eines Threats aus dem Quarantäne-Manager* (Seite 36)).
  2. Scannen Sie erneut nach dem Threat.
  3. Aktivieren Sie den Schreibzugriff auf das Volume.
  4. Bereinigen Sie den Threat im Quarantäne-Manager (entsprechende Anweisungen finden Sie hier: *Verarbeiten von Threats im Quarantäne-Manager* (Seite 34)).

6 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 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.

7 Rechtlicher Hinweis

ACE™, TAO™, CIAO™, and CoSMIC™

and that they waive any claims to copyright or ownership. In addition, submitters acknowledgethat any such submission might become part of the copyright maintained on the overall body of code, which comprises the DOC software. By making a submission, submitter agree to these terms. Furthermore, submitters acknowledge that the incorporation or modification of such submissions is entirely at the discretion of the moderators of the open-source DOC software projects or their designees.

The names ACE, TAO, CIAO, CoSMIC, WashingtonUniversity, UC Irvine, and Vanderbilt University, may not be used to endorse or promote products or services derived from this source without express written permission from Washington University, UC Irvine, or Vanderbilt University. Further, products or services derived from this source may not be called ACE, TAO, CIAO, or CoSMIC nor may the name Washington University, UC Irvine, or Vanderbilt University appear in their names, without express written permission from Washington University, UC Irvine, and Vanderbilt University.

If you have any suggestions, additions, comments, or questions, please let me[21] know.

Douglas C. Schmidt[22]

Quellen

1. http://www.cs.wustl.edu/~schmidt/ACE.html
2. http://www.cs.wustl.edu/~schmidt/TAO.html
3. http://www.dre.vanderbilt.edu/CIAO/
4. http://www.dre.vanderbilt.edu/cosmic/
5. http://www.dre.vanderbilt.edu/~schmidt/
6. http://www.cs.wustl.edu/~schmidt/ACE-members.html
7. http://www.wustl.edu/
8. http://www.uci.edu/
9. http://www.vanderbilt.edu/
10. mailto:doc_group@cs.wustl.edu
11. http://www.cs.wustl.edu/~schmidt/ACE-users.html
12. http://www.cs.wustl.edu/~schmidt/commercial-support.html
13. http://www.cs.wustl.edu/~schmidt/ACE.html
14. http://www.cs.wustl.edu/~schmidt/TAO.html
15. http://www.dre.vanderbilt.edu/CIAO/
16. http://www.dre.vanderbilt.edu/cosmic/
17. http://www.dre.vanderbilt.edu/
18. http://www.isis.vanderbilt.edu/
19. http://www.cs.wustl.edu/~schmidt/doc-center.html
20. http://www.opensource.org/
21. mailto:d.schmidt@vanderbilt.edu
22. http://www.dre.vanderbilt.edu/~schmidt/

Boost

Version 1.0, 17 August 2003

Permission is hereby granted, free of charge, to any person or organization obtaining a copy of the software and accompanying documentation covered by this license (the "Software") to use, reproduce, display, distribute, execute, and transmit the Software, and to prepare derivative

works of the Software, and to permit third-parties to whom the Software is furnished to do so, all subject to the following:

The copyright notices in the Software and this entire statement, including the above license grant, this restriction and the following disclaimer, must be included in all copies of the Software, in whole or in part, and all derivative works of the Software, unless such copies or derivative works are solely in the form of machine-executable object code generated by a source language processor.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR ANYONE DISTRIBUTING THE SOFTWARE BE LIABLE FOR ANY DAMAGES OR OTHER LIABILITY, WHETHER IN CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

dlcompat

Copyright © 2002 Jorge Acereda (jacereda@users.sourceforge.net) & Peter O'Gorman (ogorman@users.sourceforge.net)

Portions may be copyright others, see the Authors section below.

Maintained by Peter O'Gorman (ogorman@users.sourceforge.net)

Bug Reports and other queries should go to ogorman@users.sourceforge.net

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Authors

Original code by Jorge Acereda (jacereda@users.sourceforge.net). This was heavily modified by Peter O'Gorman (ogorman@users.sourceforge.net).

With input from (in alphabetical order):

- Stéphane Conversy (conversy@lri.fr)
- Francis James Franklin (fjf@alinameridon.com)

- Ben Hines (bhines@alumni.ucsd.edu)
- Max Horn (max@quendi.de)
- Karin Kosina (kyrah@sim.no)
- Darin Ohashi (DOhashi@maplesoft.com)
- Benjamin Reed (ranger@befunk.com)

Forgive me if I missed you, and e-mail me (ogorman@users.sourceforge.net) to get added to this list.

dtoa.c

The author of this software is David M. Gay.

Copyright © 1991, 2000 by Lucent Technologies.

Permission to use, copy, modify, and distribute this software for any purpose without fee is hereby granted, provided that this entire notice is included in all copies of any software which is or includes a copy or modification of this software and in all copies of the supporting documentation for such software.

THIS SOFTWARE IS BEING PROVIDED "AS IS", WITHOUT ANY EXPRESS OR IMPLIED WARRANTY. IN PARTICULAR, NEITHER THE AUTHOR NOR LUCENT MAKES ANY REPRESENTATION OR WARRANTY OF ANY KIND CONCERNING THE MERCHANTABILITY OF THIS SOFTWARE OR ITS FITNESS FOR ANY PARTICULAR PURPOSE.

libxml2

Except where otherwise noted in the source code (e.g. the files hash.c, list.c and the trio files, which are covered by a similar licence but with different Copyright notices) all the files are:

Copyright © 1998–2003 Daniel Veillard. All Rights Reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE DANIEL VEILLARD BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of Daniel Veillard shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization from him.

Authors

- Daniel Veillard (daniel@veillard.com)
- Bjorn Reese (breese@users.sourceforge.net)
- William Brack (wbrack@mmm.com.hk)
- Igor Zlatkovic (igor@zlatkovic.com) for the Windows port
- Aleksey Sanin (aleksey@aleksey.com)

OpenSSL cryptographic toolkit

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL license

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

   "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

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

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING

NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay license

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscape's SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"

   The word "cryptographic" can be left out if the routines from the library being used are not cryptographic related :-).
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

   "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License.]

Python

PYTHON SOFTWARE FOUNDATION LICENSE VERSION 2

1. This LICENSE AGREEMENT is between the Python Software Foundation ("PSF"), and the Individual or Organization ("Licensee") accessing and otherwise using this software ("Python") in source or binary form and its associated documentation.
2. Subject to the terms and conditions of this License Agreement, PSF hereby grants Licensee a nonexclusive, royalty-free, worldwide license to reproduce, analyze, test, perform and/or display publicly, prepare derivative works, distribute, and otherwise use Python alone or in any derivative version, provided, however, that PSF's License Agreement and PSF's notice of copyright, i.e., "Copyright © 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009 Python Software Foundation; All Rights Reserved" are retained in Python alone or in any derivative version prepared by Licensee.
3. In the event Licensee prepares a derivative work that is based on or incorporates Python or any part thereof, and wants to make the derivative work available to others as provided herein, then Licensee hereby agrees to include in any such work a brief summary of the changes made to Python.
4. PSF is making Python available to Licensee on an "AS IS" basis. PSF MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED. BY WAY OF EXAMPLE, BUT NOT LIMITATION, PSF MAKES NO AND DISCLAIMS ANY REPRESENTATION OR WARRANTY OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF PYTHON WILL NOT INFRINGE ANY THIRD PARTY RIGHTS.
5. PSF SHALL NOT BE LIABLE TO LICENSEE OR ANY OTHER USERS OF PYTHON FOR ANY INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES OR LOSS AS A RESULT OF MODIFYING, DISTRIBUTING, OR OTHERWISE USING PYTHON, OR ANY DERIVATIVE THEREOF, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.
6. This License Agreement will automatically terminate upon a material breach of its terms and conditions.
7. Nothing in this License Agreement shall be deemed to create any relationship of agency, partnership, or joint venture between PSF and Licensee. This License Agreement does not grant permission to use PSF trademarks or trade name in a trademark sense to endorse or promote products or services of Licensee, or any third party.
8. By copying, installing or otherwise using Python, Licensee agrees to be bound by the terms and conditions of this License Agreement.

Simple ECMAScript Engine

Copyright © 2003, 2004, 2005, 2006, 2007 David Leonard. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of David Leonard nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

strcasestr.c

Copyright © 1990, 1993 The Regents of the University of California. All rights reserved.

This code is derived from software contributed to Berkeley by Chris Torek.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

strnstr.c

Copyright © 2001 Mike Barcroft (mike@FreeBSD.org). Copyright © 1990, 1993 The Regents of the University of California. All rights reserved.

This code is derived from software contributed to Berkeley by Chris Torek.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

UnRAR

The source code of UnRAR utility is freeware. This means:

1. All copyrights to RAR and the utility UnRAR are exclusively owned by the author - Alexander Roshal.
2. The UnRAR sources may be used in any software to handle RAR archives without limitations free of charge, but cannot be used to re-create the RAR compression algorithm, which is proprietary. Distribution of modified UnRAR sources in separate form or as a part of other software is permitted, provided that it is clearly stated in the documentation and source comments that the code may not be used to develop a RAR (WinRAR) compatible archiver.
3. The UnRAR utility may be freely distributed. It is allowed to distribute UnRAR inside of other software packages.
4. THE RAR ARCHIVER AND THE UnRAR UTILITY ARE DISTRIBUTED "AS IS". NO WARRANTY OF ANY KIND IS EXPRESSED OR IMPLIED. YOU USE AT YOUR OWN RISK. THE AUTHOR WILL NOT BE LIABLE FOR DATA LOSS, DAMAGES, LOSS OF PROFITS OR ANY OTHER KIND OF LOSS WHILE USING OR MISUSING THIS SOFTWARE.
5. Installing and using the UnRAR utility signifies acceptance of these terms and conditions of the license.
6. If you don't agree with terms of the license you must remove UnRAR files from your storage devices and cease to use the utility.

Thank you for your interest in RAR and UnRAR.

Alexander L. Roshal

netaddr

Copyright © 2008-2011, David P. D. Moss. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of David P. D. Moss nor the names of contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

License(s) for incorporated software

intset.py - Immutable integer set type

Copyright © 2006, Heiko Wundram.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

- The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.