SOPHOS
Security made simple.

Sophos Anti-Virus für Mac OS X

Für Netzwerke und Einzelplatzrechner unter Mac OS X

Produktversion: 9
Stand: September 2015

Inhalt

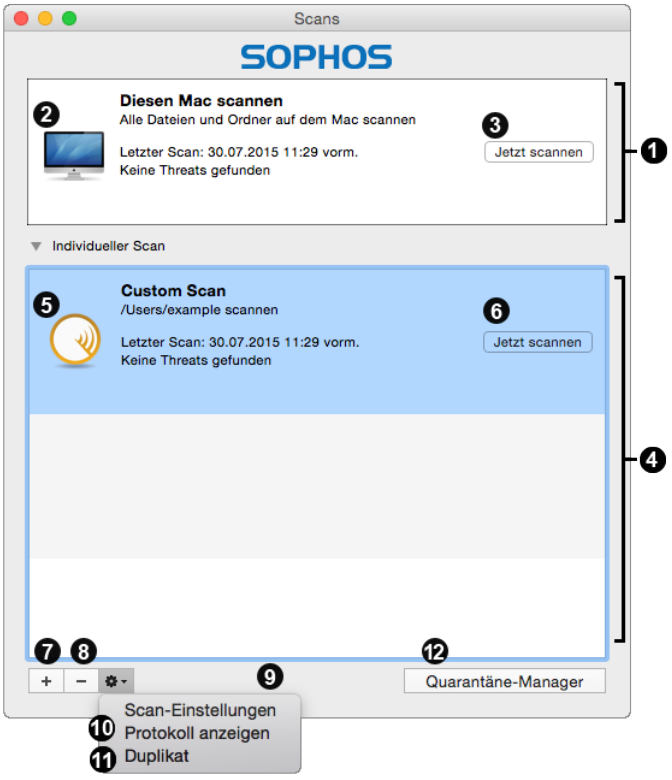
1 Über Sophos Anti-Virus

Sophos Anti-Virus for Mac OS X ist eine Software, die Threats auf Ihrem Mac oder im Netzwerk erkennt und verarbeitet (Viren, Würmer und Trojaner). 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. Weitere Informationen finden Sie unter Scannen von Macs (Seite 16).
2	Doppelklicken Sie darauf, um die Einstellungen aufzurufen. Weitere Informationen finden Sie unter Konfigurieren von Scans (Seite 17).

❸	Klicken Sie darauf, um Ihren Mac zu scannen. Weitere Informationen finden Sie unter Diesen Mac scannen (Seite 17).
❹	Die Liste der von Ihnen hinzugefügten Scans. Weitere 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. Weitere 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. Weitere 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. Weitere 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. Weitere Informationen finden Sie unter Kopieren von individuellen Scans (Seite 20).
⓬	Klicken Sie zum Öffnen des **Quarantäne-Managers** auf die Option **Quarantäne-Manager**. Weitere Informationen finden Sie unter Allgemeine Informationen (Seite 33).

2 Scannen auf Threats

2.1 Informationen zum Scannen auf Threats

Die **On-Access-Scanfunktion** ist der Hauptmechanismus zum Schutz vor Viren und sonstigen Threats. Beim Zugriff auf eine Datei (d.h. Kopieren, Speichern, Verschieben oder Öffnen der Datei) scannt Sophos Anti-Virus die Datei und gewährt nur dann Zugriff auf die Datei, wenn sie keine Bedrohung darstellt. 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-Überprüfungen 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:

- **Diesen Mac scannen**

  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.

  Sie möchten diesen Scan aus einem der folgenden Gründe ausführen: Sie möchten einen von Sophos Anti-Virus erkannten Threat verarbeiten, Sie lassen keinen On-Access-Scan auf diesem Mac laufen, da es sich bei dem Mac um einen Server handelt, oder Sie möchten infizierte Dateien *vor dem Verwenden* auffinden.

  Sie möchten diesen Scan ausführen da Sie einen Threat verarbeiten möchten den Sophos Anti-Virus erkannt hat 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.

  Ein Objekt-Scan im Finder bietet sich an, wenn Sie 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 möchten.

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

On-Access-Scans sind Ihre wichtigste Funktion zum Schutz vor Threats. Beim Zugriff auf eine Datei (d.h. Kopieren, Speichern, Verschieben oder Öffnen der Datei) scannt Sophos Anti-Virus die Datei und gewährt nur dann Zugriff auf die Datei, wenn sie keine Bedrohung darstellt. 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 grau dargestellt sind:, klicken Sie auf das Schloss-Symbol und geben Sie den Namen und das Kennwort eines Administrators ein.
   - Wenn das Schloss-Symbol angezeigt wird, klicken Sie darauf und geben Sie den Namen und das Kennwort eines Administrators ein.
   - Wenn das Manipulationsschutz-Symbol angezeigt wird, klicken Sie darauf und geben Sie das Manipulationsschutz-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 grau.

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 grau dargestellt sind:, klicken Sie auf das Schloss-Symbol und geben Sie den Namen und das Kennwort eines Administrators ein.
   - Wenn das Schloss-Symbol angezeigt wird, klicken Sie darauf und geben Sie den Namen und das Kennwort eines Administrators ein.
   - Wenn das Manipulationsschutz-Symbol angezeigt wird, klicken Sie darauf und geben Sie das Manipulationsschutz-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 grau dargestellt sind:, klicken Sie auf das Schloss-Symbol und geben Sie den Namen und das Kennwort eines Administrators ein.
   - Wenn das Schloss-Symbol angezeigt wird, klicken Sie darauf und geben Sie den Namen und das Kennwort eines Administrators ein.
   - Wenn das Manipulationsschutz-Symbol angezeigt wird, klicken Sie darauf und geben Sie das Manipulationsschutz-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
`/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

Pfad	Ausgeschlossene Objekte
`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 grau dargestellt sind:, klicken Sie auf das Schloss-Symbol und geben Sie den Namen und das Kennwort eines Administrators ein.
   - Wenn das Schloss-Symbol angezeigt wird, klicken Sie darauf und geben Sie den Namen und das Kennwort eines Administrators ein.
   - Wenn das Manipulationsschutz-Symbol angezeigt wird, klicken Sie darauf und geben Sie das Manipulationsschutz-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 grau dargestellt sind:, klicken Sie auf das Schloss-Symbol und geben Sie den Namen und das Kennwort eines Administrators ein.
   - Wenn das Schloss-Symbol angezeigt wird, klicken Sie darauf und geben Sie den Namen und das Kennwort eines Administrators ein.
   - Wenn das Manipulationsschutz-Symbol angezeigt wird, klicken Sie darauf und geben Sie das Manipulationsschutz-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 grau dargestellt sind:, klicken Sie auf das Schloss-Symbol und geben Sie den Namen und das Kennwort eines Administrators ein.
   - Wenn das Schloss-Symbol angezeigt wird, klicken Sie darauf und geben Sie den Namen und das Kennwort eines Administrators ein.
   - Wenn das Manipulationsschutz-Symbol angezeigt wird, klicken Sie darauf und geben Sie das Manipulationsschutz-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.

Wir empfehlen, Threats über den Quarantäne-Manager zu bereinigen (siehe 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 grau dargestellt sind:, klicken Sie auf das Schloss-Symbol und geben Sie den Namen und das Kennwort eines Administrators ein.
   - Wenn das Schloss-Symbol angezeigt wird, klicken Sie darauf und geben Sie den Namen und das Kennwort eines Administrators ein.
   - Wenn das Manipulationsschutz-Symbol angezeigt wird, klicken Sie darauf und geben Sie das Manipulationsschutz-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.

Wir empfehlen, Threats über den Quarantäne-Manager zu bereinigen (siehe 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.

Wichtig: Diese Option sollten Sie nur verwenden, wenn Sie im Supportforum dazu aufgefordert wurden. 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 grau dargestellt sind:, klicken Sie auf das Schloss-Symbol und geben Sie den Namen und das Kennwort eines Administrators ein.
   - Wenn das Schloss-Symbol angezeigt wird, klicken Sie darauf und geben Sie den Namen und das Kennwort eines Administrators ein.
   - Wenn das Manipulationsschutz-Symbol angezeigt wird, klicken Sie darauf und geben Sie das Manipulationsschutz-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.

Wir empfehlen, Threats über den Quarantäne-Manager zu bereinigen (siehe 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.

Wichtig: Diese Option sollten Sie nur verwenden, wenn Sie im Supportforum dazu aufgefordert wurden. 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 grau dargestellt sind:, klicken Sie auf das Schloss-Symbol und geben Sie den Namen und das Kennwort eines Administrators ein.
   - Wenn das Schloss-Symbol angezeigt wird, klicken Sie darauf und geben Sie den Namen und das Kennwort eines Administrators ein.
   - Wenn das Manipulationsschutz-Symbol angezeigt wird, klicken Sie darauf und geben Sie das Manipulationsschutz-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. Wenn dies nicht der Fall ist, werden die von Sophos empfohlenen Voreinstellungen übernommen.

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

So können Sie die von Sophos empfohlenen Standardeinstellungen für On-Access-Scans wiederherstellen:

1. Wählen Sie **Sophos Anti-Virus** > **Einstellungen**.
2. Klicken Sie auf **On-Access-Scans**.
3. Wenn bestimmte Einstellungen grau dargestellt sind:, klicken Sie auf das Schloss-Symbol und geben Sie den Namen und das Kennwort eines Administrators ein.
   - Wenn das Schloss-Symbol angezeigt wird, klicken Sie darauf und geben Sie den Namen und das Kennwort eines Administrators ein.
   - Wenn das Manipulationsschutz-Symbol angezeigt wird, klicken Sie darauf und geben Sie das Manipulationsschutz-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 grau dargestellt sind:, klicken Sie auf das Schloss-Symbol und geben Sie den Namen und das Kennwort eines Administrators ein.
   - Wenn das Schloss-Symbol angezeigt wird, klicken Sie darauf und geben Sie den Namen und das Kennwort eines Administrators ein.
   - Wenn das Manipulationsschutz-Symbol angezeigt wird, klicken Sie darauf und geben Sie das Manipulationsschutz-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:

So können Sie die von Sophos empfohlenen Standardeinstellungen für Alerts wiederherstellen:

1. Wählen Sie **Sophos Anti-Virus** > **Einstellungen**.
2. Klicken Sie auf **Benachrichtigung**.
3. Wenn bestimmte Einstellungen grau dargestellt sind:, klicken Sie auf das Schloss-Symbol und geben Sie den Namen und das Kennwort eines Administrators ein.
   - Wenn das Schloss-Symbol angezeigt wird, klicken Sie darauf und geben Sie den Namen und das Kennwort eines Administrators ein.
   - Wenn das Manipulationsschutz-Symbol angezeigt wird, klicken Sie darauf und geben Sie das Manipulationsschutz-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 grau dargestellt sind:, klicken Sie auf das Schloss-Symbol und geben Sie den Namen und das Kennwort eines Administrators ein.
   - Wenn das Schloss-Symbol angezeigt wird, klicken Sie darauf und geben Sie den Namen und das Kennwort eines Administrators ein.
   - Wenn das Manipulationsschutz-Symbol angezeigt wird, klicken Sie darauf und geben Sie das Manipulationsschutz-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. Wenn dies nicht der Fall ist, werden die von Sophos empfohlenen Voreinstellungen übernommen.

So stellen Sie die Protokolleinstellungen wieder her:

So können Sie die von Sophos empfohlenen Standardeinstellungen für Protokolle wiederherstellen:

1. Wählen Sie **Sophos Anti-Virus** > **Einstellungen**.
2. Klicken Sie auf **Protokoll**.
3. Wenn bestimmte Einstellungen grau dargestellt sind:, klicken Sie auf das Schloss-Symbol und geben Sie den Namen und das Kennwort eines Administrators ein.
   - Wenn das Schloss-Symbol angezeigt wird, klicken Sie darauf und geben Sie den Namen und das Kennwort eines Administrators ein.
   - Wenn das Manipulationsschutz-Symbol angezeigt wird, klicken Sie darauf und geben Sie das Manipulationsschutz-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 von Macs

Sie können jederzeit einen Scan Ihres Mac starten. Dabei werden alle Dateien gescannt, zu denen Sie auf lokalen Laufwerken Zugang haben. Wenn Sie sich als Administrator authentifizieren, werden auch Dateien gescannt, auf die Sie nicht zugreifen können. Hierzu zählen auch angeschlossene Wechselmedien.

Sie möchten aus einem der folgenden Gründe scannen: Sie wollen infizierte Objekte bearbeiten, die von Sophos Anti-Virus gefunden wurden, Sie lassen keinen On-Access-Scan auf Ihrem Mac laufen, weil es sich um einen Server handelt oder Sie wollen infizierte Dateien vor dem Verwenden auffinden.

Sie möchten Scannen, weil Sie ein infiziertes Objekt bearbeiten wollen, das von Sophos Anti-Virus gefunden wurde oder Sie möchten infizierte Dateien *vor dem Verwenden* auffinden.

2.3.1 Diesen Mac scannen

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** > **Diesen Mac scannen**.

  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 **Jetzt scannen** auf die Wiedergabeschaltfläche.
- Klicken Sie auf das Sophos Anti-Virus Symbol auf der rechten Seite der Menüleiste und wählen Sie anschließend die Option **Jetzt 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 **Diesen Mac scannen** aus.

2.3.2 Konfigurieren von Scans

2.3.2.1 Scannen in Archiven und komprimierten Dateien deaktivieren

Das Scannen in Archiven und komprimierten Dateien bei ist standardmäßig auf Ihrem Mac aktiviert.

So deaktivieren Sie das Scannen in Archiven und komprimierten Dateien:

1. Doppelklicken Sie im Fenster **Scans** auf das Feld **Diesen Mac scannen**.
2. Wählen Sie **Optionen**.
3. Deaktivieren Sie **In Archiven und komprimierten Dateien scannen**.

2.3.2.2 Konfigurieren von Objekt-Scans zum automatischen Bereinigen von Threats

Wir empfehlen, Threats über den Quarantäne-Manager zu bereinigen (siehe 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. Doppelklicken Sie im Fenster **Scans** auf das Feld **Diesen Mac scannen**.
2. Wählen Sie **Optionen**.
3. Wählen Sie die Option **Threat bereinigen** aus dem Einblendmenü **Bei Erkennung eines Threats** aus.
4. 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 von Objekt-Scans zum automatischen Verschieben von Threats

Wir empfehlen, Threats über den Quarantäne-Manager zu bereinigen (siehe Vorgehensweise bei Threaterkennung (Seite 33)). Sie können 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.

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.

Wichtig: Diese Option sollten Sie nur verwenden, wenn Sie im Supportforum dazu aufgefordert wurden. 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. Doppelklicken Sie im Fenster **Scans** auf das Feld **Diesen Mac scannen**.
2. Wählen Sie **Optionen**.
3. Wählen Sie 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 Scan-Protokoll werden alle Maßnahmen, die Sophos Anti-Virus bei infizierten Objekten vorgenommen hat, festgehalten.

2.3.2.4 Konfigurieren von Objekt-Scans zum automatischen Löschen von Threats

Wir empfehlen, Threats über den Quarantäne-Manager zu bereinigen (siehe Vorgehensweise bei Threaterkennung (Seite 33)). Sie können 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.

Wichtig: Diese Option sollten Sie nur verwenden, wenn Sie im Supportforum dazu aufgefordert wurden. Sophos Anti-Virus fordert den Benutzer vor dem Löschen eines Threats nicht zur Bestätigung auf.

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

1. Doppelklicken Sie im Fenster **Scans** auf das Feld **Diesen Mac scannen**.
2. Wählen Sie **Optionen**.
3. Wählen Sie im Feld **Diesen Mac scannen** die Option **Threat löschen** aus dem Einblendmenü **Bei Erkennung eines Threats** aus.

Im Scan-Protokoll 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.

2.3.3 Anzeigen des Scan-Protokolls

- Wählen Sie **ScanProtokoll 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 21) 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 24).

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 21) 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 24).

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 „Command-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.
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

Scannen in Archiven und komprimierten Dateien ist standardmäßig aktiviert.

Gehen Sie zum Deaktivieren des Scannens in Archiven und komprimierten Dateien bei individuellen Scans wie folgt vor:

1. Öffnen Sie den Scaneditor, falls dieser nicht geöffnet ist. Anweisungen zur Vorgehensweise 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

Wir empfehlen, Threats über den Quarantäne-Manager zu bereinigen (siehe 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

Wir empfehlen, Threats über den Quarantäne-Manager zu bereinigen (siehe 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.

Wichtig: Diese Option sollten Sie nur verwenden, wenn Sie im Supportforum dazu aufgefordert wurden. 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, falls dieser nicht geöffnet ist. Anweisungen zur Vorgehensweise 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

Wir empfehlen, Threats über den Quarantäne-Manager zu bereinigen (siehe 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.

Wichtig: Diese Option sollten Sie nur verwenden, wenn Sie im Supportforum dazu aufgefordert wurden. 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, falls dieser nicht geöffnet ist. Anweisungen zur Vorgehensweise 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 **Delete** (-).

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 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, benutzerinitiierte Scans, 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 grau dargestellt sind:, klicken Sie auf das Schloss-Symbol und geben Sie den Namen und das Kennwort eines Administrators ein.
   - Wenn das Schloss-Symbol angezeigt wird, klicken Sie darauf und geben Sie den Namen und das Kennwort eines Administrators ein.
   - Wenn das Manipulationsschutz-Symbol angezeigt wird, klicken Sie darauf und geben Sie das Manipulationsschutz-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.

   Hinweis: Sie können mehr als eine Absenderadresse verwenden, indem Sie sie mit Kommas voneinander trennen.

2.6 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:

So können Sie die von Sophos empfohlenen Standardeinstellungen für Alerts wiederherstellen:

1. Wählen Sie **Sophos Anti-Virus** > **Einstellungen**.
2. Klicken Sie auf **Benachrichtigung**.
3. Wenn bestimmte Einstellungen grau dargestellt sind:, klicken Sie auf das Schloss-Symbol und geben Sie den Namen und das Kennwort eines Administrators ein.
   - Wenn das Schloss-Symbol angezeigt wird, klicken Sie darauf und geben Sie den Namen und das Kennwort eines Administrators ein.
   - Wenn das Manipulationsschutz-Symbol angezeigt wird, klicken Sie darauf und geben Sie das Manipulationsschutz-Kennwort ein.
4. Klicken Sie auf **Voreinstellungen wiederherstellen**.

2.7 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 **Live-Schutz**.
3. Wenn bestimmte Einstellungen grau dargestellt sind:, klicken Sie auf das Schloss-Symbol und geben Sie den Namen und das Kennwort eines Administrators ein.
   - Wenn das Schloss-Symbol angezeigt wird, klicken Sie darauf und geben Sie den Namen und das Kennwort eines Administrators ein.

- Wenn das Manipulationsschutz-Symbol angezeigt wird, klicken Sie darauf und geben Sie das Manipulationsschutz-Kennwort ein.

4. Stellen Sie den Schalter auf "**Ein**", um den Live-Schutz zu aktivieren.

2.8 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:

So stellen Sie die von Sophos empfohlene Standardeinstellung des Live-Schutzes wieder her:

1. Wählen Sie **Sophos Anti-Virus** > **Einstellungen**.
2. Klicken Sie auf **Live-Schutz**.
3. Wenn bestimmte Einstellungen grau dargestellt sind:, klicken Sie auf das Schloss-Symbol und geben Sie den Namen und das Kennwort eines Administrators ein.
   - Wenn das Schloss-Symbol angezeigt wird, klicken Sie darauf und geben Sie den Namen und das Kennwort eines Administrators ein.
   - Wenn das Manipulationsschutz-Symbol angezeigt wird, klicken Sie darauf und geben Sie das Manipulationsschutz-Kennwort ein.
4. Klicken Sie auf **Voreinstellungen wiederherstellen**.

2.9 Web-Schutz

Der Web-Schutz von Sophos bietet besseren Schutz vor Threats aus dem Internet. Die Komponente basiert auf einem Abgleich mit den URLs in der Datenbank infizierter Websites von Sophos. Websites, auf denen bekanntermaßen Malware gehostet wird, werden gesperrt.

2.9.1 Unterstützte Browser

Der Web-Schutz wird von folgenden Browsern unterstützt:

- Firefox
- Google Chrome
- Safari
- Opera
- OmniWeb
- Camino
- Cruz
- curl
- wget

2.9.2 Allgemeine Einstellungen

Web-Schutz kann so konfiguriert werden, dass entweder der Zugang zu bösartigen Websites blockiert wird oder Downloads gescannt werden, um gegen bösartige Inhalte zu schützen oder beides. Um Web-Schutz zu konfigurieren:

1. Wählen Sie **Sophos Anti-Virus** > **Einstellungen**.
2. Wählen Sie **Web-Schutz**.
3. Klicken Sie auf **Allgemein** im Bereich **Web-Schutz**.
4. Wenn bestimmte Einstellungen grau dargestellt sind:, klicken Sie auf das Schloss-Symbol und geben Sie den Namen und das Kennwort eines Administrators ein.
   - Wenn das Schloss-Symbol angezeigt wird, klicken Sie darauf und geben Sie den Namen und das Kennwort eines Administrators ein.
   - Wenn das Manipulationsschutz-Symbol angezeigt wird, klicken Sie darauf und geben Sie das Manipulationsschutz-Kennwort ein.
5. Stellen Sie den oberen Schalter auf **Ein**, um Ihren Mac vor Sites zu schützen, die Sophos identifiziert hat, schadhafte Inhalte zu verbreiten.
6. Stellen Sie den unteren Schalter auf **Ein**, um schadhafte Downloads zu blockieren, bevor sie Ihren Browser erreichen. Dadurch wird eine zusätzliche Prüfung ausgeführt bei der Downloads durch einen Rechner, der Inhalte scannt, geprüft werden.

2.9.3 Zugelassene Websites

Möglicherweise möchten Sie bestimmte Websites vom Web-Schutz ausschließen. Sie können den Domänennamen hinzufügen, um das Web-Schutz-Filtern einer ganzen Domäne zu umgehen. Sie können auch eine IPv4-Adresse hinzufügen, um das Web-Schutz-Filtern für diese Adresse zum umgehen. Um eine erlaubte Website hinzuzufügen gehen Sie wie folgt vor:

1. Wählen Sie **Sophos Anti-Virus** > **Einstellungen**.
2. Wählen Sie **Web-Schutz**.
3. Klicken Sie auf **Erlaubte Websites** im Feld **Web-Schutz**.
4. Wenn bestimmte Einstellungen grau dargestellt sind:, klicken Sie auf das Schloss-Symbol und geben Sie den Namen und das Kennwort eines Administrators ein.
   - Wenn das Schloss-Symbol angezeigt wird, klicken Sie darauf und geben Sie den Namen und das Kennwort eines Administrators ein.
   - Wenn das Manipulationsschutz-Symbol angezeigt wird, klicken Sie darauf und geben Sie das Manipulationsschutz-Kennwort ein.

5. Klicken Sie auf die Schaltfläche **+**, um die Site hinzuzufügen, die vom Web-Schutz ausgeschlossen werden soll. Geben Sie den Domänennamen, die IP-Adresse oder den IP-Adressbereich der Site in CIDR-Notation ein, die Sie vom Web-Schutz ausschließen wollen. Sie können keinen spezifischen Pfad eingeben.

   Beispiele gültiger erlaubter Websites:

   - **`example.com`** erlaubt alle zur **`example.com`**-Domäne gehörigen Websites.
   - **`address.example.com`** erlaubt alle zu **`address.example.com`** oder **`this.address.example.com`** zugehörigen Websites, nicht aber zu **`different.example.com`**.
   - **`192.0.2.0`** erlaubt nur **`192.0.2.0`**.
   - **`192.0.2.0/24`** erlaubt alle Adressen von **`192.0.2.0`** bis **`192.0.2.255`**.

   Hinweis: Lokale Adressen sind automatisch in der Liste der erlaubten Websites enthalten.

2.10 Device Control

Device Control erkennt und blockiert bestimmte überwachte Geräte, die für eine Büroumgebung ungeeignet sind. Konfigurieren von Device Control:

1. Wählen Sie **Sophos Anti-VirusEinstellungen**.
2. Klicken Sie auf **Device Control**.
3. Wenn bestimmte Einstellungen grau dargestellt sind:
   - Wenn das Schloss-Symbol angezeigt wird, klicken Sie darauf und geben Sie den Namen und das Kennwort eines Administrators ein.
   - Wenn das Manipulationsschutz-Symbol angezeigt wird, klicken Sie darauf und geben Sie das Manipulationsschutz-Kennwort ein.
4. Stellen Sie den Schalter auf "**Ein**", um Device Control zu aktivieren.

2.11 Wiederherstellen der Standardeinstellungen von Device Control

Sie können die Standardeinstellungen von Device Control wiederherstellen. Wenn Ihre Organisation Standardeinstellungen von Device Control vorgenommen hat, werden diese verwendet. Andernfalls werden die von Sophos empfohlenen Standardwerte übernommen.

So stellen Sie die Standardeinstellungen von Device Control wieder her:

1. Wählen Sie **Sophos Anti-VirusEinstellungen**.
2. Klicken Sie auf **Device Control**.
3. Wenn bestimmte Einstellungen grau dargestellt sind:
   - Wenn das Schloss-Symbol angezeigt wird, klicken Sie darauf und geben Sie den Namen und das Kennwort eines Administrators ein.
   - Wenn das Manipulationsschutz-Symbol angezeigt wird, klicken Sie darauf und geben Sie das Manipulationsschutz-Kennwort ein.
4. Klicken Sie auf **Voreinstellungen wiederherstellen**.

2.12 Benutzen von Sophos Anti-Virus mit 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.
   Öffnen Sie hierzu `/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 von Sophos Anti-Virus aufgeführt. Öffnen Sie den Quarantäne-Manager und verarbeiten Sie den Threat dort.

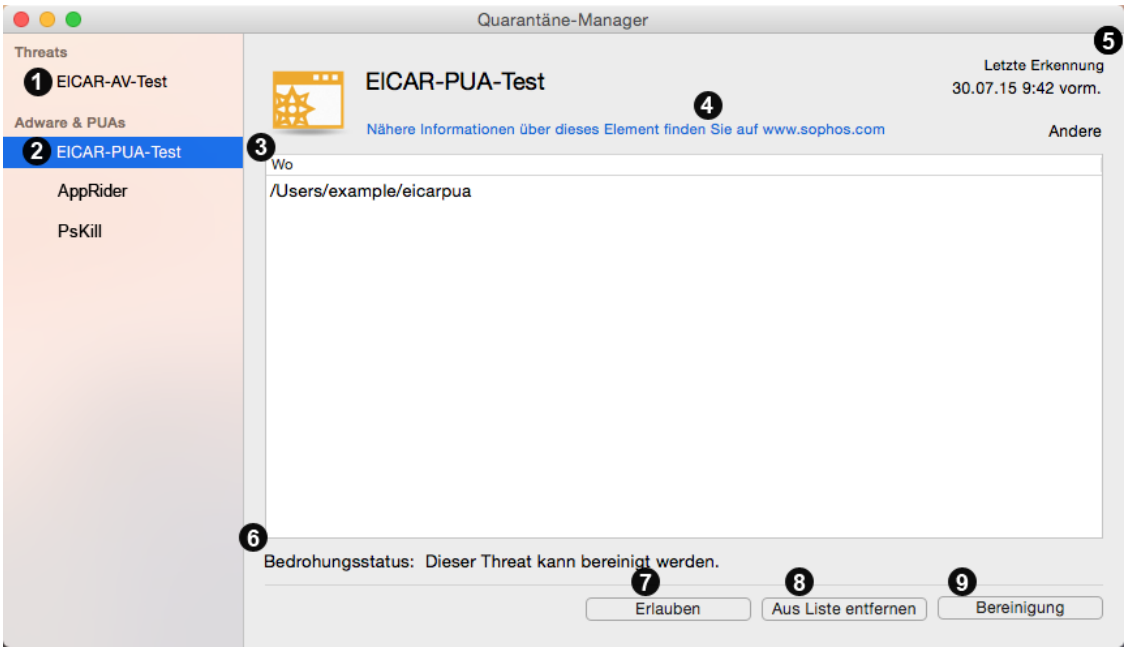
3.1 Öffnen des Quarantäne-Managers

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 Allgemeine Informationen

Im Quarantäne-Manager werden alle beim Scan erkannten Threats, Adware und potenziell unerwünschte Anwendungen (PUAs) aufgeführt, so dass Sie sie verarbeiten können. Die Bestandteile des **Quarantäne-Manager**-Fensters werden unten angezeigt:



1	Eine Liste aller erkannten Threats. Wählen Sie ein Objekt aus, um zusätzliche Informationen und Optionen anzuzeigen.

❷	Die Liste der erkannten Adware und PUAs. Wählen Sie ein Objekt aus, um zusätzliche Informationen und Optionen anzuzeigen.
❸	Eine Liste der Dateipfade, in denen der ausgewählte Threat bzw. die ausgewählte Adware oder PUA erkannt wurde. Fahren Sie mit der Maus über den Dateipfad, um den Finder an dem Speicherort zu öffnen, mit dem das ausgewählte Objekt in Verbindung steht. Klicken Sie auf den Pfeil, der rechts neben dem Dateipfad angezeigt wird.
❹	Ein Link zu detaillierten Informationen über das ausgewählte Objekt auf der Sophos Website.
❺	Datum und Uhrzeit der Erkennung. Wenn ein Threat mehrmals erkannt wurde, wird hier nur die neueste Erkennung aufgeführt.
❻	Die zur Verfügung stehenden Maßnahmen sowie ggf. eine Zusammenfassung aller bisher ergriffenen Maßnahmen.
❼	Wenn Sie eine Anwendung ausführen möchten, diese jedoch als Adware oder PUA erkannt wird, fügen Sie sie in den Einstellungen zur Autorisierungsliste hinzu. Für Threats ist diese Option nicht verfügbar.
❽	Klicken Sie auf „**Aus der Liste entfernen**“, um einen ausgewählten Threat bzw. eine ausgewählte Adware oder PUA aus dem Quarantäne-Manager zu entfernen, ohne den Threat selbst zu verarbeiten. Halten Sie beim Klicken die Wahltaste gedrückt, um die gesamte Liste zu entfernen. Weitere Informationen finden Sie unter Löschen von Threats, Adware oder potenziell unerwünschten Anwendungen (PUAs) aus dem Quarantäne-Manager (Seite 36).
❾	Klicken Sie auf **Bereinigung**, um einen ausgewählten Threat, eine Adware oder PUA zu bereinigen. Weitere Informationen finden Sie unter Verarbeiten von Threats im Quarantäne-Manager (Seite 35).

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 Allgemeine Informationen (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 **Kopieren der Dateipfade** im Einblendmenü aus.

3.4 Verarbeiten von Threats im Quarantäne-Manager

1. Wählen Sie einen Threat, eine Adware oder potenziell unerwünschte Anwendung aus, bei der die Maßnahme „**Bereinigen**“ lautet.
2. Klicken Sie auf **Bereinigung**.

   Bereinigte Objekte werden aus der Liste gelöscht.

3. Wenn die Maßnahme für bestimmte Threats **Neu starten** lautet, wird die Bereinigung erst nach einem Neustart des Macs abgeschlossen.
4. Wenn Threats vorhanden sind, bei denen die Maßnahme **Diesen Mac scannen** verfügbar ist, scannen Sie die lokalen Laufwerke (Details hierzu finden Sie unter Diesen Mac scannen (Seite 17)).
5. Wenn Threats vorhanden sind, bei denen die Maßnahme **Bereinigen** lautet, gehen Sie wieder zu Schritt 1 zurück.
6. 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 wie in Ausführen eines individuellen Scans (Seite 19) beschrieben aus.

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 grau dargestellt sind:, klicken Sie auf das Schloss-Symbol und geben Sie den Namen und das Kennwort eines Administrators ein.

   - Wenn das Schloss-Symbol angezeigt wird, klicken Sie darauf und geben Sie den Namen und das Kennwort eines Administrators ein.
   - Wenn das Manipulationsschutz-Symbol angezeigt wird, klicken Sie darauf und geben Sie das Manipulationsschutz-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 von Threats, Adware oder potenziell unerwünschten Anwendungen (PUAs) aus dem Quarantäne-Manager

Sie möchten ein Objekt möglicherweise aus folgenden Gründen löschen:

- Es wurde als falsche Erkennung bestätigt
- 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 ein Objekt aus dem Quarantäne-Manager:

1. Wählen Sie im Quarantäne-Manager den Threat aus, den Sie löschen möchten.
2. Klicken Sie auf „**Aus Liste entfernen**“.
   Um alle Objekte aus der Liste zu entfernen, halten Sie beim Klicken die Wahltaste gedrückt.

Dadurch werden keine Dateien gelöscht.

4 Update

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

Die Home Edition von Sophos Anti-Virus für Mac wird werksseitig zum Updaten von Sophos konfiguriert. Daher ist der Optionsumfang begrenzt.

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 grau dargestellt sind:, klicken Sie auf das Schloss-Symbol und geben Sie den Namen und das Kennwort eines Administrators ein.
   - Wenn das Schloss-Symbol angezeigt wird, klicken Sie darauf und geben Sie den Namen und das Kennwort eines Administrators ein.
   - Wenn das Manipulationsschutz-Symbol angezeigt wird, klicken Sie darauf und geben Sie das Manipulationsschutz-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 grau dargestellt sind:, klicken Sie auf das Schloss-Symbol und geben Sie den Namen und das Kennwort eines Administrators ein.
   - Wenn das Schloss-Symbol angezeigt wird, klicken Sie darauf und geben Sie den Namen und das Kennwort eines Administrators ein.
   - Wenn das Manipulationsschutz-Symbol angezeigt wird, klicken Sie darauf und geben Sie das Manipulationsschutz-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 grau dargestellt sind:, klicken Sie auf das Schloss-Symbol und geben Sie den Namen und das Kennwort eines Administrators ein.
   - Wenn das Schloss-Symbol angezeigt wird, klicken Sie darauf und geben Sie den Namen und das Kennwort eines Administrators ein.
   - Wenn das Manipulationsschutz-Symbol angezeigt wird, klicken Sie darauf und geben Sie das Manipulationsschutz-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 grau dargestellt sind:, klicken Sie auf das Schloss-Symbol und geben Sie den Namen und das Kennwort eines Administrators ein.
   - Wenn das Schloss-Symbol angezeigt wird, klicken Sie darauf und geben Sie den Namen und das Kennwort eines Administrators ein.
   - Wenn das Manipulationsschutz-Symbol angezeigt wird, klicken Sie darauf und geben Sie das Manipulationsschutz-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 grau dargestellt sind:, klicken Sie auf das Schloss-Symbol und geben Sie den Namen und das Kennwort eines Administrators ein.
   - Wenn das Schloss-Symbol angezeigt wird, klicken Sie darauf und geben Sie den Namen und das Kennwort eines Administrators ein.
   - Wenn das Manipulationsschutz-Symbol angezeigt wird, klicken Sie darauf und geben Sie das Manipulationsschutz-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 mit dem Netzwerk ein Update durchführen soll, wählen Sie **Suche nach Updates bei Verbindung zum Netzwerk oder Internet**.

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:

So können Sie die von Sophos empfohlenen Standardeinstellungen für Updates wiederherstellen:

1. Wählen Sie **Sophos Anti-Virus** > **Einstellungen**.
2. Klicken Sie auf **AutoUpdate**.

3. Wenn bestimmte Einstellungen grau dargestellt sind:, klicken Sie auf das Schloss-Symbol und geben Sie den Namen und das Kennwort eines Administrators ein.
   - Wenn das Schloss-Symbol angezeigt wird, klicken Sie darauf und geben Sie den Namen und das Kennwort eines Administrators ein.
   - Wenn das Manipulationsschutz-Symbol angezeigt wird, klicken Sie darauf und geben Sie das Manipulationsschutz-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 grau dargestellt sind:, klicken Sie auf das Schloss-Symbol und geben Sie den Namen und das Kennwort eines Administrators ein.
   - Wenn das Schloss-Symbol angezeigt wird, klicken Sie darauf und geben Sie den Namen und das Kennwort eines Administrators ein.
   - Wenn das Manipulationsschutz-Symbol angezeigt wird, klicken Sie darauf und geben Sie das Manipulationsschutz-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. Wenn dies nicht der Fall ist, werden die von Sophos empfohlenen Voreinstellungen übernommen.

So stellen Sie die Protokolleinstellungen wieder her:

So können Sie die von Sophos empfohlenen Standardeinstellungen für Protokolle wiederherstellen:

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

2. Klicken Sie auf **Protokoll**.
3. Wenn bestimmte Einstellungen grau dargestellt sind:, klicken Sie auf das Schloss-Symbol und geben Sie den Namen und das Kennwort eines Administrators ein.
   - Wenn das Schloss-Symbol angezeigt wird, klicken Sie darauf und geben Sie den Namen und das Kennwort eines Administrators ein.
   - Wenn das Manipulationsschutz-Symbol angezeigt wird, klicken Sie darauf und geben Sie das Manipulationsschutz-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 16).

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 Kreuz auf dem Sophos Anti-Virus Symbol im rechten Bereich der Menüleiste.

Mögliche Ursachen

Das Update-Protokoll kann Aufschluss über die Ursachen geben. Weitere Informationen finden Sie unter Aufrufen von On-Access-Scan- und Update-Protokollen (Seite 16).

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 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 40). 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

Siehe 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.

Mögliche 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**.

Mögliche 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 wie in Ausführen eines individuellen Scans (Seite 19) beschrieben aus.

  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. Löschen Sie den Threat aus dem Quarantäne-Manager (siehe Löschen von Threats, Adware oder potenziell unerwünschten Anwendungen (PUAs) 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 35)).

6 Technischer Support

Technischen Support zu Sophos Produkten können Sie wie folgt abrufen:

- Rufen Sie das SophosTalk-Forum unter community.sophos.com/ auf und suchen Sie nach Benutzern mit dem gleichen Problem.
- Durchsuchen Sie die Support-Knowledgebase unter www.sophos.com/de-de/support.aspx.
- Begleitmaterial zu den Produkten finden Sie hier: www.sophos.com/de-de/support/documentation/.
- 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

Copyright © 2014 Sophos Limited. Alle Rechte vorbehalten. Diese Publikation darf weder elektronisch oder mechanisch reproduziert, elektronisch gespeichert oder übertragen, noch fotokopiert oder aufgenommen werden, es sei denn, Sie verfügen entweder über eine gültige Lizenz, gemäß der die Dokumentation in Übereinstimmung mit dem Lizenzvertrag reproduziert werden darf, oder Sie verfügen über eine schriftliche Genehmigung des Urheberrechtsinhabers.

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

ACE™, TAO™, CIAO™, and CoSMIC™

ACE[1], TAO[2], CIAO[3], and CoSMIC[4] (henceforth referred to as “DOC software”) are copyrighted by Douglas C. Schmidt[5] and his research group[6] at Washington University[7], University of California[8], Irvine, and Vanderbilt University[9], Copyright © 1993–2005, all rights reserved.

Since DOC software is open-source10, free software, you are free to use, modify, copy, and distribute–perpetually and irrevocably–the DOC software source code and object code produced from the source, as well as copy and distribute modified versions of this software. You must, however, include this copyright statement along with code built using DOC software.

You can use DOC software in commercial and/or binary software releases and are under no obligation to redistribute any of your source code that is built using DOC software. Note, however, that you may not do anything to the DOC software code, such as copyrighting it yourself or claiming authorship of the DOC software code, that will prevent DOC software from being distributed freely using an open-source development model. You needn’t inform anyone that you’re using DOC software in your software, though we encourage you to let us[10] know so we can promote your project in the DOC software success stories[11].

DOC software is provided as is with no warranties of any kind, including the warranties of design, merchantability, and fitness for a particular purpose, noninfringement, or arising from a course of dealing, usage or trade practice. Moreover, DOC software is provided with no support and without any obligation on the part of Washington University, UC Irvine, Vanderbilt University, their employees, or students to assist in its use, correction, modification, or enhancement. A number of companies[12] around the world provide commercial support for DOC software, however. DOC software is Y2K-compliant, as long as the underlying OS platform is Y2K-compliant.

Washington University, UC Irvine, Vanderbilt University, their employees, and students shall have no liability with respect to the infringement of copyrights, trade secrets or any patents by DOC software or any part thereof. Moreover, in no event will Washington University, UC Irvine, or Vanderbilt University, their employees, or students be liable for any lost revenue or profits or other special, indirect and consequential damages.

The ACE[13], TAO[14], CIAO[15], and CoSMIC[16] web sites are maintained by the DOC Group[17] at the Institute for Software Integrated Systems (ISIS)[18] and the Center for Distributed Object Computing of Washington University, St. Louis[19] for the development of open-source software as part of the open-source software community[20]. By submitting comments, suggestions, code, code snippets, techniques (including that of usage), and algorithms, submitters acknowledge that they have the right to do so, that any such submissions are given freely and unreservedly, 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

http://www.cs.wustl.edu/~schmidt/ACE.html

http://www.cs.wustl.edu/~schmidt/TAO.html

http://www.dre.vanderbilt.edu/CIAO/

http://www.dre.vanderbilt.edu/cosmic/

http://www.dre.vanderbilt.edu/~schmidt/

http://www.cs.wustl.edu/~schmidt/ACE-members.html

http://www.wustl.edu/

http://www.uci.edu/

http://www.vanderbilt.edu/

mailto:doc_group@cs.wustl.edu

http://www.cs.wustl.edu/~schmidt/ACE-users.html

http://www.cs.wustl.edu/~schmidt/commercial-support.html

http://www.cs.wustl.edu/~schmidt/ACE.html

http://www.cs.wustl.edu/~schmidt/TAO.html

http://www.dre.vanderbilt.edu/CIAO/

http://www.dre.vanderbilt.edu/cosmic/

http://www.dre.vanderbilt.edu/

http://www.isis.vanderbilt.edu/

http://www.cs.wustl.edu/~schmidt/doc-center.html

http://www.opensource.org/

mailto:d.schmidt@vanderbilt.edu

http://www.dre.vanderbilt.edu/~schmidt/

Apache

The Sophos software that is described in this document may include some software programs that are licensed (or sublicensed) to the user under the Apache License. A copy of the license agreement for any such included software can be found at http://www.apache.org/licenses/LICENSE-2.0.

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.

Common Public License

The Sophos software that is described in this document includes or may include some software programs that are licensed (or sublicensed) to the user under the Common Public License (CPL), which, among other rights, permits the user to have access to the source code. The CPL requires for any software licensed under the terms of the CPL, which is distributed in object code form, that the source code for such software also be made available to the users of the object code form. For any such software covered under the CPL, the source code is available via mail order by submitting a request to Sophos; via email to support@sophos.de or via the web at http://www.sophos.com/de-de/support/contact-support/contact-information.aspx. A copy of the license agreement for any such included software can be found at http://opensource.org/licenses/cpl1.0.php

ConvertUTF

Copyright 2001–2004 Unicode, Inc.

This source code is provided as is by Unicode, Inc. No claims are made as to fitness for any particular purpose. No warranties of any kind are expressed or implied. The recipient agrees to determine applicability of information provided. If this file has been purchased on magnetic or optical media from Unicode, Inc., the sole remedy for any claim will be exchange of defective media within 90 days of receipt.

Unicode, Inc. hereby grants the right to freely use the information supplied in this file in the creation of products supporting the Unicode Standard, and to make copies of this file in any form for internal or external distribution as long as this notice remains attached.

curl

Copyright (c) 1996 - 2011, Daniel Stenberg, <daniel@haxx.se>.

Alle Rechte vorbehalten.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

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 OF THIRD PARTY RIGHTS. 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.

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

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.

GNU General Public License

Some software programs are licensed (or sublicensed) to the user under the GNU General Public License (GPL) or similar Free Software licenses which, among other rights, permit the user to copy, modify, and redistribute certain programs, or portions thereof, and have access to the source code. The GPL requires for any software licensed under the GPL, which is distributed to a user in an executable binary format, that the source code also be made available to those users. For any such software which is distributed along with this Sophos product, the source code is available by submitting a request to Sophos via email to savlinuxgpl@sophos.com. Eine Kopie der GPL Bestimmungen steht unter www.gnu.org/copyleft/gpl.html zum Abruf bereit.

ICU

ICU version 1.8.1 or later

COPYRIGHT AND PERMISSION NOTICE

Copyright © 1995–2008 International Business Machines Corporation and others

Alle Rechte vorbehalten.

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, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do

so, provided that the above copyright notice(s) and this permission notice appear in all copies of the Software and that both the above copyright notice(s) and this permission notice appear in supporting documentation.

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 OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR HOLDERS INCLUDED IN THIS NOTICE BE LIABLE FOR ANY CLAIM, OR ANY SPECIAL INDIRECT OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

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

All trademarks and registered trademarks mentioned herein are the property of their respective owners.

Info-ZIP

Copyright © 1990-2005 Info-ZIP. Alle Rechte vorbehalten.

For the purposes of this copyright and license, “Info-ZIP” is defined as the following set of individuals:

Mark Adler, John Bush, Karl Davis, Harald Denker, Jean-Michel Dubois, Jean-loup Gailly, Hunter Goatley, Ed Gordon, Ian Gorman, Chris Herborth, Dirk Haase, Greg Hartwig, Robert Heath, Jonathan Hudson, Paul Kienitz, David Kirschbaum, Johnny Lee, Onno van der Linden, Igor Mandrichenko, Steve P. Miller, Sergio Monesi, Keith Owens, George Petrov, Greg Roelofs, Kai Uwe Rommel, Steve Salisbury, Dave Smith, Steven M. Schweda, Christian Spieler, Cosmin Truta, Antoine Verheijen, Paul von Behren, Rich Wales, Mike White

This software is provided “as is,” without warranty of any kind, express or implied. In no event shall Info-ZIP or its contributors be held liable for any direct, indirect, incidental, special or consequential damages arising out of the use of or inability to use this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

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

Redistributions in binary form (compiled executables) must reproduce the above copyright notice, definition, disclaimer, and this list of conditions in documentation and/or other materials provided with the distribution. The sole exception to this condition is redistribution of a standard UnZipSFX binary (including SFXWiz) as part of a self-extracting archive; that is permitted without inclusion of this license, as long as the normal SFX banner has not been removed from the binary or disabled.

Altered versions—including, but not limited to, ports to new operating systems, existing ports with new graphical interfaces, and dynamic, shared, or static library versions—must be plainly marked as such and must not be misrepresented as being the original source. Such altered versions also must not be misrepresented as being Info-ZIP releases—including, but not limited to, labeling of the altered versions with the names “Info- ZIP” (or any variation thereof, including, but not limited to, different capitalizations), “Pocket UnZip,” “WiZ” or “MacZip” without the explicit permission of Info-ZIP. Such altered versions are further prohibited from misrepresentative use of the Zip-Bugs or Info-ZIP e-mail addresses or of the Info-ZIP URL(s).

Info-ZIP retains the right to use the names “Info-ZIP,” “Zip,” “UnZip,” “UnZipSFX,” “WiZ,” “Pocket UnZip,” “Pocket Zip,” and “MacZip” for its own source and binary releases.

libmagic – file type detection

Copyright © Ian F. Darwin 1986, 1987, 1989, 1990, 1991, 1992, 1994, 1995.

Software written by Ian F. Darwin and others; maintained 1994–2004 Christos Zoulas.

This software is not subject to any export provision of the United States Department of Commerce, and may be exported to any country or planet.

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 immediately at the beginning of the file, without modification, 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.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR 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 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.

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)

Loki

The MIT License (MIT)

Copyright © 2001 by Andrei Alexandrescu

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.

Medusa web server

Medusa was once distributed under a ‘free for non-commercial use’ license, but in May of 2000 Sam Rushing changed the license to be identical to the standard Python license at the time. The standard Python license has always applied to the core components of Medusa, this change just frees up the rest of the system, including the http server, ftp server, utilities, etc. Medusa is therefore under the following license:

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of Sam Rushing not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission.

SAM RUSHING DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL SAM RUSHING BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Sam would like to take this opportunity to thank all of the folks who supported Medusa over the years by purchasing commercial licenses.

mt19937ar.c

Copyright (c) 1997–2002 Makoto Matsumoto and Takuji Nishimura. Alle Rechte vorbehalten.

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.

The names of its contributors may not 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.

netaddr

Copyright © 2008-2011, David P. D. Moss. Alle Rechte vorbehalten.

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 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.

Open Source Initiative

The Sophos software that is described in this document may include some software that is licensed (or sublicensed) to the user under the Open Source Initiative (OSI), which, among other rights, permits the user to copy, modify, and redistribute certain programs or portions thereof, and have access to the source code. OSI licenses require for any software licensed under their terms which is distributed in object code form, that the source code for such software also be made available to the users of the object code. For any such software, the source code is available by submitting a request to Sophos; via email to support@sophos.de or via the web at http://www.sophos.com/de-de/support/contact-support/contact-information.aspx. The license agreement for any such included software can be found at http://opensource.org/licenses/eclipse-1.0.php

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

Copyright © 1998-2011 The OpenSSL Project. 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.
>
> 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/)”

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.

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.

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

Copyright © 1995–1998 Eric Young (eay@cryptsoft.com) All rights reserved.

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:

Redistributions of source code must retain the 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.

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 :-).

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.]

OPSWAT, Inc.

Diese Software enthält lizenzierte Technologie von © OPSWAT, Inc. OPSWAT ist eine Marke von OPSWAT, Inc.

Protocol Buffers

Copyright © 2008, Google Inc.

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 Google Inc. 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.

pycrypto

Distribute and use freely; there are no restrictions on further dissemination and usage except those imposed by the laws of your country of residence. This software is provided “as is” without warranty of fitness for use or suitability for any purpose, express or implied. Use at your own risk or not at all.

Incorporating the code into commercial products is permitted; you do not have to make source available or contribute your changes back (though that would be nice).

– –amk (www.amk.ca)

Python

PYTHON SOFTWARE FOUNDATION LICENSE VERSION 2

> 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.
>
> 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.
>
> 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.
>
> 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.
>
> 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.
>
> This License Agreement will automatically terminate upon a material breach of its terms and conditions.
>
> 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.
>
> By copying, installing or otherwise using Python, Licensee agrees to be bound by the terms and conditions of this License Agreement.

Regex++, Index

Part of PureMessage uses Regex++, Index (version 3.04, 18 April 2000).

Copyright © 1998-2000, Dr John Maddock

Permission to use, copy, modify, distribute and sell the Regex ++, index library and its documentation for any purpose is hereby granted without fee, provided that the above copyright notice appears in all copies and that both that copyright notice and this permission notice appear in supporting documentation.

Shavlik Technologies

This software contains HFNetChk technology licensed from Shavlik Technologies, LLC. © Shavlik Technologies, LLC.

Simple ECMAScript Engine

Copyright © 2003, 2004, 2005, 2006, 2007 David Leonard. Alle Rechte vorbehalten.

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 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. Alle Rechte vorbehalten.

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:

- 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 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. Alle Rechte vorbehalten.

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:

- 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 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.

TinyXML XML parser

www.sourceforge.net/projects/tinyxml

Original code by Lee Thomason (www.grinninglizard.com)

This software is provided ‘as-is’, without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

- The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
- Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
- This notice may not be removed or altered from any source distribution.

Unicode

UNICODE, INC. LICENSE AGREEMENT – DATA FILES AND SOFTWARE

Unicode Data Files include all data files under the directories http://www.unicode.org/Public/, http://www.unicode.org/reports/, and http://www.unicode.org/cldr/data/. Unicode Software includes any source code published in the Unicode Standard or under the directories http://www.unicode.org/Public/, http://www.unicode.org/reports/, and http://www.unicode.org/cldr/data/.

NOTICE TO USER: Carefully read the following legal agreement. BY DOWNLOADING, INSTALLING, COPYING OR OTHERWISE USING UNICODE INC.'S DATA FILES ("DATA FILES"), AND/OR SOFTWARE ("SOFTWARE"), YOU UNEQUIVOCALLY ACCEPT, AND AGREE TO BE BOUND BY, ALL OF THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE, DO NOT DOWNLOAD, INSTALL, COPY, DISTRIBUTE OR USE THE DATA FILES OR SOFTWARE.

COPYRIGHT AND PERMISSION NOTICE

Copyright © 1991–2007 Unicode, Inc. All rights reserved. Distributed under the Terms of Use in http://www.unicode.org/copyright.html.

Permission is hereby granted, free of charge, to any person obtaining a copy of the Unicode data files and any associated documentation (the "Data Files") or Unicode software and any associated documentation (the "Software") to deal in the Data Files or Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, and/or sell copies of the Data Files or Software, and to permit persons to whom the Data Files or Software are furnished to do so, provided that (a) the above copyright notice(s) and this permission notice appear with all copies of the Data Files or Software, (b) both the above copyright notice(s) and this permission notice appear in associated documentation, and (c) there is clear notice in each modified Data File or in the Software as well as in the documentation associated with the Data File(s) or Software that the data or software has been modified.

THE DATA FILES AND SOFTWARE ARE 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 OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR HOLDERS INCLUDED IN THIS NOTICE BE LIABLE FOR ANY CLAIM, OR ANY SPECIAL INDIRECT OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THE DATA FILES OR SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in these Data Files or Software without prior written authorization of the copyright holder.

UnRAR

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

All copyrights to RAR and the utility UnRAR are exclusively owned by the author - Alexander Roshal.

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.

The UnRAR utility may be freely distributed. It is allowed to distribute UnRAR inside of other software packages.

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.

Installing and using the UnRAR utility signifies acceptance of these terms and conditions of the license.

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

WilsonORMapper

Copyright © 2007, Paul Wilson

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.

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 HOLDER 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.

XPExplorerBar

Copyright © 2004–2005, Mathew Hall

Alle Rechte vorbehalten.

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.

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.

zlib compression tools

© 1995–2002 Jean-loup Gailly and Mark Adler

This software is provided ‘as-is’, without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

This notice may not be removed or altered from any source distribution.

Jean-loup Gailly jloup@gzip.org

Mark Adler madler@alumni.caltech.edu

If you use the zlib library in a product, we would appreciate *not* receiving lengthy legal documents to sign. The sources are provided for free but without warranty of any kind. The library has been entirely written by Jean-loup Gailly and Mark Adler; it does not include third-party code.

If you redistribute modified sources, we would appreciate that you include in the file ChangeLog history information documenting your changes.