

SOPHOS

Sophos Anti-Virus für UNIX 7 Benutzerhandbuch

Dokumentdatum: Oktober 2008



Inhalt

1	Einleitung.....	3
2	Über Sophos Anti-Virus für UNIX	4
3	Ausführen einer On-Demand-Überprüfung.....	5
4	Konfigurieren der On-Demand-Überprüfung.....	7
5	Was passiert, wenn ein Virus bzw. Spyware erkannt wird?.....	11
6	Viren- und Spywarebereinigung.....	12
7	Abrufen des Sophos Anti-Virus-Protokolls.....	15
8	Sofortiges Update für Sophos Anti-Virus	16
9	Anhang A: CID-basierte Konfiguration.....	17
10	Anhang B: Konfigurieren zeitgesteuerter Überprüfungen.....	22
11	Anhang C: Konfigurieren der E-Mail-Benachrichtigung.....	26
12	Anhang D: Konfigurieren der Protokollierung.....	28
13	Anhang E: Konfigurieren der Updates.....	29
14	Fehlersuche.....	32
15	Glossar.....	35
16	Technischer Support.....	37
17	Copyright.....	38

1 Einleitung

Diese Anleitung beschreibt den Einsatz und die Konfiguration von Sophos Anti-Virus für UNIX.

In diesem Handbuch wird davon ausgegangen, dass Sie Sophos Anti-Virus über ein von EM Library erstelltes zentrales Installationsverzeichnis installieren und aktualisieren.

Hinweis: EM Library ist eine Komponente von Sophos Enterprise Console.

Die *Installation* von Sophos Anti-Virus wird in der *Sophos Endpoint Security and Control Netzwerk-Startup-Anleitung* beschrieben.

Die Sophos Dokumentation finden Sie unter www.sophos.de/support/docs/ und auf den Sophos-CDs.

1.1 Typografische Konventionen

Wenn in diesem Handbuch eine Befehlszeileneingabe über eine Zeile hinausgeht, wird die Eingabe auf der Folgezeile eingerückt dargestellt. Beispiel:

```
/opt/sophos-av/bin/savconfig update NamedScans Daily  
/home/fred/DailyScan
```

Geben Sie die gesamte Zeile ohne Zeilenumbruch ein.

2 Über Sophos Anti-Virus für UNIX

2.1 Funktion von Sophos Anti-Virus

Mit Sophos Anti-Virus können Sie Computer unter UNIX, Linux, Windows und Mac OS vor Viren und Spyware schützen. Dies erreichen Sie, indem Sie eine vollständige oder teilweise On-Demand-Überprüfung oder zeitgesteuerte Überprüfung der Festplatte (und von Wechselspeichern) eines oder mehrerer Computer im Netzwerk durchführen.

2.2 Benutzerschnittstelle von Sophos Anti-Virus

Sophos Anti-Virus wird über die Befehlszeile ausgeführt.

Hinweis: Alle Befehle mit Ausnahme von **savscan**, dem Befehl für die On-Demand-Überprüfung, erfordern root-Berechtigungen.

In diesem Handbuch wird davon ausgegangen, dass Sophos Anti-Virus im Standardverzeichnis installiert wurde: /opt/sophos-av. Die Pfade der beschriebenen Befehle sind an diesem Verzeichnis orientiert.

2.3 Konfiguration von Sophos Anti-Virus

Sophos Anti-Virus für UNIX wird gewöhnlich wie folgt konfiguriert:

- Die **On-Demand-Überprüfung** wird über die Befehlszeile konfiguriert.
- Die **zeitgesteuerte Überprüfung, Benachrichtigungen und Alarme** sowie die **Protokolle und Updates** werden zentral über Sophos Enterprise Console konfiguriert. Nähere Informationen finden Sie in der Hilfe zu Enterprise Console.

Sie können auch eine Konfigurationsdatei im zentralen Installationsverzeichnis (CID), über das Sophos Anti-Virus seine Updates bezieht, bearbeiten. Diese Konfigurationsmethode bezeichnen wir als „CID-basierte Konfiguration“.

Hinweis: Greifen Sie nur auf die CID-basierte Konfiguration zurück, wenn Ihnen der technische Support dazu rät oder wenn Ihnen Enterprise Console nicht zur Verfügung steht.



Vorsicht: Eine Konfiguration über Enterprise Console lässt sich nicht gemeinsam mit einer CID-basierten Konfiguration einsetzen.

Wenn Sie Enterprise Console verwenden, gilt Folgendes:

- Parameter, die sich nicht über Enterprise Console verändern lassen, können auf jedem Endpoint lokal über den Befehl **savconfig** festgelegt werden (siehe [Konfiguration mit „savconfig“](#) auf Seite 20). Enterprise Console ignoriert diese Parameter.
- Die automatischen Updates müssen über Enterprise Console eingerichtet werden: Auf den Endpoints ist dies nicht möglich.

3 Ausführen einer On-Demand-Überprüfung

Über *On-Demand-Überprüfungen* werden Computer vollständig oder nur in bestimmten Bereichen auf Viren und Spyware überprüft. Sie können zu festgesetzten Zeiten oder je nach Bedarf durchgeführt werden.

Der Befehl zur Einleitung einer On-Demand-Überprüfung lautet **savscan**.

3.1 Überprüfen des Computers

Hinweis: Eine vollständige Systemüberprüfung auf einem oder mehreren Computern können Sie auch über Enterprise Console durchführen. Nähere Informationen finden Sie in der Hilfe zu Enterprise Console.

☞ Durch Eingabe des folgenden Befehls wird eine Überprüfung durchgeführt:

```
savscan /
```

3.2 Überprüfen eines Verzeichnisses oder einer Datei

☞ Wenn Sie ein bestimmtes Verzeichnis oder eine Datei überprüfen möchten, geben Sie den entsprechenden Pfad an. Beispiel:

```
savscan /usr/Verzeichnis/Datei
```

3.3 Überprüfen eines Dateisystems

☞ Wenn ein Dateisystem überprüft werden soll, geben Sie den entsprechenden Namen ein. Beispiel:

```
savscan /home
```

Sie können mehrere Dateisysteme hintereinander in die Befehlszeile eingeben.

3.4 Fehlercodes

Beim Auftreten eines Fehlers oder bei Erkennung von Viren und/oder Spyware gibt **savscan** einen Fehlercode aus.

Fehlercode	Beschreibung
0	Es sind weder Fehler noch Viren/Spyware aufgetreten.
1	Die Ausführung des Befehls wurde durch die Tastenkombination STRG+C unterbrochen.

Fehlercode	Beschreibung
2	Es ist ein Fehler aufgetreten, der die weitere Ausführung der Überprüfung verhindert.
3	Es wurden Viren, Virenfragmente und/oder Spyware erkannt.

3.4.1 Erweiterte Fehlercodes

Erweiterte Fehlercodes werden ausgegeben, wenn **savscan** mit dem Parameter **-eec** ausgeführt wird.

Erweiterter Fehlercode	Beschreibung
0	Es sind weder Fehler noch Viren/Spyware aufgetreten.
8	Es sind Fehler aufgetreten, die sich nicht auf die Überprüfung auswirken.
16	Es wurden kennwortgeschützte Dateien erkannt, jedoch nicht überprüft.
20	Es wurden Viren und/oder Spyware erkannt und desinfiziert.
24	Es wurden Viren und/oder Spyware erkannt, jedoch nicht desinfiziert.
28	Im Speicher wurden Viren und/oder Spyware erkannt.
32	Bei der Integritätsüberprüfung ist ein Fehler aufgetreten.
36	Es sind unüberwindbare Fehler aufgetreten.
40	Die Ausführung des Befehls wurde unterbrochen.

4 Konfigurieren der On-Demand-Überprüfung

In diesem Abschnitt bezieht sich der Platzhalter *Pfad* hinter einem Befehl auf den zu überprüfenden Pfad.

Eine vollständige Liste der Optionen in Zusammenhang mit der On-Demand-Überprüfung erhalten Sie durch Eingabe von:

```
man savscan
```

4.1 Überprüfen aller Dateitypen

Sophos Anti-Virus überprüft:

- Ausführbare Windows-/DOS-Dateien
- .sh- und .pl-Dateien
- Dateien, die für Makroviren anfällig sind
- HTML-Dateien
- PKLite-, LZEXE- und Diet-Archive
- Unterverzeichnisse
- Symbolisch verknüpfte Objekte

Eine vollständige Liste der von Sophos Anti-Virus standardmäßig überprüften Dateitypen erhalten Sie durch Eingabe von **savscan** gefolgt von der Option **-vv**.

☞ Sollen *alle* Dateitypen überprüft werden, geben Sie die Option **-all** an. Geben Sie Folgendes ein:

```
savscan Pfad -all
```

Hinweis: Diese Überprüfung dauert länger als gewöhnlich und kann die Leistung des Servers beeinträchtigen. Außerdem kann es zu Fehlmeldungen erkannter Viren und Spyware kommen.

4.2 Überprüfen bestimmter Dateitypen

Sophos Anti-Virus überprüft:

- Ausführbare Windows-/DOS-Dateien
- .sh- und .pl-Dateien
- Dateien, die für Makroviren anfällig sind
- HTML-Dateien
- PKLite-, LZEXE- und Diet-Archive
- Unterverzeichnisse
- Symbolisch verknüpfte Objekte

Eine vollständige Liste der von Sophos Anti-Virus standardmäßig überprüften Dateitypen erhalten Sie durch Eingabe von **savscan** gefolgt von der Option **-vv**.

- ¶ Sollen nur bestimmte Dateitypen überprüft werden, geben Sie die Option **-ext** gefolgt von einem Gleichheitszeichen und einer durch Kommas getrennten Liste der Dateinamenerweiterungen der Dateitypen ein, die überprüft werden sollen. Wenn z.B. nur Dateien mit der Erweiterung `.txt` überprüft werden sollen, geben Sie Folgendes ein:

```
savscan Pfad -ext=txt
```

- ¶ Sollen bestimmte Dateitypen von der Überprüfung ausgeschlossen werden, geben Sie die Option **-next** gefolgt von einem Gleichheitszeichen und einer durch Kommas getrennten Liste der Dateinamenerweiterungen der Dateitypen ein, die nicht überprüft werden sollen.

4.3 Überprüfen von Archiven

Mit Sophos Anti-Virus lässt sich auch der Inhalt von Archiven überprüfen. Eine Liste der Archivtypen, die überprüft werden können, erhalten Sie durch Eingabe von **savscan** gefolgt von der Option **-vv**.

- ¶ Sollen alle Archivtypen überprüft werden, geben Sie als Option **-archive** an. Geben Sie Folgendes ein:

```
savscan Pfad -archive
```

Archive, die in andere Archive eingebettet sind (z.B. ein TAR-Archiv in einem ZIP-Archiv) werden rekursiv überprüft.

Wenn Sie über viele umfangreiche Archive verfügen, kann die Überprüfung mehr Zeit in Anspruch nehmen. Dies sollten Sie bei der Planung zeitgesteuerter Überprüfungen berücksichtigen.

4.4 Überprüfen bestimmter Archivtypen

Sie können die Überprüfung mit Sophos Anti-Virus auch auf ganz bestimmte Archivtypen beschränken. Eine Liste der Archivtypen, die überprüft werden können, erhalten Sie durch Eingabe von **savscan** gefolgt von der Option **-vv**.

- ¶ Soll ein bestimmter Archivtyp überprüft werden, geben Sie die in der vollständigen Liste aufgeführte Option an. Durch folgende Eingabe werden z.B. nur TAR- und ZIP-Archive überprüft:

```
savscan Pfad -tar -zip
```

Archive, die in andere Archive eingebettet sind (z.B. ein TAR-Archiv in einem ZIP-Archiv) werden rekursiv überprüft.

Wenn Sie über viele umfangreiche Archive verfügen, kann die Überprüfung mehr Zeit in Anspruch nehmen. Dies sollten Sie bei der Planung zeitgesteuerter Überprüfungen berücksichtigen.

4.5 Überprüfen von Remote-Computern

Sophos Anti-Virus überprüft in der Regel keine Objekte auf Remote-Computern (d.h. SAV durchquert keine Remote Mount Points).

- ¶ Zum Überprüfen von Remote-Computern verwenden Sie die Option **--no-stay-on-machine**. Geben Sie Folgendes ein:

```
savscan Pfad --no-stay-on-machine
```

4.6 Deaktivieren der Überprüfung symbolisch verknüpfter Objekte

Standardmäßig überprüft Sophos Anti-Virus symbolisch verknüpfte Objekte.

- ¶ Wenn Sie die Überprüfung symbolisch verknüpfter Objekte deaktivieren möchten, verwenden Sie die Option **--no-follow-symlinks**. Muster:

```
savscan Pfad --no-follow-symlinks
```

Wenn Objekte nicht mehr als einmal überprüft werden sollen, verwenden Sie als Option **--backtrack-protection**.

4.7 Überprüfen des ursprünglichen Dateisystems

Sophos Anti-Virus kann so konfiguriert werden, dass nur das Dateisystem überprüft wird, in dem sich der angegebene Pfad befindet. So kann eine Überprüfung mehrerer Mount Points verhindert werden.

- ¶ Um nur das ursprüngliche Dateisystem zu überprüfen, verwenden Sie die Option **--stay-on-filesystem**. Geben Sie Folgendes ein:

```
savscan Pfad --stay-on-filesystem
```

4.8 Ausschließen von Objekten von der Überprüfung

Mit der Option **-exclude** können Sie bestimmte Objekte (Dateien, Verzeichnisse oder Dateisysteme) von der Überprüfung ausschließen. Sophos Anti-Virus schließt alle hinter dieser Option angegebenen Objekte von der Überprüfung aus. Wenn z.B. die Objekte „fred“ und „harry“, nicht aber „tom“ und „peter“ überprüft werden sollen, geben Sie Folgendes ein:

```
savscan fred harry -exclude tom peter
```

Sie können auch Verzeichnisse und Dateien von der Überprüfung ausschließen, die einem Verzeichnis *untergeordnet* sind. Wenn z.B. Freds gesamtes „home“-Verzeichnis überprüft werden soll, nicht aber das Verzeichnis „games“ (inklusive aller untergeordneten Verzeichnisse und Dateien), geben Sie Folgendes ein:

```
savscan /home/fred -exclude /home/fred/games
```

Außerdem können Sie Sophos Anti-Virus mit der Option **-include** mitteilen, dass die aufgezählten Objekte in die Überprüfung *eingeschlossen* werden sollen. Wenn z.B. die Objekte

„fred“, „harry“ und „bill“, nicht aber „tom“ und „peter“ überprüft werden sollen, geben Sie Folgendes ein:

```
savscan fred harry -exclude tom peter -include bill
```

4.9 Überprüfen ausführbarer UNIX-Dateien

Normalerweise überprüft Sophos Anti-Virus keine Dateien, die UNIX als ausführbar betrachtet.

- ¶ Sollen Dateien überprüft werden, die UNIX als ausführbar betrachtet, verwenden Sie die Option **--examine-x-bit**. Geben Sie Folgendes ein:

```
savscan Pfad --examine-x-bit
```

Sophos Anti-Virus überprüft weiterhin auch alle Dateitypen, die standardmäßig dafür festgelegt sind. Eine Liste dieser Dateinamenerweiterungen erhalten Sie durch Eingabe von **savscan** gefolgt von der Option **-vv**.

5 Was passiert, wenn ein Virus bzw. Spyware erkannt wird?

Wenn Sophos Anti-Virus bei einer Überprüfung einen Virus oder Spyware erkennt, wird der Fund in einer Zeile gemeldet, die mit >>> beginnt und dahinter entweder Virus oder Virus Fragment enthält:

```
SAVScan virus detection utility Version 4.28.0 [Solaris/SPARC]
Virus data version 4.27, March 2008 Includes detection for
361731 viruses, trojans and worms Copyright (c) 1989-2008 Sophos
Plc, www.sophos.com

System time 12:00:53, System date 18 March 2008

Quick Scanning

>>> Virus 'EICAR-AV-Test' found in file
/usr/mydirectory/eicar.src

33 files scanned in 2 seconds. 1 virus was discovered. 1 file
out of 33 was infected. Please send infected samples to Sophos
for analysis. For advice consult www.sophos.com or email
support@sophos.com End of Scan.
```

Sophos Anti-Virus verzeichnet Viren- und Spywarefunde außerdem im Sophos Anti-Virus-Protokoll (siehe [Abrufen des Sophos Anti-Virus-Protokolls](#) auf Seite 15) und sendet eine E-Mail an root@localhost. Wenn Sophos Anti-Virus von Enterprise Console verwaltet wird, wird ein Alarm an Enterprise Console gesendet.

Informationen zur Beseitigung von Viren- und Spyware finden Sie unter [Viren- und Spywarebereinigung](#) auf Seite 12.

6 Viren- und Spywarebereinigung

6.1 Informationen zur Bereinigung

Auf der Sophos Website erhalten Sie weitere Informationen und Bereinigungshinweise zu Viren und Spyware.

1. Rufen Sie die Seite mit den Sicherheitsanalysen auf: www.sophos.de/security/analyses.
2. Suchen Sie die Analyse des Virus und/oder der Spyware anhand des von Sophos Anti-Virus gemeldeten Namens.

6.2 Isolieren infizierter Dateien

Sophos Anti-Virus kann infizierte Dateien in Quarantäne verschieben (d.h. sie von jeglichen Zugriffen isolieren), sodass sie keinen Schaden auf dem Computer anrichten können. Dies wird durch Änderung der Besitz- und Zugriffsrechte der infizierten Dateien erreicht.

Hinweis: Wenn Sie sowohl Desinfektion (siehe [Bereinigen infizierter Dateien](#) auf Seite 13) als auch Quarantäne auswählen, versucht Sophos Anti-Virus zunächst, die infizierten Objekte zu desinfizieren. Wenn dies nicht gelingt, werden die Dateien in Quarantäne verschoben und somit isoliert.

6.2.1 Parameter für Quarantäne

¶ Der Befehlszeilenparameter zum Isolieren von Dateien lautet **--quarantine**. Geben Sie Folgendes ein:

```
savscan Pfad --quarantine
```

Geben Sie als *Pfad* den Pfad an, der die zu überprüfenden Dateien und Ordner enthält.

6.2.2 Parameter für Besitz- und Zugriffsrechte

Beim Isolieren geschieht Folgendes:

- Der Benutzer, der Sophos Anti-Virus ausführt, wird zum Eigentümer der infizierten Datei.
- Die Gruppe, der der Benutzer angehört, erhält das Besitzrecht an der Datei.
- Die Zugriffsrechte auf die Datei werden in `-r-----` (0400) geändert.

Sie können den Eigentümer, das Gruppenbesitzrecht und die Zugriffsrechte, die infizierten Dateien von Sophos Anti-Virus automatisch zugewiesen werden, jedoch selbst angeben. Dazu gibt es folgende Parameter:

```
uid=nnn user=Benutzername gid=nnn group=Gruppenname mode=ppp
```

Zum Festlegen des Eigentümers oder des Gruppenbesitzes dürfen Sie nicht mehr als einen Parameter angeben. Zum Beispiel ist es nicht möglich, den Parameter **uid** und den Parameter **user** anzugeben.

Für alle nicht von Ihnen verwendeten Parameter wird der Vorgabewert (siehe oben) übernommen.

Beispiel:

```
savscan fred --quarantine:user=virus,group=virus,mode=0400
```

Dieser Befehl weist einer infizierten Datei den Eigentümer „virus“, die Gruppe „virus“ und die Zugriffsberechtigung `-r-----` zu. Die Datei gehört folglich dem Benutzer „virus“ und der Gruppe „virus“ an, doch nur der Benutzer namens „virus“ erhält (Lese-)Zugriff auf die Datei. Bis auf den Benutzer „root“ kann niemand etwas an der Datei ändern.

Als Voraussetzung zum Ändern der Besitz- und Zugriffsrechte kann die Anmeldung mit besonderen Rechten erforderlich sein (z.B. als „superuser“).

6.3 Bereinigen infizierter Dateien

Sophos Anti-Virus kann infizierte Dateien bei einer On-Demand-Überprüfung bereinigen (desinfizieren oder löschen). Alle von Sophos Anti-Virus gegen infizierte Dateien ergriffenen Maßnahmen sind in einer Zusammenfassung und im Sophos Anti-Virus-Protokoll aufgeführt. Standardmäßig ist die Bereinigung deaktiviert.

6.3.1 Desinfizieren einer bestimmten Datei

- ¶ Zum Desinfizieren einer bestimmten Datei geben Sie den Parameter `-di` an. Geben Sie Folgendes ein:

```
savscan Dateipfad -di
```

Sie müssen Ihre Eingabe bestätigen, bevor Sophos Anti-Virus die Datei desinfiziert.

Durch das Desinfizieren von Dokumenten werden keine bis dahin vom Virus verursachten Schäden rückgängig gemacht. (Im Abschnitt [Informationen zur Bereinigung](#) auf Seite 12 erfahren Sie, wo Sie auf der Sophos Website nähere Informationen über das Verhalten von Viren erhalten.)

6.3.2 Desinfizieren aller Dateien auf einem Computer

- ¶ Zum Desinfizieren aller Dateien auf einem Computer geben Sie folgenden Befehl ein:

```
savscan / -di
```

Sie müssen Ihre Eingabe bestätigen, bevor Sophos Anti-Virus die Datei desinfiziert.

Durch das Desinfizieren von Dokumenten werden keine bis dahin vom Virus verursachten Schäden rückgängig gemacht. (Im Abschnitt [Informationen zur Bereinigung](#) auf Seite 12 erfahren Sie, wo Sie auf der Sophos Website nähere Informationen über das Verhalten von Viren erhalten.)

6.3.3 Löschen einer bestimmten infizierten Datei

- ¶ Zum Desinfizieren einer bestimmten infizierten Datei geben Sie den Parameter `-remove` an. Geben Sie Folgendes ein:

```
savscan Dateipfad -remove
```

Sie müssen Ihre Eingabe bestätigen, bevor Sophos Anti-Virus die Datei löscht.

6.3.4 Löschen aller infizierten Dateien auf einem Computer

- ¶ Zum Löschen aller infizierten Dateien auf einem Computer geben Sie folgenden Befehl ein:

```
savscan / -remove
```

Sie müssen Ihre Eingabe bestätigen, bevor Sophos Anti-Virus die Datei löscht.

6.4 Beheben von Virenschäden

Das Vorgehen zum Beheben eines virenbedingten Schadens richtet sich danach, auf welche Weise der Computer infiziert wurde. Einige Viren hinterlassen keine Schäden, während andere Viren einen so großen Schaden verursachen, dass die gesamte Festplatte davon betroffen sein kann.

Einige Viren nehmen nach und nach geringfügige Änderungen an Daten vor. Diese progressive Beschädigungsart lässt sich oft schwer erkennen. Daher raten wir Ihnen, die Sicherheitsanalysen auf der Sophos Website zu lesen und betroffene Dokumente nach der Desinfizierung sorgfältig zu überprüfen.

Es ist auf jeden Fall wichtig, unversehrte Sicherungskopien zur Hand zu haben. Falls Sie vor einer Infizierung noch keine Sicherungskopien angelegt hatten, sollten Sie nach der Bereinigung und Desinfizierung damit anfangen, damit Sie in Zukunft besser vorbereitet sind.

Manchmal lassen sich jedoch noch Daten auf von Viren beschädigten Festplatten retten. Sophos verfügt über Tools zur Behebung bestimmter Virenschäden. Wenn Sie mehr dazu erfahren möchten, wenden Sie sich bitte an den technischen Support von Sophos: siehe [Technischer Support](#) auf Seite 37.

7 Abrufen des Sophos Anti-Virus-Protokolls

Sophos Anti-Virus schreibt alle Überprüfungsvorgänge in das Sophos Anti-Virus-Protokoll und in das *syslog*-Protokoll. Im Sophos Anti-Virus-Protokoll werden außerdem Spyware- und Virenvorfälle sowie aufgetretene Fehler verzeichnet. Die Meldungen im Sophos Anti-Virus-Protokoll werden in alle vom Produkt unterstützten Sprachen übersetzt.

- ¶ Zum Abrufen des Sophos Anti-Virus-Protokolls geben Sie den Befehl **savlog** ein. Durch die Verwendung von Optionen kann die Ausgabe auf bestimmte Meldungen beschränkt werden. Außerdem lässt sich die Darstellungsweise bestimmen.

Wenn Sie z.B. alle Meldungen abrufen möchten, die in den letzten 24 Stunden im Sophos Anti-Virus-Protokoll festgehalten wurden, und das Datum sowie die Uhrzeit gemäß der ISO-Norm 8601 im UTC-Format angegeben werden sollen, lautet der Befehl wie folgt:

```
/opt/sophos-av/bin/savlog --today --utc
```

Eine vollständige Liste der Optionen in Zusammenhang mit **savlog** erhalten Sie durch Eingabe von:

```
man savlog
```

8 Sofortiges Update für Sophos Anti-Virus

Wenn Auto-Updates aktiviert sind, wird Sophos Anti-Virus automatisch auf den neuesten Stand gebracht.

Sie können ein Update auch sofort durchführen lassen, sodass Sie nicht auf das nächste automatische Update warten müssen.

Sofort-Updates sind über Sophos Enterprise Console möglich. Oder gehen Sie zu jedem Computer und verfahren Sie wie folgt:

¶ Geben Sie folgenden Befehl ein:

```
/opt/sophos-av/bin/savupdate
```

9 Anhang A: CID-basierte Konfiguration

Die CID-basierte Konfiguration ist eine Alternative zur Konfiguration über Sophos Enterprise Console.



Vorsicht: Greifen Sie nur auf die CID-basierte Konfiguration zurück, wenn Ihnen der technische Support dazu rät oder wenn Ihnen Enterprise Console nicht zur Verfügung steht.

Hinweis: Dieser Abschnitt gilt nicht für die Konfiguration der On-Demand-Überprüfung. Diese wird unter [Konfigurieren der On-Demand-Überprüfung](#) auf Seite 7 beschrieben.

Für die CID-basierte Konfiguration ist keine Windows-Plattform erforderlich. Bei dieser Art der Konfiguration ändern Sie über den Befehl **savconfig** (siehe [Konfiguration mit „savconfig“](#) auf Seite 20) die Parameterwerte einer Konfigurationsdatei, die anschließend im CID gespeichert wird. Wenn Endpoints ihre Updates über ein CID beziehen, übernehmen sie auch diese Konfiguration.

Sie können Parameter sperren, sodass sie sich auf den Endpoints nicht ändern lassen. So legen Sie die Konfiguration von Sophos Anti-Virus für jeden Endpoint fest, ohne befürchten zu müssen, dass die Einstellungen von Benutzern nach eigenem Ermessen wieder geändert werden können.

Es gibt zwei Konfigurationsdateien: a) eine Live-Konfigurationsdatei im CID und b) eine Offline-Konfigurationsdatei, die an einem anderen Ort gespeichert ist. Wenn die Live-Datei geändert werden soll, nehmen Sie die Änderungen zunächst an der Offline-Datei vor und ersetzen daraufhin die Live-Datei durch diese Datei. Dies wird in den folgenden Abschnitten genauer beschrieben.

9.1 Erstellen einer CID-Konfiguration

1. Über den Befehl **savconfig** können Sie den Wert jedes Parameters in der Offline-Konfigurationsdatei ändern.

Es gilt folgende Syntax:

```
/opt/sophos-av/bin/savconfig -f Konfigurationsdatei -c Vorgang  
Parameter Wert
```

Hierbei gilt:

- **-f** gibt an, dass die Einstellung in der Offline-Datei geändert werden soll.
- *Konfigurationsdatei* ist der Pfad zur Offline-Datei, ein beliebiges Verzeichnis außerhalb des CIDs. Die Datei wird von **savconfig** erstellt.
- **-c** kündigt an, dass auf die Corporate-Ebene der Offline-Datei zugegriffen werden soll. (Näheres über Ebenen erfahren Sie im Abschnitt [Konfigurationsebenen](#) auf Seite 19.)
- *Vorgang*: entweder **set** (setzen), **update** (aktualisieren), **add** (hinzufügen), **remove** (entfernen) oder **delete** (löschen).
- *Parameter* ist der Parameter, der geändert werden soll.
- *Wert* ist der Wert, den der Parameter erhalten soll.

Durch den folgenden Befehl wird beispielsweise im Verzeichnis ./config eine Datei namens „CIDconfig.cfg“ angelegt und E-Mail-Benachrichtigungen werden deaktiviert:

```
/opt/sophos-av/bin/savconfig -f ./config/CIDconfig.cfg -c  
set EmailNotifier Disabled
```

Weitere Informationen zu **savconfig** entnehmen Sie bitte dem Abschnitt [Konfiguration mit „savconfig“](#) auf Seite 20.

2. Zum Anzeigen der Parameterwerte geben Sie als Vorgang **query** an. Es lassen sich sowohl der Wert eines einzelnen Parameters als auch die Werte aller Parameter anzeigen. Um z.B. die Werte aller festgelegten Parameter anzuzeigen, geben Sie Folgendes ein:

```
/opt/sophos-av/bin/savconfig -f ./config/CIDconfig.cfg -c  
query
```

3. Wenn Sie alle Parameter Ihren Anforderungen gemäß festgelegt bzw. geändert haben, aktualisieren Sie Sophos Anti-Virus:

```
/opt/sophos-av/bin/savupdate
```

4. Geben Sie den Befehl **addcfg** mit dem Parameter **-f** gefolgt vom Pfad der Offline-Konfigurationsdatei ein:

```
/opt/sophos-av/update/cache/Primary-unpacked/addcfg.sh -f  
Konfigurationsdatei
```

5. Kopieren Sie das Verzeichnis /opt/sophos-av/update/cache/Primary-unpacked/config in das CID.

Die neue Konfiguration befindet sich nun im CID und steht Endpoints beim nächsten Update zum Download bereit.

9.2 Aktualisieren einer CID-Konfiguration

1. Über den Befehl **savconfig** können Sie den Wert jedes Parameters in der Offline-Konfigurationsdatei ändern.

Es gilt folgende Syntax:

```
/opt/sophos-av/bin/savconfig -f Konfigurationsdatei -c Vorgang  
Parameter Wert
```

Hierbei gilt:

- **-f** gibt an, dass die Einstellung in der Offline-Datei geändert werden soll.
- *Konfigurationsdatei* ist der Pfad der Offline-Datei.
- **-c** kündigt an, dass auf die Corporate-Ebene der Offline-Datei zugegriffen werden soll. (Näheres über Ebenen erfahren Sie im Abschnitt [Konfigurationsebenen](#) auf Seite 19.)
- *Vorgang*: entweder **set** (setzen), **update** (aktualisieren), **add** (hinzufügen), **remove** (entfernen) oder **delete** (löschen).
- *Parameter* ist der Parameter, der geändert werden soll.
- *Wert* ist der Wert, den der Parameter erhalten soll.

Durch den folgenden Befehl wird beispielsweise im Verzeichnis `./config` eine Datei namens `„CIDconfig.cfg“` aktualisiert und E-Mail-Benachrichtigungen werden deaktiviert:

```
/opt/sophos-av/bin/savconfig -f ./config/CIDconfig.cfg -c  
set EmailNotifier Disabled
```

Weitere Informationen zu `savconfig` entnehmen Sie bitte dem Abschnitt [Konfiguration mit „savconfig“](#) auf Seite 20.

Hinweis: Es müssen *alle* Parameter gesetzt werden, die Sie in der Corporate-Ebene der Live-Datei behalten wollen, nicht nur diejenigen, die Sie aktualisieren möchten. Um mit einer Kopie der derzeitigen Live-Konfigurationsdatei zu arbeiten, kopieren Sie die Datei `„CorporateLayer.cfg“` in ein Verzeichnis außerhalb des CIDs. `„CorporateLayer.cfg“` befindet sich im CID im Verzeichnis `config`.

2. Zum Anzeigen der Parameterwerte geben Sie als Vorgang **query** an. Es lassen sich sowohl der Wert eines einzelnen Parameters als auch die Werte aller Parameter anzeigen. Um z.B. die Werte aller festgelegten Parameter anzuzeigen, geben Sie Folgendes ein:

```
/opt/sophos-av/bin/savconfig -f ./config/CIDconfig.cfg -c  
query
```

3. Wenn Sie alle Parameter Ihren Anforderungen gemäß festgelegt bzw. geändert haben, aktualisieren Sie Sophos Anti-Virus:

```
/opt/sophos-av/bin/savupdate
```

4. Geben Sie den Befehl **addcfg** mit dem Parameter **-f** gefolgt vom Pfad der Offline-Konfigurationsdatei ein:

```
/opt/sophos-av/update/cache/Primary-unpacked/addcfg.sh -f  
Konfigurationsdatei
```

5. Kopieren Sie das Verzeichnis `/opt/sophos-av/update/cache/Primary-unpacked/config` in das CID.

Die neue Konfiguration befindet sich nun im CID und steht Endpoints beim nächsten Update zum Download bereit.

9.3 Konfigurationsebenen

Mit jeder Installation von Sophos Anti-Virus wird eine lokale Konfigurationsdatei angelegt, die Einstellungen für alle Komponenten von Sophos Anti-Virus mit Ausnahme der On-Demand-Überprüfung enthält.

Eine lokale Konfigurationsdatei kann aus mehreren Ebenen aufgebaut sein:

- **Sophos:** Diese Ebene ist immer vorhanden. In ihr sind werkseitige Voreinstellungen enthalten, die nur von Sophos geändert werden.
- **Corporate:** Diese Ebene ist vorhanden, wenn Sophos Anti-Virus über das CID konfiguriert wird.
- **User:** Diese Ebene ist vorhanden, wenn Sophos Anti-Virus lokal konfiguriert wird. Sie enthält Einstellungen, die nur für Sophos Anti-Virus auf dem lokalen Computer gelten.

Jede Ebene enthält die gleichen Parameter. So lässt sich ein Parameter für mehrere Ebenen festlegen. Beim Abrufen eines Parameterwerts folgt Sophos Anti-Virus jedoch einer Hierarchie:

- Standardmäßig hat die Corporate-Ebene eine höhere Priorität als die User-Ebene.
- Die Corporate-Ebene und die User-Ebene haben Vorrang vor der Sophos-Ebene.

Wenn z.B. ein bestimmter Parameter sowohl in der User-Ebene als auch in der Corporate-Ebene gesetzt ist, gilt der Wert der Corporate-Ebene. Die Werte einzelner Parameter in der Corporate-Ebene lassen sich jedoch entsperren und so durch die jeweiligen Parameterwerte einer anderen Ebene überschreiben.

Beim Aktualisieren der lokalen Konfigurationsdatei über die Live-Konfigurationsdatei im CID wird die Corporate-Ebene in der lokalen Datei durch die Corporate-Ebene der Live-Datei ersetzt.

9.4 Konfiguration am Einzelplatz

Über den Befehl **savconfig** führen Sie eine Konfiguration an einem Einzelplatzrechner durch. Weitere Informationen zu **savconfig** entnehmen Sie bitte dem Abschnitt *Konfiguration mit „savconfig“* auf Seite 20. Die mit **savconfig** vorgenommenen Konfigurationseinstellungen werden in der User-Ebene der lokalen Konfigurationsdatei gespeichert.

9.5 Konfiguration mit „savconfig“

Mit dem Befehl **savconfig** können Sie die Sophos Anti-Virus-Konfiguration ändern oder abrufen. Der Pfad zu diesem Programm bzw. Befehl lautet `/opt/sophos-av/bin`. Die Konfiguration bestimmter Funktionen von Sophos Anti-Virus anhand dieses Befehls wird nach und nach in diesem Handbuch erläutert. In diesem Unterabschnitt wird lediglich die Syntax erläutert.

Folgende Syntax gilt für den Befehl **savconfig**:

```
savconfig [Option] ... [Vorgang] [Parameter] [Wert] ...
```

Eine vollständige Liste der Optionen, Vorgänge und Parameter erhalten Sie durch Eingabe von:

```
man savconfig
```

9.5.1 Option

Sie können eine oder mehrere Optionen angeben. Die Optionen beziehen sich größtenteils auf die *Ebenen* in der lokalen Konfigurationsdatei einer Installation. Weitere Informationen zu Ebenen finden Sie unter *Konfigurationsebenen* auf Seite 19. Standardmäßig adressiert der Befehl die User-Ebene. Wenn die Corporate-Ebene adressiert werden soll, verwenden Sie die Option **-c** oder **--corporate**.

Normalerweise sind die Parameterwerte in der Corporate-Ebene gesperrt und deaktivieren somit die Werte in der User-Ebene. Wenn eine Corporate-Einstellung von Benutzern überschrieben werden soll, entsperren Sie sie über die Option **--nolock**. Um z.B. den Wert von **LogMaxSizeMB** festzulegen und ihn gleichzeitig zu entsperren, damit er überschrieben werden kann, geben Sie Folgendes ein:

```
/opt/sophos-av/bin/savconfig --nolock -f corpconfig.cfg -c
LogMaxSizeMB 50
```

Wenn Sie Enterprise Console verwenden, können Sie sich über die Option **--consoleav** nur die Parameterwerte der Virenschutzrichtlinie anzeigen lassen. Geben Sie Folgendes ein:

```
/opt/sophos-av/bin/savconfig --consoleav query
```

Über die Option **--consoleupdate** rufen Sie die Werte der Update-Richtlinie von Enterprise Console ab. Geben Sie Folgendes ein:

```
/opt/sophos-av/bin/savconfig --consoleupdate query
```

9.5.2 Vorgang

Sie können einen Vorgang angeben. Die Vorgänge beziehen sich hauptsächlich auf Parameter. Einige Parameter können nur einen Wert besitzen, andere können eine ganze Liste von Werten aufweisen. Mit Vorgängen fügen Sie einer Liste Werte hinzu oder entfernen Werte aus einer Liste. Ein Beispiel: Der Parameter **Email** ist eine *Liste* von E-Mail-Empfängern.

Zum Anzeigen der Parameterwerte geben Sie als Vorgang **query** an. Um z.B. den Wert des Parameters **EmailNotifier** abzurufen, geben Sie Folgendes ein:

```
/opt/sophos-av/bin/savconfig query EmailNotifier
```

Wenn Sie Enterprise Console verwenden und **savconfig** Parameterwerte ausgibt, werden die Werte, die mit der entsprechenden Enterprise Console-Richtlinie in Konflikt stehen, eindeutig durch den Hinweis „Conflict“ gekennzeichnet.

9.5.3 Parameter

Sie können einen Parameter angeben. Durch folgende Eingabe werden alle modifizierbaren Grundparameter aufgelistet:

```
/opt/sophos-av/bin/savconfig -v
```

Für einige Parameter ist außerdem die Eingabe eines Zweitparameters erforderlich.

9.5.4 Wert

Sie können einen oder mehrere Werte angeben, die einem Parameter zugewiesen werden sollen. Sollte ein Wert Leerzeichen enthalten, muss der Wert in Apostrophe gesetzt werden.

9.6 Konfiguration mit „savsetup“

Mit dem Befehl **savsetup** können Sie die Update-Konfiguration ändern oder abrufen. Im Vergleich zur Konfiguration mit **savconfig** erhalten Sie nur Zugriff auf einige Parameter, doch der Umgang mit diesem Befehl ist einfacher. Sie werden zur Eingabe von Parameterwerten aufgefordert. Sie brauchen die Werte also nur einzugeben oder auszuwählen. Durch folgende Eingabe starten Sie **savsetup**:

```
/opt/sophos-av/bin/savsetup
```

10 Anhang B: Konfigurieren zeitgesteuerter Überprüfungen

Sophos Anti-Virus kann Definitionen mehrerer zeitgesteuerter Überprüfungen speichern.

Hinweis: Auch Enterprise Console oder der Befehl **crontab** ermöglicht Ihnen das Überprüfen von Computern zu festgelegten Zeiten. Weitere Informationen erhalten Sie in der Hilfe zu Enterprise Console und im [Sophos Support-Artikel 12176](#). Zeitgesteuerte Überprüfungen, die mit Enterprise Console erstellt wurden, weisen das Präfix „SEC:“ auf und können nur über Enterprise Console geändert oder entfernt werden.

10.1 Laden einer zeitgesteuerten Überprüfung aus einer Datei

1. Um eine Vorlagen-Überprüfungsdefinition als Startpunkt zu verwenden, öffnen Sie `/opt/sophos-av/doc/namedscan.example.en`.
Um eine neue Überprüfungsdefinition zu erstellen, öffnen Sie eine neue Textdatei.
2. Bestimmen Sie die Objekte und die Zeitpunkte für die Überprüfung, und legen Sie anhand der Parameter in der Vorlage sonstige Optionen fest.
Zur Planung der Überprüfung müssen zumindest ein Tag und eine Uhrzeit eingestellt werden.
3. Speichern Sie die Datei in einem beliebigen Verzeichnis. Achten Sie jedoch darauf, dass die Vorlage nicht überschrieben wird.
4. Weisen Sie die über den Befehl **savconfig** gefolgt vom Vorgang **add** und dem Parameter **NamedScans** die zeitgesteuerte Überprüfung Sophos Anti-Virus zu. Geben Sie den Namen der Überprüfung und den Pfad der Überprüfungsdefinitionsdatei an.

Um z.B. eine Überprüfung namens „Daily“ zu laden, die sich unter dem Pfad `/home/fred/DailyScan` befindet, geben Sie ein:

```
/opt/sophos-av/bin/savconfig add NamedScans Daily  
/home/fred/DailyScan
```

10.2 Einrichten einer zeitgesteuerten Überprüfung über Tastatureingabe

1. Weisen Sie die über den Befehl **savconfig** gefolgt vom Vorgang **add** und dem Parameter **NamedScans** die zeitgesteuerte Überprüfung Sophos Anti-Virus zu. Geben Sie den Namen der Überprüfung gefolgt von einem Bindestrich ein. Somit geben Sie an, dass die Definition über die Tastatur eingelesen werden soll.

Um zum Beispiel eine Überprüfung namens „Daily“ einzurichten, geben Sie Folgendes ein:

```
/opt/sophos-av/bin/savconfig add NamedScans Daily -
```

Wenn Sie die Eingabetaste drücken, wartet Sophos Anti-Virus auf Ihre Eingabe der Definition für die zeitgesteuerte Überprüfung.

2. Bestimmen Sie die Objekte und die Zeitpunkte für die Überprüfung, und legen Sie anhand der Parameter in der Vorlagen-Überprüfungsdefinition sonstige Optionen fest.

/opt/sophos-av/doc/namedscan.example.en. Drücken Sie nach Eingabe jedes Parameters und des Werts jeweils die Eingabetaste.

Zur Planung der Überprüfung müssen zumindest ein Tag und eine Uhrzeit eingestellt werden.

3. Wenn Sie mit der Definition fertig sind, drücken Sie STRG+D.

10.3 Exportieren einer zeitgesteuerten Überprüfung in eine Datei

- ¶ Wenn Sie über Sophos Anti-Virus eine zeitgesteuerte Überprüfung in eine Datei exportieren möchten, geben Sie den Befehl **savconfig** gefolgt vom Vorgang **query** und dem Parameter **NamedScans** ein. Geben Sie den Namen der Überprüfung und den Pfad der Datei ein, in die Sie die Überprüfung exportieren möchten.

Um z.B. eine Überprüfung namens „Daily“ in die Datei /home/fred/DailyScan zu exportieren, geben Sie ein:

```
/opt/sophos-av/bin/savconfig query NamedScans Daily >
/home/fred/DailyScan
```

10.4 Exportieren aller zeitgesteuerten Überprüfungen in eine Datei

- ¶ Wenn Sie alle zeitgesteuerten Überprüfungen (einschl. der mit Enterprise Console erstellten Überprüfungen) von Sophos Anti-Virus in eine Datei exportieren möchten, geben Sie den Befehl **savconfig** gefolgt vom Vorgang **query** und dem Parameter **NamedScans** ein. Geben Sie den Pfad der Datei an, in die die Überprüfungen exportiert werden sollen.

Um z.B. alle zeitgesteuerten Überprüfungen in die Datei /home/fred/AllScans zu exportieren, geben Sie ein:

```
/opt/sophos-av/bin/savconfig query NamedScans >
/home/fred/AllScans
```

Hinweis: Die Überprüfung **SEC:FullSystemScan** ist immer definiert, wenn der Computer von Enterprise Console verwaltet wird.

10.5 Senden einer zeitgesteuerten Überprüfung an die Standardausgabe

- ¶ Wenn Sie eine zeitgesteuerte Überprüfung von Sophos Anti-Virus an die Standardausgabe senden möchten, geben Sie den Befehl **savconfig** gefolgt vom Vorgang **query** und dem Parameter **NamedScans** ein. Geben Sie den Namen der Überprüfung ein.

Um zum Beispiel die Definition der Überprüfung „Daily“ an die Standardausgabe zu senden, geben Sie ein:

```
/opt/sophos-av/bin/savconfig query NamedScans Daily
```

10.6 Senden aller zeitgesteuerten Überprüfungen an die Standardausgabe

- ¶ Wenn alle zeitgesteuerten Überprüfungen (einschl. der mit Enterprise Console erstellten Überprüfungen) von Sophos Anti-Virus an die Standardausgabe gesendet werden sollen, geben Sie den Befehl **savconfig** gefolgt vom Vorgang **query** und dem Parameter **NamedScans** ein.

Um alle zeitgesteuerten Überprüfungen an die Standardausgabe zu senden, geben Sie Folgendes ein:

```
/opt/sophos-av/bin/savconfig query NamedScans
```

Hinweis: Die Überprüfung `SEC:FullSystemScan` ist immer definiert, wenn der Computer von Enterprise Console verwaltet wird.

10.7 Ändern einer zeitgesteuerten Überprüfung, die aus einer Datei geladen wurde

Hinweis: Sie können keine zeitgesteuerten Überprüfungen ändern, die mit Enterprise Console erstellt wurden.

1. Öffnen Sie die Datei, in der die zeitgesteuerte Überprüfung definiert ist, die geändert werden soll.

Wenn die Überprüfung nicht bereits in einer Datei definiert wurde, können Sie die Überprüfung in eine Datei exportieren. Lesen Sie dazu den Abschnitt [Exportieren einer zeitgesteuerten Überprüfung in eine Datei](#) auf Seite 23.

2. Passen Sie die Definition ggf. an. Verwenden Sie dabei nur Parameter, die in der Vorlagen-Überprüfungsdefinition aufgeführt sind:
`/opt/sophos-av/doc/namedscan.example.en`. Die Überprüfung muss vollständig definiert werden, d.h. Sie dürfen nicht nur die Bereiche angeben, die geändert werden sollen.
3. Speichern Sie die Datei.
4. Ändern Sie die zeitgesteuerte Überprüfung in Sophos Anti-Virus über den Befehl **savconfig** gefolgt vom Vorgang **update** und dem Parameter **NamedScans**. Geben Sie den Namen der Überprüfung und den Pfad der Überprüfungsdefinitionsdatei an.

Um z.B. eine Überprüfung namens „Daily“ zu ändern, die sich unter dem Pfad `/home/fred/DailyScan` befindet, geben Sie ein:

```
/opt/sophos-av/bin/savconfig update NamedScans Daily  
/home/fred/DailyScan
```

10.8 Ändern einer zeitgesteuerten Überprüfung über Tastatureingabe

Hinweis: Sie können keine zeitgesteuerten Überprüfungen ändern, die mit Enterprise Console erstellt wurden.

1. Ändern Sie die zeitgesteuerte Überprüfung in Sophos Anti-Virus über den Befehl **savconfig** gefolgt vom Vorgang **update** und dem Parameter **NamedScans**. Geben Sie den Namen der Überprüfung gefolgt von einem Bindestrich ein. Somit geben Sie an, dass die Definition über die Tastatur eingelesen werden soll.

Um zum Beispiel eine Überprüfung namens „Daily“ zu ändern, geben Sie ein:

```
/opt/sophos-av/bin/savconfig update NamedScans Daily -
```

Wenn Sie die Eingabetaste drücken, wartet Sophos Anti-Virus auf Ihre Eingabe der Definition für die zeitgesteuerte Überprüfung.

2. Bestimmen Sie die Objekte und die Zeitpunkte für die Überprüfung, und legen Sie anhand der Parameter in der Vorlagen-Überprüfungsdefinition sonstige Optionen fest. `/opt/sophos-av/doc/namedscan.example.en`. Drücken Sie nach Eingabe jedes Parameters und des Werts jeweils die Eingabetaste. Die Überprüfung muss vollständig definiert werden, d.h. Sie dürfen nicht nur die Bereiche angeben, die geändert werden sollen.

Zur Planung der Überprüfung müssen zumindest ein Tag und eine Uhrzeit eingestellt werden.

3. Wenn Sie mit der Definition fertig sind, drücken Sie STRG+D.

10.9 Löschen einer zeitgesteuerten Überprüfung

Hinweis: Sie können keine zeitgesteuerten Überprüfungen löschen, die mit Enterprise Console erstellt wurden.

- ¶ Wenn Sie eine zeitgesteuerte Überprüfung aus Sophos Anti-Virus löschen möchten, geben Sie den Befehl **savconfig** gefolgt vom Vorgang **remove** und dem Parameter **NamedScans** ein. Geben Sie den Namen der Überprüfung ein.

Um zum Beispiel eine Überprüfung namens „Daily“ zu löschen, geben Sie ein:

```
/opt/sophos-av/bin/savconfig remove NamedScans Daily
```

10.10 Löschen aller zeitgesteuerten Überprüfungen

Hinweis: Sie können keine zeitgesteuerten Überprüfungen löschen, die mit Enterprise Console erstellt wurden.

- ¶ Geben Sie folgenden Befehl ein, wenn Sie alle zeitgesteuerten Überprüfungen aus Sophos Anti-Virus löschen möchten:

```
/opt/sophos-av/bin/savconfig delete NamedScans
```

11 Anhang C: Konfigurieren der E-Mail-Benachrichtigung



Vorsicht: Wenn Sie einen einzigen Computer im Netzwerk konfigurieren, könnte die Konfiguration beim Download einer neuen Konfiguration (über Konsole oder CID) auf diesem Computer überschrieben werden.

11.1 Aktivieren und Deaktivieren von E-Mail-Benachrichtigungen

Standardmäßig sind E-Mail-Benachrichtigungen aktiviert.

- ¶ Zum Aktivieren und Deaktivieren von E-Mail-Benachrichtigungen setzen Sie den Parameter **EmailNotifier** auf „enabled“ bzw. „disabled“. Geben Sie Folgendes ein:

```
/opt/sophos-av/bin/savconfig set EmailNotifier disabled
```

11.2 Angeben des Hostnamens bzw. der IP-Adresse des SMTP-Servers

Standardmäßig lauten Hostname und Port des SMTP-Servers „localhost:25“.

- ¶ Über den Parameter **EmailServer** geben Sie den Hostnamen bzw. die IP-Adresse des SMTP-Servers ein. Beispiel:

```
/opt/sophos-av/bin/savconfig set EmailServer 171.17.31.184
```

11.3 Angeben der Sprache

- ¶ Über den Parameter **EmailLanguage** geben Sie die Sprache an, in der die E-Mail-Benachrichtigungen ausgegeben werden sollen. Zurzeit können Sie zwischen den Werten *en*, *English* und *Japanese* wählen. Beispiel:

```
/opt/sophos-av/bin/savconfig set EmailLanguage Japanese
```

Hinweis: Die Sprachauswahl bezieht sich nur auf die Benachrichtigung an sich, nicht die Meldungen, die in den folgenden Abschnitten beschrieben werden.

11.4 Angeben der E-Mail-Empfänger

Standardmäßig sendet Sophos Anti-Virus E-Mail-Benachrichtigungen an root@localhost.

- ¶ Über den Parameter **Email** geben Sie die Empfänger von E-Mail-Benachrichtigungen an. Beispiel:

```
/opt/sophos-av/bin/savconfig add Email admin@localhost
```

Hinweis: Sie können mehrere Empfänger hintereinander in die Befehlszeile eingeben. Mehrere Empfänger trennen Sie durch ein Leerzeichen voneinander ab.

11.5 Aktivieren/Deaktivieren der E-Mail-Zusammenfassungen über erkannte Viren/Spyware

Bei Erkennung von Viren/Spyware sendet Sophos Anti-Virus standardmäßig eine E-Mail-Zusammenfassung der Überprüfung.

- ¶ Um die Benachrichtigung über erkannte Viren und Spyware zu aktivieren bzw. deaktivieren, setzen Sie den Parameter **EmailDemandSummaryIfThreat** auf „enabled“ bzw. „disabled“. Beispiel:

```
/opt/sophos-av/bin/savconfig set EmailDemandSummaryIfThreat disabled
```

11.6 Ändern der Protokollmeldung

Standardmäßig sendet Sophos Anti-Virus eine E-Mail-Benachrichtigung mit einer voreingestellten Protokollmeldung, wenn im Sophos Anti-Virus-Protokoll ein Ereignis festgehalten wird.

- ¶ Über den Parameter **LogMessage** können Sie die von Sophos Anti-Virus ausgegebene Protokollmeldung ändern. Sie können die Meldung in Englisch oder Japanisch eingeben. Beispiel:

```
/opt/sophos-av/bin/savconfig set LogMessage 'Contact IT'
```

12 Anhang D: Konfigurieren der Protokollierung



Vorsicht: Wenn Sie einen einzigen Computer im Netzwerk konfigurieren, könnte die Konfiguration beim Download einer neuen Konfiguration (über Konsole oder CID) auf diesem Computer überschrieben werden.

Standardmäßig werden die Überprüfungsvorgänge im Sophos Anti-Virus-Protokoll festgehalten: `/opt/sophos-av/log/savd.log`. Wenn ein Protokoll auf 1 MB anwächst, werden im gleichen Verzeichnis automatisch eine Sicherungskopie und ein neues Protokoll wird angelegt.

¶ Wenn Sie wissen möchten, wie viele Protokolle standardmäßig angelegt werden können, geben Sie ein:

```
/opt/sophos-av/bin/savconfig -s query LogMaxSizeMB
```

¶ Über den Parameter `LogMaxSizeMB` legen Sie die maximale Anzahl an Protokollen fest. Beispiel:

```
/opt/sophos-av/bin/savconfig set LogMaxSizeMB 50
```

13 Anhang E: Konfigurieren der Updates

Wichtig: Wenn Sie Sophos Anti-Virus für UNIX über Enterprise Console verwalten, müssen Sie die Updates mit Enterprise Console konfigurieren. Einzelheiten dazu finden Sie unter Hilfe zu Enterprise Console in diesem Abschnitt.

13.1 Grundbegriffe

Update-Server

Unter *Update-Server* ist ein Computer mit Sophos Anti-Virus für UNIX zu verstehen, der anderen Computern als Update-Quelle dient. Die anderen Computer können entweder Update-Server oder Update-Endpoints sein. Dies richtet sich danach, auf welche Weise Sophos Anti-Virus im Netzwerk eingesetzt wird.

Update-Endpoint

Unter *Update-Endpoint* ist ein Computer mit Sophos Anti-Virus für UNIX zu verstehen, der anderen Computern **nicht** als Update-Quelle dient.

Primäre Update-Quelle

Bei der *primären Update-Quelle* handelt es sich um den Pfad, über den Computer gewöhnlich ihre Updates beziehen. Zum Zugriff auf diesen Pfad sind u.U. Zugangsdaten erforderlich.

Sekundäre Update-Quelle

Bei der *sekundären Update-Quelle* handelt es sich um den Pfad, über den Computer ihre Updates beziehen, wenn die primäre Update-Quelle nicht verfügbar ist. Zum Zugriff auf diesen Pfad sind u.U. Zugangsdaten erforderlich.

13.2 Anzeigen der Auto-Update-Konfiguration auf einem Computer

1. Geben Sie auf dem Computer, dessen Auto-Update-Konfiguration Sie sich ansehen möchten, den Befehl **savsetup** ein:

```
/opt/sophos-av/bin/savsetup
```

Nun fordert **savsetup** Sie zur Auswahl einer Aktion auf.

2. Wählen Sie **Display update configuration**, um die aktuelle Konfiguration anzuzeigen.

13.3 Konfigurieren von Updates für mehrere Update-Endpoints

Hinweis: Wenn Sie die Konfiguration für nur einen Update-Endpoint ändern möchten, lesen Sie bitte den Abschnitt [Konfigurieren von Updates für einen Update-Endpoint](#) auf Seite 31.

Auf dem Update-Server nehmen Sie Ihre Änderungen an der Offline-Konfigurationsdatei vor und übertragen die Änderungen auf die Live-Konfigurationsdatei, sodass die Update-Endpoints für den nächsten Download korrekt konfiguriert sind. Im Folgenden steht *Konfigurationsdatei* für den Pfad der Offline-Konfigurationsdatei.

In diesem Abschnitt wird davon ausgegangen, dass Sie die *primäre* Update-Quelle ändern möchten. Wenn Sie jedoch die *zweite* Update-Quelle konfigurieren möchten, geben Sie

stattdessen die Parameter der zweiten Update-Quelle an. Verwenden Sie z.B. statt **PrimaryUpdateSourcePath** den Parameter **SecondaryUpdateSourcePath**.

1. Geben Sie hinter dem Parameter **PrimaryUpdateSourcePath** als Adresse der primären Update-Quelle den Pfad des zentralen Installationsverzeichnisses an. Sie können entweder eine HTTP-Adresse oder einen UNC-Pfad angeben, je nachdem, wie Sie den Update-Server eingerichtet haben. Beispiel:

```
/opt/sophos-av/bin/savconfig -f Konfigurationsdatei -c set  
PrimaryUpdateSourcePath 'http://www.mywebcid.com/cid'
```

2. Falls für den Zugriff auf die primäre Update-Quelle eine Anmeldung erforderlich ist, legen Sie über die Parameter **PrimaryUpdateUsername** und **PrimaryUpdatePassword** jeweils einen Benutzernamen und ein Kennwort fest. Beispiel:

```
/opt/sophos-av/bin/savconfig -f Konfigurationsdatei -c set  
PrimaryUpdateUsername 'fred'
```

```
/opt/sophos-av/bin/savconfig -f Konfigurationsdatei -c set  
PrimaryUpdatePassword 'j23rjfwj'
```

3. Wenn Sie die Verbindung zur primären Update-Quelle über einen Proxyserver herstellen, legen Sie über die Parameter **PrimaryUpdateProxyAddress**, **PrimaryUpdateProxyUsername** und **PrimaryUpdateProxyPassword** jeweils die Adresse, den Benutzernamen und das Kennwort fest. Beispiel:

```
/opt/sophos-av/bin/savconfig -f Konfigurationsdatei -c set  
PrimaryUpdateProxyAddress 'http://www-cache.xyz.com:8080'
```

```
/opt/sophos-av/bin/savconfig -f Konfigurationsdatei -c set  
PrimaryUpdateProxyUsername 'penelope'
```

```
/opt/sophos-av/bin/savconfig -f Konfigurationsdatei -c set  
PrimaryUpdateProxyPassword 'fj202jrjf'
```

4. Wenn Sie alle Parameter Ihren Anforderungen gemäß festgelegt bzw. geändert haben, aktualisieren Sie Sophos Anti-Virus:

```
/opt/sophos-av/bin/savupdate
```

5. Geben Sie den Befehl **addcfg** mit dem Parameter **-f** gefolgt vom Pfad der Offline-Konfigurationsdatei ein:

```
/opt/sophos-av/update/cache/Primary-unpacked/addcfg.sh -f  
Konfigurationsdatei
```

6. Kopieren Sie das Verzeichnis `/opt/sophos-av/update/cache/Primary-unpacked/config` in das CID.

Die neue Konfiguration befindet sich nun im CID und steht Endpoints beim nächsten Update zum Download bereit.

13.4 Konfigurieren von Updates für einen Update-Endpoint

Hinweis: Wenn Sie die Konfiguration für mehrere Update-Endpoints ändern möchten, lesen Sie bitte den Abschnitt [Konfigurieren von Updates für mehrere Update-Endpoints](#) auf Seite 29.

1. Geben Sie auf dem zu konfigurierenden Computer den Befehl **savsetup** ein:

```
/opt/sophos-av/bin/savsetup
```

Nun fordert **savsetup** Sie zur Auswahl einer Aktion auf.

2. Wählen Sie die Option zur Konfiguration der primären (oder sekundären) Update-Quelle auf Ihrem Server.

Geben Sie daraufhin die Details der Update-Quelle ein.

3. Geben Sie die Adresse der Update-Quelle und ggf. die Zugangsdaten (Benutzername und Kennwort) ein.

Sie können entweder eine HTTP-Adresse oder einen UNC-Pfad angeben, je nachdem, wie Sie den Update-Server eingerichtet haben.

Nun fragt **savsetup**, ob die Verbindung zum Update-Server über einen Proxyserver hergestellt werden soll.

4. Wenn dies der Fall ist, drücken Sie „Y“ und geben Sie die entsprechenden Details ein.

14 Fehlersuche

Dieser Abschnitt enthält Tipps zur Fehlerbehebung in Zusammenhang mit Sophos Anti-Virus.

Nähere Informationen zu den von Sophos Anti-Virus bei der On-Demand-Überprüfung ausgegebenen Fehlercodes finden Sie unter [Fehlercodes](#) auf Seite 5.

14.1 Befehl wird nicht ausgeführt

Wenn Sie einen bestimmten Befehl nicht ausführen können, verfügen Sie möglicherweise nicht über die erforderlichen Berechtigungen. Melden Sie sich als „root“ an.

14.2 Meldung „man page not found“ wird ausgegeben

Wenn beim Aufruf einer Sophos Anti-Virus-Manpage diese Meldung ausgegeben wird, müssen Sie wahrscheinlich Ihre Systemeinstellungen ändern. Die Umgebungsvariable MANPATH in /etc/login oder /etc/profile muss /usr/local/man enthalten. Wenn dieser Pfad nicht darin enthalten ist, fügen Sie ihn wie folgt beschrieben hinzu. Ändern Sie nicht die vorhandenen Einstellungen.

¶ Wenn Sie als Shell **sh**, **ksh** oder **bash** verwenden, geben Sie ein:

```
MANPATH=$MANPATH:/usr/local/man
```

```
export MANPATH
```

¶ Wenn Sie als Shell **csh** oder **tsh** verwenden, geben Sie ein:

```
setenv MANPATH Werte:/usr/local/man
```

Dabei ist *Werte* durch die vorhandenen Einstellungen zu ersetzen.

Hinweis: Wenn Sie über kein Anmeldeskript verfügen, müssen Sie diese Werte nach jedem Neustart des Computers erneut festlegen.

14.3 Nicht genug Speicherplatz auf Festplatte

Dieses Problem kann beim Überprüfen umfangreicher Archive auftreten. Folgende Ursachen sind möglich:

- Beim Entpacken der Archive lagert Sophos Anti-Virus die Zwischenergebnisse im temporären Verzeichnis (/tmp) aus. Wenn dieses Verzeichnis nicht groß genug ist, kann Sophos Anti-Virus nicht alle erforderlichen Dateien darin auslagern.
- Sophos Anti-Virus hat das Speicherkontingent des Benutzers überschritten.

Um dies zu umgehen, vergrößern Sie entweder die Kapazität des temporären Verzeichnisses (/tmp) oder das Speicherkontingent des Benutzers. Oder geben Sie für die Auslagerung der Zwischenergebnisse ein anderes Verzeichnis an. Verwenden Sie dazu die Umgebungsvariable SAV_TMP.

14.4 Langsame On-Demand-Überprüfung

Dieses Problem kann zwei Ursachen haben:

- Normalerweise führt Sophos Anti-Virus eine schnelle Überprüfung durch, die nur die auf Virenbefall verdächtigen Bereiche einer Datei untersucht. Wenn jedoch (über die Option `-f`) die vollständige Überprüfung eingestellt ist, werden die Dateien gründlich untersucht. Folglich nimmt die Überprüfung mehr Zeit in Anspruch.
- Normalerweise überprüft Sophos Anti-Virus nur bestimmte Dateitypen. Wenn jedoch die Überprüfung *aller* Dateitypen eingestellt ist, dauert der Vorgang länger. Sollen Dateien mit bestimmten Erweiterungen überprüft werden, nehmen Sie diese Erweiterungen in die Liste der von Sophos Anti-Virus standardmäßig überprüften Dateitypen auf. Weitere Informationen finden Sie unter [Überprüfen bestimmter Dateitypen](#) auf Seite 7.

14.5 Archiver legt Backups aller Dateien an, die einer On-Demand-Überprüfung unterzogen wurden

Ihr Archivierungsprogramm kann so eingestellt sein, dass es nach einer On-Demand-Überprüfung immer Backups der Dateien anlegt. Dies kann auf Änderungen zurückzuführen sein, die Sophos Anti-Virus in der Zeit des geänderten Status von Dateien vornimmt.

Standardmäßig versucht Sophos Anti-Virus, die Zugriffszeit (**atime**) von Dateien auf die vor der Überprüfung angegebene Zeit zurückzusetzen. Dadurch wird jedoch das im Indexeintrag festgesetzte Attribut „status-changed time“ (**ctime**) geändert. Wenn Ihr Archivierungsprogramm anhand der **ctime** ermittelt, ob eine Datei geändert wurde, legt es von allen überprüften Dateien Backups an.

Um dies abzustellen, führen Sie `savscan` mit der Option `--no-reset-atime` aus.

14.6 Viren/Spyware nicht beseitigt

Wenn Sophos Anti-Virus einen Virus bzw. Spyware nicht beseitigt hat, überprüfen Sie, ob die automatische Bereinigung aktiviert ist.

Wenn Sophos Anti-Virus den Virus nicht beseitigen konnte (`Disinfection failed`), könnte es daran liegen, dass zum Zeitpunkt der Überprüfung keine Desinfektion dieses Virentyps möglich war.

Prüfen Sie auch Folgendes:

- Wenn es sich um einen Wechseldatenträger (z.B. Diskette oder CD-ROM) handelt, heben Sie den Schreibschutz auf.
- Wenn sich die Dateien auf einem NTFS-Dateisystem befinden, bereinigen Sie sie lokal auf dem Computer, auf dem der Virus bzw. die Spyware erkannt wurde.

Solange Sophos Anti-Virus keine exakte Viren-/Spyware-Entsprechung findet, können Viren-/Spyware-Fragmente nicht beseitigt werden.

14.7 Viren-/Spyware-Fragment wurde gemeldet

Wenn ein Viren-/Spyware-Fragment gemeldet wird, laden Sie auf dem betroffenen Computer die neuesten Viren-Updates für Sophos Anti-Virus herunter. Danach sollten Sie eine Überprüfung auf dem Computer durchführen. Sollten immer noch Viren-/Spyware-Fragmente gemeldet werden, wenden Sie sich an den technischen Support von Sophos: siehe [Technischer Support](#) auf Seite 37.

Die Meldung eines Viren-/Spyware-Fragments deutet darauf hin, dass eine Datei teilweise einem Viren- oder Spywaremuster entspricht. Es sind drei Ursachen möglich:

- Viele neue Viren oder Spywareobjekte basieren auf vorhandenen Mustern, die zum Teil bereits in bekannten Viren bzw. Spywareobjekten aufgetreten sind. Die Meldung eines Viren-/Spyware-Fragments kann durchaus bedeuten, dass Sophos Anti-Virus einen neuen Virus bzw. ein neues Spywareobjekt erkannt hat, der bzw. das freigesetzt werden könnte.
- Viele Viren enthalten Bugs in ihren Vervielfältigungsroutinen, wodurch die Zielfdateien auf die falsche Weise betroffen werden. Der untätige, womöglich größte Teil des Virus kann in der Trägerdatei auftreten. Dies wird von Sophos Anti-Virus erkannt. Ein beschädigter Virus kann sich nicht verbreiten.
- Beim Durchführen einer vollständigen Überprüfung kann Sophos Anti-Virus den Fund eines Virus bzw. eines Spywareobjekts in einer Datenbankdatei melden.

15 Glossar

Bereinigung	Unter diesem Begriff ist die Desinfektion und die Entfernung von Viren/Spyware zu verstehen.
CID	Siehe „zentrales Installationsverzeichnis“.
CID-Konfigurationsdatei	Eine im CID gespeicherte Datei, in der die Konfiguration von Sophos Anti-Virus gespeichert ist, die für das gesamte Netzwerk gilt. Änderungen werden gewöhnlich erst an der Offline-Konfigurationsdatei vorgenommen, die sich in einem anderen Verzeichnis befindet. Danach werden die Änderungen über einen bestimmten Befehl an die Live-Konfigurationsdatei im CID übertragen.
Desinfektion / Beseitigung	Unter Desinfektion bzw. Beseitigung ist das Löschen eines Virus aus einer Datei oder dem Bootsektor zu verstehen. Durch diesen Vorgang werden jedoch keine Schäden rückgängig gemacht, die der Virus bereits angerichtet haben könnte.
Konfiguration über Enterprise Console	Diese Konfiguration wird über eine grafische Benutzeroberfläche (Enterprise Console) durchgeführt, ist allerdings nur unter Windows möglich und bietet nicht alle Einstellungsoptionen.
Konfiguration über zentrales Installationsverzeichnis	Bei dieser Art der Konfiguration ändern Sie über den Befehl savconfig die Parameterwerte einer Konfigurationsdatei, die anschließend im CID gespeichert wird. Wenn Endpoints ihre Updates über ein CID beziehen, übernehmen sie auch diese Konfiguration.
Lokale Konfigurationsdatei	Eine auf einem Endpoint ausgelagerte Datei, in der die für diesen Endpoint geltenden Sophos Anti-Virus-Konfigurationsdaten festgehalten sind.
On-Demand-Überprüfung	Eine vollständige oder teilweise Überprüfung eines Computers auf Viren und Spyware, die zu festgesetzten Zeiten oder je nach Bedarf durchgeführt werden kann.
Primäre Update-Quelle	Hierbei handelt es sich um den Netzwerkpfad, über den Updates verfügbar gemacht werden. Zum Zugriff auf diesen Pfad sind u.U. Zugangsdaten erforderlich.
Schnelle Überprüfung	Bei dieser Art der On-Demand-Überprüfung handelt es sich um die Standardeinstellung. Sophos Anti-Virus überprüft nur die auf Virenbefall verdächtigsten Bereiche der Dateien.
Sekundäre Update-Quelle	Hierbei handelt es sich um den Netzwerkpfad, über den Updates verfügbar gemacht werden, wenn die primäre Update-Quelle nicht verfügbar ist. Zum Zugriff auf diesen Pfad sind u.U. Zugangsdaten erforderlich.

Spyware	Ein Programm, das sich hinterlistig und unbemerkt auf dem Computer eines ahnungslosen Benutzers installiert und auf diesem Computer gespeicherte Informationen ohne Erlaubnis oder Benachrichtigung des Benutzers an Dritte weiterleitet. Unter die Kategorie Spyware fallen Programme, die Unternehmensdaten entwenden, finanzielle Verluste herbeiführen und Netzwerkschäden verursachen. Dabei kann es sich u.a. um Keylogger, Backdoortrojaner, Kennwortdiebe und Botnet-Würmer handeln.
Update-Endpoint	Ein Computer, auf dem Sophos Anti-Virus für UNIX installiert ist, der anderen Computern nicht als Update-Quelle dient.
Update-Server	Ein Computer, auf dem Sophos Anti-Virus für UNIX installiert ist, der anderen Computern als Update-Quelle dient. Die anderen Computer können entweder Update-Server oder Update-Endpoints sein. Dies richtet sich danach, auf welche Weise Sophos Anti-Virus im Netzwerk eingesetzt wird.
Virus	Ein Programm, das sich durch Anhängen an andere Programme vervielfältigt und sich so auf mehrere Computer und Netzwerke ausbreiten kann.
Vollständige Überprüfung	Wenn Sophos Anti-Virus auf vollständige On-Demand-Überprüfungen eingestellt ist, werden die Dateien im angegebenen Bereich vollständig überprüft. Eine vollständige Überprüfung nimmt deutlich mehr Zeit in Anspruch als eine schnelle Überprüfung. Diese ausführliche Überprüfung ist gelegentlich angebracht, um bestimmte Viren ausfindig zu machen. Zur Aktivierung der vollständigen Überprüfung geben Sie die Option -f an.
Zentrales Installationsverzeichnis	Hierbei handelt es sich um das zentrale Netzwerkverzeichnis, über das Sophos Anti-Virus installiert und durch Updates aktualisiert wird. Jede Plattform erfordert ein eigenes zentrales Installationsverzeichnis. Jedes Verzeichnis muss stets auf dem neuesten Stand gehalten werden.

16 Technischer Support

Falls Sie Technischen Support für diese Beta-Version benötigen, beachten Sie bitte Folgendes:

1. Halten Sie die Ihnen von Sophos per E-Mail zugeschickte Webadresse bereit.
2. Rufen Sie die Adresse auf.
3. Füllen Sie das Formular aus und schicken Sie es ab.

17 Copyright

Copyright © 2008 Sophos Group. 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 und Sophos Anti-Virus sind eingetragene Marken der Sophos Plc und der Sophos Group. Alle anderen erwähnten Produkt- und Unternehmensnamen sind Marken oder eingetragene Marken der jeweiligen Inhaber.

Für einige Softwareprogramme wird Benutzern gemäß GNU General Public License (GPL) oder ähnlichen Lizenzen für kostenlose Software eine Lizenz oder Unterlizenz gewährt, die ihnen unter anderem das Recht geben, bestimmte Programme oder Teile von Programmen zu kopieren, zu verändern oder weiterzuverbreiten und Zugriff auf den Quellcode geben. Die GPL bestimmt, dass für unter der GPL lizenzierte Software, die an Benutzer in einem ausführbaren Binärformat verteilt wird, diesen Benutzern der Quellcode ebenfalls zur Verfügung gestellt werden muss. Für diese Art von Software, die mit diesem Sophos Produkt geliefert wird, steht der Quellcode per Postversand zur Verfügung. Richten Sie dazu eine Anfrage an Sophos:

E-Mail: savlinuxgpl@sophos.com

Postanschrift: Sophos Plc, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, Großbritannien.

Eine Kopie der GPL Bestimmungen steht unter www.gnu.org/copyleft/gpl.html zum Abruf bereit.

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:

1. 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.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

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.

Python

PYTHON SOFTWARE FOUNDATION LICENSE VERSION 2

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

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)

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 © 1998–2006 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:

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

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

4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

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

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

This product includes cryptographic software written by Eric Young (ey@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:

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

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

The word “cryptographic” can be left out if the routines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

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

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

The licence 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 licence [including the GNU Public Licence.]

TinyXML XML parser

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:

1. 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.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

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:

1. 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.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. 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.

Copyright and licensing information for ACE™, TAO™, CIAO™, and CoSMIC™

ACE¹, TAO², CIAO³, and CoSMIC⁴ (henceforth referred to as “DOC software”) are copyrighted by Douglas C. Schmidt⁵ and his research group⁶ at Washington University⁷, University of California⁸, Irvine, and Vanderbilt University⁹, 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 us¹¹ know so we can promote your project in the DOC software success stories¹².

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 companies¹³ 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 ACE¹⁴, TAO¹⁵, CIAO¹⁶, and CoSMIC¹⁷ web sites are maintained by the DOC Group¹⁸ at the Institute for Software Integrated Systems (ISIS)¹⁹ and the Center for Distributed Object Computing of Washington University, St. Louis²⁰ for the development of open-source software as part of the open-source software community²¹. 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 acknowledge that 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 me²² know.

Douglas C. Schmidt²³

The ACE home page is <http://www.cs.wustl.edu/ACE.html>

Quellen

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

Index

A

Archive, On-Demand-Überprüfung 8
 Ausführbare UNIX-Dateien,
 On-Demand-Überprüfung 10
 Ausschließen von Objekten von der
 On-Demand-Überprüfung 9

B

Backups überprüfter Dateien 33
 Befehlszeilenbenachrichtigung 11
 Benachrichtigungen
 Befehlszeile 11
 E-Mail 26
 Bereinigen infizierter Dateien 13
 Bereinigung, Informationen 12

C

Computer, On-Demand-Überprüfung 5

D

Dateisysteme, On-Demand-Überprüfung 5, 9
 Dateitypen, On-Demand-Überprüfung 7, 10
 Desinfizieren bestimmter Dateien 13

E

E-Mail-Benachrichtigungen 26
 Ebenen 19

F

Fehlercodes 5

I

Infizierte Dateien
 Bereinigung 13
 Desinfizieren 13
 Isolieren 12
 Löschen 13
 Isolieren infizierter Dateien 12

K

Konfiguration am Einzelplatz 20
 Konfiguration im Netzwerk 17
 Konfiguration über zentrales
 Installationsverzeichnis 17

L

Langsame On-Demand-Überprüfungen 33
 Löschen infizierter Dateien 13

M

man page not found 32

O

On-Demand-Überprüfung
 Archive 8
 Ausführbare UNIX-Dateien 10
 Ausschließen von Objekten 9
 Computer 5
 Dateisysteme 5, 9
 Dateitypen 7, 10
 definiert 5
 Remote-Computer 9
 Symbolisch verknüpfte Objekte 9
 Verzeichnisse und Dateien 5

P

Protokoll, Sophos Anti-Virus
 Abrufen 15
 Konfigurieren 28

R

Remote-Computer, On-Demand-Überprüfung 9

S

savconfig, Überblick 20
 savsetup, Überblick 21
 Sophos Anti-Virus-Protokoll
 Abrufen 15
 Konfigurieren 28
 Speicherplatz auf Festplatte nicht genug 32
 Spyware
 Analyse 12

Spyware (*Fortsetzung*)

erkannt 11, 27

Fragment gemeldet 34

nicht beseitigt 33

Symbolisch verknüpfte Objekt,

On-Demand-Überprüfung 9

U

Updates

Konfigurieren 29

sofortige 16

V

Verzeichnisse und Dateien,

On-Demand-Überprüfung 5

Virus

Analyse 12

erkannt 11, 27

Fragment gemeldet 34

nicht beseitigt 33

Schäden 14

Z

Zeitgesteuerte Überprüfungen 22