

# SOPHOS

## Sophos Control Center Hilfe

Produktversion: 4.1  
Stand: März 2010



# Inhalt

1 Sophos Control Center.....	3
2 Einführung in Sophos Control Center.....	4
3 Überprüfen des Netzwerkschutzes.....	8
4 Schützen neuer Computer.....	10
5 Updates.....	12
6 Bearbeiten von Alerts und Threats.....	14
7 Erneuter Schutz von Computern.....	17
8 Überwachen geschützter Computer.....	18
9 Ereignisanzeige.....	21
10 Konfigurieren eines Scans.....	24
11 Konfigurieren von Updates.....	33
12 Konfigurieren der Firewall.....	36
13 Konfigurieren von Application Control.....	39
14 Konfigurieren von Device Control.....	42
15 Verwalten von Benachrichtigungen.....	45
16 Report-Verwaltung.....	49
17 Fehlersuche.....	54
18 Technischer Support.....	55
19 Copyright.....	56

# 1 Sophos Control Center

Sophos Sophos Control Center bietet folgende Optionen:

- Installation von Antiviren- und Firewall-Software im Netzwerk.  
Die Firewall ist im Lizenzumfang von Sophos Security Suite und Sophos Computer Security, jedoch nicht von Sophos Anti-Virus, enthalten.
- Automatische Software-Updates aus dem Internet.
- Zentrale Konfiguration der Erkennung und Bereinigung von Viren, Würmern, Trojanern, Spyware und potenziell unerwünschten Anwendungen (z.B. Adware, Dialer, Tools für Remote-Administration und Hacking Tools).
- Kontrolle der Anwendungen, die im Netzwerk ausgeführt werden dürfen.
- Verhindern, dass Benutzer nicht zugelassene Geräte auf Endpoints ausführen.
- Zentrale Konfiguration der Firewall sowie von Application Control und Device Control für die Computer im Netzwerk.
- Überwachung des Netzwerks zur Sicherstellung, dass Computer geschützt sind und der zentralen Konfiguration entsprechen.
- Übersicht über die Threats.
- Erstellung von Reports zu den neuesten Threats.

Folgende Systeme werden von Sophos Control Center unterstützt:

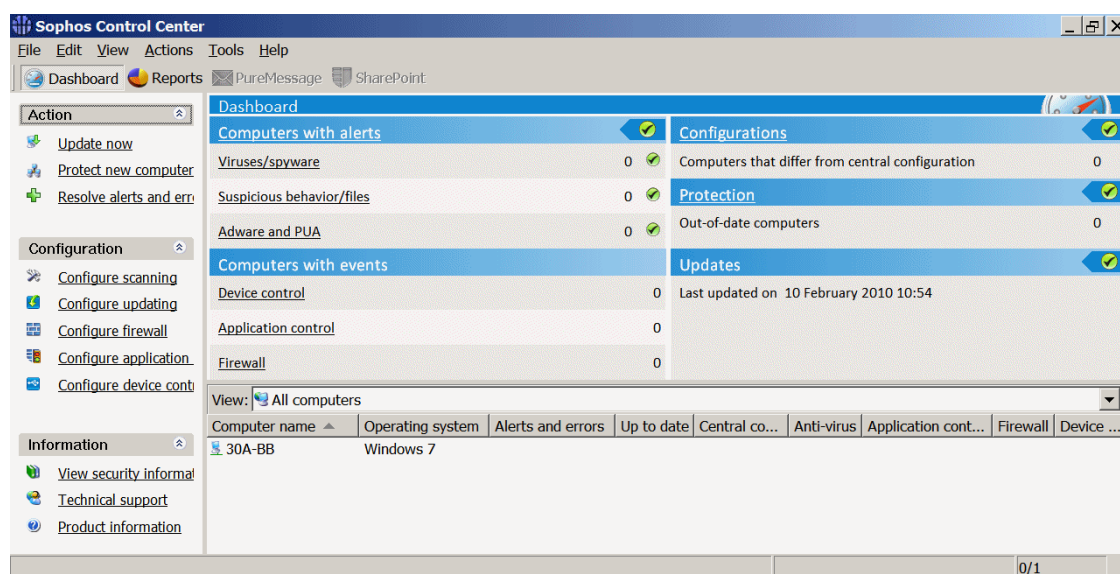
- Windows 2000 und höher
- Windows 98 (SE)
- Mac OS X

**Hinweis:** Sophos Control Center, Version 4.1, unterstützt Windows 7 und Windows Server 2008 R2.

## 2 Einführung in Sophos Control Center

### 2.1 Die Benutzeroberfläche

Sie können Sophos Anti-Virus und Sophos Client Firewall über die Benutzeroberfläche (das aktuelle Fenster auf dem Bildschirm) von Sophos Control Center verwenden und konfigurieren. Die Hauptfunktionen werden im Folgenden ausgeführt.



#### Menü „Maßnahme“

Über das Menü können Sie Sophos Anti-Virus und die Firewall (falls vorhanden) updaten, neue Computer schützen und Threats beheben.

#### Menü „Konfiguration“

Mit diesem Menü können Sie Sophos Anti-Virus und Firewall zur Ausgabe von Threat-Alerts konfigurieren.

#### Menü „Informationen“

Über dieses Menü können Sie auf die Threat-Beschreibungen auf der Sophos Website zugreifen und Sie erhalten Informationen zum technischen Support und den Produkten.

#### Symbolleiste

##### ■ Reports

Klicken Sie auf die Schaltfläche „Reports“. Das Fenster **Report Manager** wird geöffnet. Anweisungen zur Reporterstellung entnehmen Sie bitte dem Abschnitt *Erstellen eines Reports* (Seite 49).

##### ■ PureMessage

Wenn Sie PureMessage nutzen, können Sie die die PureMessage-Konsole über diese Schaltfläche aufrufen. Dies ist jedoch nur möglich, wenn die PureMessage-Konsole auf dem gleichen Computer wie Sophos Control Center installiert ist.

#### ■ **SharePoint**

Wenn Sie Sophos für Microsoft SharePoint nutzen, können Sie das Programm über diese Schaltfläche aufrufen. Hierzu muss Sophos für Microsoft SharePoint auf dem gleichen Computer wie Sophos Control Center installiert sein.

### **Dashboard**

Das **Dashboard** zeigt den Sicherheitsstatus des Netzwerks auf einen Blick an. Zum Ein- oder Ausblenden des Dashboards klicken Sie in der Symbolleiste auf **Dashboard**. Weitere Informationen finden Sie unter [Die Dashboard-Ansicht](#) (Seite 8).

### **Die Computerliste**

Die Computerliste gibt Aufschluss darüber,

- ob Sophos Anti-Virus und die Firewall aktiv, inaktiv oder nicht installiert sind.
- ob die Computer der über Sophos Control Center zentral vorgenommenen Konfiguration entsprechen.
- wo Alerts auftreten.

Die Symbole in der Computerliste werden im Abschnitt [Erklärung der Symbole](#) (Seite 5) erläutert.

Wenn Sie die Computerliste nach einer Spalte sortieren möchten, klicken Sie auf die Überschrift der gewünschten Spalte.


Doppelklicken Sie zum Aufrufen der **Computer-Details** (z.B. Version, Status von Anti-Virus, Firewall, ausstehende Alerts und Threat-Erkennungsverlauf) auf die Computerliste und das entsprechende Fenster wird geöffnet. Sie können jedoch auch einen Computer markieren, darauf rechtsklicken und die Option **Computer-Details** auswählen.


## **2.2 Erklärung der Symbole**

Die Symbole in der Computerliste weisen auf Folgendes hin:




- Alerts
- Schutz deaktiviert oder nicht auf dem neuesten Stand
- Status aller Computers (z.B. Software wird installiert)

#### **Alerts**







Symbol	Beschreibung
	Ein rotes Warnsymbol in der Spalte <b>Alerts und Fehler</b> deutet darauf hin, dass ein Virus, Wurm, Trojaner, Spyware oder verdächtiges Verhalten erkannt wurde.

Symbol	Beschreibung
	<p>Ein gelbes Warnsymbol in der Spalte <b>Alerts und Fehler</b> deutet auf eines der folgenden Probleme hin:</p> <ul style="list-style-type: none"> <li>■ Eine verdächtige Datei wurde erkannt.</li> <li>■ Adware oder eine andere potenziell unerwünschte Anwendung wurde erkannt.</li> <li>■ Ein Fehler ist aufgetreten.</li> </ul> <p>Ein gelbes Warnsymbol in der Spalte <b>Zentrale Konfiguration</b> zeigt an, dass ein Computer im Gegensatz zu den anderen Netzwerkcomputern von der zentralen Konfiguration abweicht.</p>



### Schutz deaktiviert oder nicht auf dem neuesten Stand

Symbol	Beschreibung
	Ein graues Schildsymbol und der Text „inaktiv“ in der Spalte <b>Anti-Virus</b> der Computerliste zeigen an, dass die On-Access-Scanfunktion deaktiviert wurde.
	Ein graues Firewall und der Text „inaktiv“ in der Spalte <b>Firewall</b> weist darauf hin, dass die Firewall deaktiviert wurde.
	Ein Uhrensymbol und der Text „Nein“ in der Spalte <b>Auf dem neuesten Stand</b> zeigt an, dass sich die Software nicht auf dem neuesten Stand befindet.

### Computerstatus

Symbol	Beschreibung
	Ein blaues Computer-Symbol bedeutet, dass der Computer von Sophos Control Center verwaltet wird.
	Ein Computer-Symbol mit einem gelben Pfeil bedeutet, dass die Installation von Virenschutz- und Firewall-Software aussteht.
	Ein Computer-Symbol mit einem grünen Pfeil bedeutet, dass die Installation derzeit ausgeführt wird.
	Ein Computer-Symbol mit einer Sanduhr weist darauf hin, dass die Update-Komponente von Sophos Anti-Virus installiert wurde und nun die neueste Version des Produkts herunterlädt.
	Ein graues Computer-Symbol bedeutet, dass der Computer nicht von Sophos Control Center verwaltet wird.
	Ein Computer-Symbol mit einem roten Kreuz bedeutet, dass der Computer nicht angeschlossen ist.

## Dashboard-Status

Symbol	Beschreibung
	Eine grünes Symbol entspricht dem „normalen“ Status. Die Anzahl der betroffenen Computer liegt unter dem Schwellenwert.
	Ein rotes Symbol weist darauf hin, dass der Schwellenwert in der entsprechenden Kategorie überschritten wurde.

## 2.3 Priorität von Alerts

Wenn für einen Computer mehrere Alerts vorhanden sind, wird in der Computerliste das Symbol des Alerts mit der höchsten Priorität angezeigt. Nachfolgend werden Alert-Typen nach Priorität in absteigender Reihenfolge aufgelistet.

1. Virus-/Spyware-Alert
2. Alerts bei verdächtigem Verhalten
3. Alerts bei verdächtigen Dateien
4. Adware-/PUA-Alerts
5. Software-Anwendungsfehler (beispielsweise Installationsfehler)

## 3 Überprüfen des Netzwerkschutzes

### 3.1 Die Dashboard-Ansicht

Mit dem Dashboard können Sie den Sicherheitsstatus des Netzwerks überprüfen. Zum Ein- oder Ausblenden des Dashboards klicken Sie in der Symbolleiste auf **Dashboard**.

Dashboard	
<b>Computers with alerts</b> (0 alerts, green checkmark)	<b>Configurations</b> (1 warning, red exclamation mark)
<u>Viruses/spyware</u> 0 (green checkmark)	Computers that differ from central configuration 1
<u>Suspicious behavior/files</u> 0 (green checkmark)	<b>Protection</b> (1 warning, red exclamation mark)
<u>Adware and PUA</u> 0 (green checkmark)	Out-of-date computers 1
<b>Computers over event threshold</b> (0 alerts, green checkmark)	<b>Updates</b> (1 update, green checkmark)
<u>Device control</u> 0 (green checkmark)	Last updated at Not available
<u>Application control</u> 0 (green checkmark)	
<u>Firewall</u> 0 (green checkmark)	

Das Dashboard setzt sich aus fünf Abschnitten zusammen, in denen auf Basis der jeweiligen Schwellenwerte Statusanzeigen erscheinen:

#### Computer mit Alerts

In diesem Abschnitt wird die Anzahl verwalteter Computer mit Alerts über Folgendes angezeigt:

- Bekannte und unbekannte Viren und Spyware
- Verdächtiges Verhalten und verdächtige Dateien
- Adware und andere potenziell unerwünschte Anwendungen

Klicken Sie zum Aufrufen einer Liste verwalteter Computer mit ausstehenden Alerts auf **Computer mit Alerts**.

#### Computer über Ereignis-Grenzwert

In diesem Abschnitt werden die Anzahl der Ereignisse in Zusammenhang mit Device Control, kontrollierten Anwendungen und von der Firewall blockierten Anwendungen sowie entsprechende Statusanzeigen für die einzelnen Kategorien angezeigt.

#### Konfigurationen

In diesem Abschnitt wird die Anzahl der von der zentralen Konfiguration abweichenden verwalteten Computer angezeigt.

Klicken Sie zur Anzeige einer Liste verwalteter Computer, die von der zentralen Konfiguration abweichen, auf **Richtlinien**.

## Schutz

In diesem Abschnitt werden die Anzahl verwalteter und verbundener Computer angezeigt, auf denen Sophos Anti-Virus nicht aktuell ist oder die unbekannte Erkennungsdaten verwenden.

Klicken Sie zur Anzeige einer Liste verwalteter Computer, die sich nicht auf dem neuesten Stand befinden, auf **Schutz**.

## Updates

In diesem Bereich wird das Datum und die Uhrzeit des letzten Updates von Sophos angezeigt.

## 3.2 Konfiguration des Dashboards

Das Dashboard bietet eine Statusanzeige auf der Basis des Prozentsatzes der verwalteten Computer, auf denen Alerts oder Fehler ausstehen, oder der Zeit, die seit dem letzten Update von Sophos verstrichen ist. Die Statusanzeige ändert sich, wenn ein bestimmter Schwellenwert überschritten wurde.

So können Sie die Statusanzeige im Dashboard konfigurieren:

1. Wählen Sie im Menü **Extras** die Option **Dashboard konfigurieren**.

Das Dialogfeld **Dashboard konfigurieren** wird angezeigt.

2. Ändern Sie bei Bedarf die Schwellenwerte im Textfeld „Stufe“.
  - a) Geben Sie im Bereich **Computer mit ausstehenden Alerts** an, bei wie viel Prozent der verwalteten Computer ein bestimmtes Problem auftreten muss, bis sich die entsprechende Statusanzeige ändert.
  - b) Geben Sie im Feld **Computer mit Ereignissen** an, nach wie vielen Ereignissen eine Warnung ausgegeben werden soll.
  - c) Geben Sie im Feld **Konfiguration und Schutz** an, wie viel Prozent der verwalteten Computer von einem Problem betroffen sein müssen, bis sich die entsprechende Anzeige ändert.
  - d) Geben Sie im Bereich **Neuester Schutz von Sophos** die Anzahl der seit dem letzten Update von Sophos verstrichenen Stunden an. In Abhängigkeit der Stundenzahl ändert sich die Update-Anzeige.
  - e) Klicken Sie auf **OK**.

Wenn Sie eine Stufe auf Null setzen, wird bei Empfang des ersten Alerts ein Warnhinweis ausgegeben.

Sie können einstellen, dass die von Ihnen ausgewählten Empfänger per E-Mail darüber benachrichtigt werden, wenn ein festgelegter Grenzwert erreicht wurde. Nähere Informationen hierzu finden Sie unter [Einrichten von Netzwerkstatus-E-Mail-Benachrichtigungen](#) (Seite 46).

## 4 Schützen neuer Computer

### 4.1 Schützen neuer Computer

Wenn neue Computer ins Netzwerk aufgenommen werden, müssen sie durch Antiviren- und (falls vorhanden) Firewallsoftware geschützt werden.

**Hinweis:** Die automatische Installation und automatische Upgrades erfolgen nur auf Computern unter Windows 2000 und höher, nicht jedoch unter Windows 98 oder Mac OS X.

Wenn das Betriebssystem einiger Ihrer Computer von einem bereits verwendeten Betriebssystem abweicht (die Computer also etwa unter Windows 98 oder Mac OS X laufen), befolgen Sie die Anweisungen im Abschnitt *Schützen neuer Betriebssysteme* (Seite 11).

So können Sie neue Computer schützen:

1. Rufen Sie in Sophos Control Center das Menü **Maßnahmen** auf und klicken Sie auf **Neue Computer schützen**.

Der **Sophos Assistent zum Schutz von Netzwerken** wird gestartet.

2. Geben Sie auf der Seite **Windows-Benutzerkonto** die Daten eines Administratorkontos an, über das Software auf den Computern im Netzwerk installiert werden kann.
3. Warten Sie bei Anzeige der Seite **Computer schützen**, bis die Computer erkannt wurden.

Wählen Sie in der Spalte **Schützen** die gewünschten Computer aus und klicken Sie auf **Weiter**.

4. Wählen Sie auf der Seite **Funktionen auswählen** die Komponenten aus, die auf den Computern installiert werden sollen.

- Die Antivirensoftware wird standardmäßig installiert.
- Wenn Sie die Firewall installieren möchten, aktivieren Sie das Kontrollkästchen **Firewall**.

Sophos Client Firewall kann nur auf Arbeitsplatzrechnern unter Windows 2000 und höher, nicht jedoch auf Serverbetriebssystemen installiert werden. Zur Installation der Firewall muss Sophos Anti-Virus installiert worden sein.

**Hinweis:** Alle Computer müssen neu gestartet werden, damit Sophos Client Firewall installiert und aktiviert werden kann.

- Wenn Fremdsoftware bei der Installation entfernt werden soll, aktivieren Sie das Kontrollkästchen **Fremdsoftware entfernen**.

5. Wenn Computer in der Liste **Computer, die manuell geschützt werden müssen** aufgeführt werden, klicken Sie auf **Drucken**: Eine Liste der ungeschützten Computer wird ausgedruckt.

Sie können die Liste auch durch Klicken auf **Speichern unter** speichern oder sich die Namen der Computer aufschreiben.

6. Klicken Sie auf der letzten Seite des Assistenten auf **Beenden**

Nach dem Schließen des Assistenten installiert Sophos Control Center die Software automatisch auf so vielen markierten Computern wie möglich. Die Computer werden in Sophos Control Center mit Informationen zu ihrem Status aufgelistet.

7. Gehen Sie zu allen Computern auf der Liste der ungeschützten Computer und installieren Sie die Software manuell.

Weitere Informationen zur manuellen Installation können Sie der Startup-Anleitung zu Sophos Control Center entnehmen.

## 4.2 Schützen neuer Betriebssysteme

Wenn ein Computer eines neuen Typs in Ihr Netzwerk aufgenommen wird (z.B. beim ersten Hinzufügen von Computern unter Windows 98 oder Mac OS X), muss der Download von Antiviren-Software für diesen Computertyp in Sophos Control Center aktiviert werden.

Sophos Endpoint Security and Control kann auf Computern unter Windows 2000 oder höher installiert werden.

So können Sie Computer mit neuen Betriebssystemen schützen:

1. Klicken Sie auf der linken Seite unter **Konfiguration** auf **Updates konfigurieren**.
2. Rufen Sie im Fenster **Updates konfigurieren** die Registerkarte **Software** auf und wählen Sie das Betriebssystem/die Betriebssysteme aus, die geschützt werden sollen.
3. Rufen Sie wieder das Hauptfenster von Sophos Control Center auf. Klicken Sie im Menü **Maßnahme** auf **Jetzt updaten**.
4. Gehen Sie zu allen Computern des neuen Typs und installieren Sie die Software. Anweisungen hierzu entnehmen Sie bitte der *Sophos Control Center Startup-Anleitung*.

## 5 Updates

### 5.1 Erklärung der Update-Funktion

Sophos Control Center sucht alle 60 Minuten nach Sophos Updates und lädt diese ggf. herunter.

Die aktualisierte Software steht auf dem Computer zur Verfügung, auf dem Sophos Control Center ausgeführt wird. Von Sophos Control Center verwaltete Computer werden automatisch (standardmäßig alle 5 Minuten) über diese zentral verwaltete Version upgedatet.

Im Dashboard von Sophos Control Center wird angezeigt, wann das letzte Update von Sophos heruntergeladen wurde.

### 5.2 War das Update erfolgreich?

Sicherheitssoftware wird in zwei Schritten aktualisiert:

1. Sophos Control Center lädt Updates von Sophos herunter.
2. Die Netzwerkcomputer werden über Ihren Server upgedatet.

Wenn ein Schritt nicht durchgeführt werden kann, wird folgende Meldung angezeigt:

#### ■ Sophos Control Center kann keine Updates herunterladen

Wenn der Download nicht möglich ist, wird im Dashboard von Sophos Control Center eine Fehlermeldung angezeigt. Auf Wunsch können Sie sich darüber benachrichtigen lassen. Nähere Informationen hierzu finden Sie unter [Einrichten von Netzwerkstatus-E-Mail-Benachrichtigungen](#) (Seite 46).

#### ■ Computer updaten sich nicht

In der Computerliste wird in der Spalte **Auf dem neuesten Stand** neben allen Computern, die sich nicht auf dem neuesten Stand befinden, „Nein“ angezeigt. Wenn Sie ein Update erzwingen möchten, markieren Sie den gewünschten Computer und rechtsklicken Sie darauf. Klicken Sie im Menü auf **Computer jetzt updaten**.

### 5.3 Einrichten von Benachrichtigungen zum letzten Update

Sie können Sophos Control Center so konfigurieren, dass Sie bei Problemen mit dem Download von Updates von Sophos benachrichtigt werden.

Verfahren Sie hierzu wie folgt:

1. Wählen Sie im Menü **Extras** die Option **E-Mail-Benachrichtigungen konfigurieren**.
2. Klicken Sie im Dialogfeld **E-Mail-Benachrichtigungen konfigurieren** auf **Konfigurieren** und machen Sie die erforderlichen Angaben zu Ihrem SMTP-Server.
3. Klicken Sie auf **Hinzufügen** und geben Sie die E-Mail-Adresse ein. Wählen Sie dann die Sprache aus, in der die Benachrichtigungen verfasst werden sollen.

4. Stellen Sie sicher, dass im Bereich **Abonnements** unter **Stufe überschritten** die Option **Zeit seit dem letzten Update von Sophos** aktiviert ist und klicken Sie anschließend auf **OK**.

## 5.4 Manuelle Updates

Auf Wunsch können Sie Ihre Sicherheitssoftware manuell aktualisieren.

So können Sie die Sicherheitssoftware manuell aktualisieren:

1. Klicken Sie im Menü **Maßnahme** auf **Jetzt updaten**.
2. In Sophos Control Center werden Sie durch eine Meldung dazu aufgefordert, den Update-Vorgang zu bestätigen. Klicken Sie auf **Ja**.

Sophos Control Center stellt eine Verbindung zu Sophos her und lädt die aktuelle Version der Antiviren- und (bei entsprechender Auswahl) Firewallsoftware herunter. Bei der nächsten Updatesuche in Ihrem Server führen die Netzwerkcomputer automatisch ein Update durch.

## 5.5 Updaten von Einzelcomputern

Wenn angezeigt wird, dass sich ein Computer nicht auf dem neuesten Stand befindet (in der Spalte **Auf dem neuesten Stand** steht „Nein“), können Sie ein Update erzwingen.

- ❖ Markieren Sie den gewünschten Computer in der Computerliste und rechtsklicken Sie darauf. Klicken Sie im Menü auf **Computer jetzt updaten**.

## 6 Bearbeiten von Alerts und Threats

### 6.1 Vorgehensweise bei Threats

Ein Threat wurde in Ihrem Netzwerk erkannt, jedoch noch nicht automatisch bereinigt:

- Sophos Control Center gibt einen Alert aus, sofern Scan-Alerts aktiviert sind. Nähere Informationen hierzu finden Sie unter [Einrichten von Antivirus- und HIPS-Benachrichtigungen](#) (Seite 45).
- In der Computerliste von Sophos Control Center wird ein Alert-Symbol zusammen mit dem Namen des infizierten Computers angezeigt. Die Ursache des Alerts können Sie wie folgt ermitteln: Markieren Sie den Computer in der Computerliste, rechtsklicken Sie darauf und wählen Sie die Option **Computer-Details**. Weitere Informationen zu den Alert-Symbolen finden Sie unter [Erklärung der Symbole](#) (Seite 5).
- In Sophos Control Center wird im **Dashboard** die Gesamtanzahl der im Netzwerk erkannten Viren und Spyware angezeigt.

### 6.2 Computer-Bereinigung

Verfahren Sie bei erkannten Threats, Viren, Spyware und PUA wie folgt:

1. Klicken Sie im Menü **Maßnahme** auf **Alerts und Fehler löschen**.  
Sie können jedoch auch auf die Links zu den jeweiligen Alert-Arten im Dashboard klicken.  
Das Dialogfeld **Alerts und Fehler löschen** wird angezeigt.
2. Rufen Sie die Registerkarte **Alerts** auf und wählen Sie eine Option im Dropdown-Menü **Anzeigen** aus.  
In den Spalten werden die gewählten Informationen zu den betroffenen Computern angezeigt (z.B. Name des infizierten Computers, Zeitpunkt (Datum und Uhrzeit) der Erkennung des ersten Threats, Alert-Art, Alert-Status usw.)
3. Je nach Auswahl wird in der **Status**-Spalte Folgendes angezeigt:
  - **Bereinigung möglich**  
Bereinigen Sie die infizierten Objekte über die Schaltfläche **Bereinigung**, wie nachfolgend beschrieben.
  - **Bereinigung nicht möglich**  
Wenn angezeigt wird, dass Objekte nicht in Sophos Control Center bereinigt werden können, muss die Bereinigung auf dem betroffenen Computer manuell erfolgen. Wenn der Threat nicht entfernt wurde, finden Sie im Abschnitt [Bereinigung fehlgeschlagen](#) (Seite 54) weitere Unterstützung.
  - **Bereinigung wird durchgeführt (Start <Zeit>)**  
Zeigt an, dass die Bereinigung eingeleitet wurde

- **Zeit für Bereinigung abgelaufen (Beginn <Zeit>)**  
Zeigt an, dass die Zeit bei der Bereinigung überschritten wurde und der Threat eventuell nicht beseitigt wurde. Dieses Problem kann auftreten, wenn der Computer nicht mit dem Netzwerk verbunden ist. Überprüfen Sie, ob der Computer mit dem Netzwerk verbunden ist und wiederholen Sie die Bereinigung.
- **Neustart erforderlich**  
Zeigt an, dass der Alert teilweise bereinigt wurde, die Bereinigung jedoch erst nach einem Neustart abgeschlossen werden kann.
- **Vollständige Systemüberprüfung erforderlich**  
Zeigt an, dass der Alert zwar möglicherweise beseitigt werden kann. Die Bereinigung jedoch nur nach einer vollständigen Systemüberprüfung abgeschlossen werden kann.
- **Bereinigung fehlgeschlagen**  
Zeigt an, dass ein Alert nicht bereinigt werden kann. Unter Umständen ist eine manuelle Bereinigung erforderlich.
- **Threat-Typ kann nicht bereinigt werden**  
Zeigt an, dass ein Objekt nicht bereinigt werden kann, weil der Alert-Typ nicht bereinigbar ist.

4. Folgende Optionen sind vorhanden:

- **Alles markieren/aufheben**  
Klicken Sie auf diese Schaltflächen, um alle Objekte auszuwählen oder abzuwählen. Dadurch kann eine Maßnahme für eine Objektgruppe übernommen werden. Klicken Sie zum Auswählen bzw. Abwählen eines Objekts auf das Kontrollkästchen links neben dem Objektnamen.
- **Löschen**  
Klicken Sie auf diese Option, um die ausgewählten Objekte aus der Liste zu entfernen. Die Objekte werden dabei nicht von der Festplatte gelöscht.
- **Bereinigung**  
Klicken Sie hierauf, um Threats, Viren, Spyware oder PUA auf den ausgewählten Computern zu löschen.

**Hinweis:** Ersetzen Sie die bereinigten Programme durch eine Kopie vom Original-Datenträger oder eine virenfreie Sicherungskopie.

Wenn unterschiedliche Threats vorhanden sind, wird empfohlen, zunächst eine vollständige Systemüberprüfung der Computer durchzuführen, um alle Threat-Komponenten zu ermitteln. In [Scannen von Computern zu bestimmten Zeiten](#) (Seite 29) wird erläutert, wie Sie Scans zu festen Zeiten einrichten können.

Bei Threats, die aus mehreren Komponenten bestehen, wird die Bereinigung unter Umständen erst nach einem Neustart wirksam. Wenn dies der Fall ist, wird der Benutzer durch eine Meldung aufgefordert, sofort oder später einen Neustart durchzuführen. Die abschließenden Bereinigungsschritte werden nach dem Neustart durchgeführt.

**Hinweis:** Wenn bei der Bereinigung eines Threats auf einem Computer nicht binnen einer Stunde (ab dem Zeitpunkt, zu dem die Anweisung zum Ausführen der Maßnahme von Sophos Control Center an den Computer gesendet wurde) eine Reaktion erfolgt, wird die Maßnahme als „fehlgeschlagen“ ausgewiesen.

## 6.3 Abrufen von Threat-Daten

Sie können Informationen zu den Auswirkungen erkannter Threats und ihrer Bereinigung abrufen.

So finden Sie die Threat-Daten:

1. Markieren Sie in Sophos Control Center in der Computerliste den Computer, auf dem der Threat erkannt wurde, rechtsklicken Sie darauf und wählen Sie die Option **Computer-Details**.
2. Navigieren Sie im Fenster **Computer-Details** zur Option **Ausstehende Alerts und Fehler** und klicken Sie auf den Threat-Namen.

Sophos Control Center stellt eine Verbindung zur Threat-Analyse auf der Sophos Website her.

Sie können die Sophos Website jedoch auch direkt aufrufen und dort zur gewünschten Threat-Analyse navigieren. Klicken Sie hierzu im **Hilfe**-Menü auf **Objekt-Infos**.

## 6.4 Umgang mit Fehler-Alerts

Auf der Registerkarte **Fehler** finden Sie Informationen zu Scan- und Firewall-Fehlern der letzten 30 Tage. Der Name des betroffenen Computers, der Zeitpunkt (Datum und Uhrzeit), zu dem der Fehler aufgetreten ist, die Fehlerart, der Fehlercode und eine Fehlerbeschreibung werden angezeigt.

So können Sie Anti-Virus- und Firewall-Fehler verarbeiten:

1. Klicken Sie im Menü **Maßnahme** auf **Alerts und Fehler löschen**.
2. Klicken Sie im Fenster **Alerts und Fehler löschen** auf die Registerkarte **Fehler**.
3. Folgende Optionen sind vorhanden:
  - **Alles markieren/aufheben**

Klicken Sie auf diese Schaltflächen, um alle Objekte auszuwählen oder abzuwählen. Dadurch kann eine Maßnahme für eine Objektgruppe übernommen werden. Klicken Sie zum Auswählen bzw. Abwählen eines Objekts auf das Kontrollkästchen links neben dem Objektnamen.
  - **Löschen**

Durch Klicken auf diese Option werden Fehler als erledigt markiert. Erledigte Alerts werden nicht mehr angezeigt.

## 7 Erneuter Schutz von Computern

### 7.1 Erneuter Schutz von Computern

Sie können die ursprünglich installierte Antiviren- und (falls vorhanden) Firewallsoftware auf beliebigen Computern im Netzwerk erneut installieren.

So wird der Computerschutz wiederhergestellt:

1. Markieren Sie in der Computerliste die Computer, auf denen die Software erneut installiert werden soll.
2. Öffnen Sie das Menü **Extras** und wählen Sie **Computer erneut schützen**.

Der **Assistent zum erneuten Schützen von Computern** wird geöffnet. Der Assistent leitet sie durch den Neuinstallationsvorgang.

Weitere Informationen zum manuellen Schutz von Computern können Sie der **Startup-Anleitung** zu *Sophos Control Center* entnehmen.

## 8 Überwachen geschützter Computer

### 8.1 Ermitteln von der zentralen Konfiguration entsprechenden Computern

Mit Sophos Control Center können Sie zentral eine Gruppe von Einstellungen erstellen (z.B. für Updates) und auf die Endpoints übertragen. Dies wird als zentrale Konfiguration bezeichnet.

Sie können prüfen, ob die Computer der in Sophos Control Center vorgenommenen zentralen Konfiguration der Antiviren-Software, der Update-Funktion sowie von Application und Device Control entsprechen:

Betrachten Sie die Computerliste. Wenn in der Spalte **Zentrale Konfiguration OK** steht, entspricht der Computer der zentralen Konfiguration.

- Wenn ein Computer von der zentralen Konfiguration abweicht (z.B. die Konfiguration wurde am Computer selbst geändert und der Computer wird nicht als lokal in Sophos Control Center konfiguriert angezeigt), wird in der Spalte **Zentrale Konfiguration** ein gelbes Warnsymbol sowie der Text „Geändert“ angezeigt.
- Wenn auf einem bestimmten Computer keine Sicherheitssoftware installiert wurde, wird in der Spalte **Zentrale Konfiguration** für den entsprechenden Computer kein Status angezeigt. Wenn die Software lokal konfiguriert wurde, wird „Lokal konfiguriert“ angezeigt. Wenn die zentrale Konfiguration eines Computers über Sophos Control Center ansteht, wird in der Spalte „Ausstehend“ angezeigt.

Wenn Sie die zentrale Konfiguration auf einem Computer wiederherstellen möchten, markieren Sie den Computer, rechtsklicken Sie darauf und wählen Sie **Zentrale Konfiguration wiederherstellen**.

### 8.2 Ermitteln der lokal konfigurierten Computer

Verfahren Sie wie folgt, um zu ermitteln, auf welchen Computern die Antiviren- und Firewallsoftware lokal konfiguriert wird:

- **Anzeige der lokal konfigurierten Computer**

Verfahren Sie hierzu wie folgt:

Wählen Sie im Dropdown-Menü **Ansicht** die Option **Lokal konfigurierte Computer**.

- **Prüfen von Einzelcomputern**

Wenn Sie überprüfen möchten, ob ein Einzelcomputer lokal konfiguriert wird, rechtsklicken Sie auf den Computernamen. Wenn die Option **Zentrale Konfiguration übernehmen** nicht aktiviert ist, wird der Computer lokal konfiguriert.

## 8.3 Überprüfen des Computerschutzes

In Sophos Control Center wird eine Liste der Computer sowie deren Status angezeigt.

- Wenn in der Spalte **Auf dem neuesten Stand** „Ja“ steht, befindet sich der Computerschutz durch Sophos Produkte auf dem neuesten Stand. Bei Anzeige eines Uhrensymbols und des Texts „Nein“ befindet sich der Schutz nicht auf dem neuesten Stand.

Wenn Sie Computer danach sortieren möchten, ob sie sich auf dem neuesten Stand befinden oder nicht, klicken Sie auf die Überschrift der Spalte **Auf dem neuesten Stand**.

- Wenn in der Spalte **Anti-Virus** „Aktiv“ steht, werden On-Access-Scans ausgeführt. Ein graues Schildsymbol und der Text „Inaktiv“ weisen darauf hin, dass die On-Access-Scanfunktion deaktiviert ist.

**Hinweis:** Wenn die On-Access-Scanfunktion auf den Computern der Benutzer ausgeführt wird, muss sie auf einem Fileserver unter Windows 2000 oder 2003 in der Regel nicht aktiviert werden.

Wenn die Software auf dem Computer nicht installiert ist, wird in dieser Spalte der Text „Nicht installiert“ angezeigt.

- Wenn in der Spalte **Application Control** „Aktiv“ steht, ist Application Control auf dem Computer aktiviert. Ein graues Schildsymbol und der Text „Inaktiv“ weisen darauf hin, dass Application Control deaktiviert ist.
- Wenn in der Spalte **Firewall** „Aktiv“ steht, ist die Firewall aktiviert. Ein graues Firewall-Symbol und der Text „Inaktiv“ weisen darauf hin, dass die Firewall deaktiviert ist. Wenn die Software nicht auf dem Computer installiert ist, wird für den entsprechenden Computer kein Status angezeigt.

## 8.4 Auffinden von gelöschten Computern

Sie können Computer, die aus der Computerliste entfernt wurden, in Sophos Control Center auffinden.

Gelöschte Computer müssen als neue Computer gesucht werden. Informationen zum Auffinden von Computern entnehmen Sie bitte dem Abschnitt [Schützen neuer Computer](#) (Seite 10).

## 8.5 Anzeige von Computern nach Status

Sie können sich eine Liste der Computer auf der Basis ihres Status anzeigen lassen.

So können Sie einen Computer auf der Basis seines Status aufrufen:

- ❖ Öffnen Sie in Sophos Control Center das Dropdown-Menü **Ansicht** und wählen Sie einen Status aus. Der folgenden Tabelle bietet eine Übersicht:

Option	Beschreibung
Alle Computer	Anzeige einer Liste der Computer, die mit dem Netzwerk verbunden sind und von Sophos Control Center verwaltet werden.

Option	Beschreibung
<b>Computer mit Alerts und Fehlern</b>	Anzeige einer Liste der Computer mit Alerts. Die Ursache des Alerts können Sie wie folgt ermitteln: Markieren Sie den Computer in der Computerliste, rechtsklicken Sie darauf und wählen Sie die Option <b>Computer-Details</b> .
<b>Nicht verwaltete Computer</b>	Anzeige einer Liste der Computer, die nicht von Sophos Control Center verwaltet werden.
<b>Verwaltete Computer, die sich nicht auf dem neuesten Stand befinden</b>	Anzeige einer Liste der verwalteten Computer, deren Software sich nicht auf dem neuesten Stand befindet. Wenn Sie einen bestimmten Computer updaten möchten, rechtsklicken Sie auf den entsprechenden Eintrag in der Computerliste und wählen Sie die Option <b>Computer jetzt updaten</b> .
<b>Verwaltete Computer</b>	Anzeige einer Liste der Computer, die von Sophos Control Center verwaltet werden.
<b>Lokal konfigurierte Computer</b>	Anzeige einer Liste der Computer, die lokal konfiguriert werden. Wenn Sie einem Computer die zentrale Konfiguration wieder zuweisen möchten, rechtsklicken Sie auf den Namen des Computers und wählen Sie die Option <b>Zentrale Konfiguration übernehmen</b> .
<b>Verbundene Computer</b>	Anzeige einer Liste der verwalteten Computer, die verfügbar sind.
<b>Vom Netzwerk getrennte Computer</b>	Anzeige einer Liste der verwalteten Computer, die derzeit nicht verfügbar sind (z.B heruntergefahren wurden).

Wenn für einen Computer mehrere Alerts vorhanden sind, wird das Symbol des Alerts mit der höchsten Priorität angezeigt. Details zur Priorität der einzelnen Symbole entnehmen Sie bitte dem Abschnitt [Priorität von Alerts](#) (Seite 7).

## 8.6 Ausdrucken der Threat-Übersicht und der Computerliste

Sie können eine Übersicht der Threats auf dem Computer und der Computerliste für eine gewählte Ansicht ausdrucken.

Verfahren Sie hierzu wie folgt:

1. Klicken Sie in Sophos Control Center im Menü **Datei** auf **Drucken**.

Das Dialogfeld **Drucken** wird angezeigt.

2. Wählen Sie die gewünschten Druckeinstellungen aus und klicken Sie auf **OK**. Die Druckausgabe umfasst folgende Informationen:

- Unternehmensname
- Datum und Uhrzeit des Drucks
- Informationen, die in der Computerliste für die gewählte Ansicht angezeigt werden

## 9 Ereignisanzeige

### 9.1 Ereignisse

Application Control-, Firewall-, Data Control- und Device Control-Ereignisse auf einem Endpoint (z.B. die Firewall hat eine Anwendung blockiert) werden an Sophos Control Center übertragen und können in der jeweiligen Ereignisanzeige abgerufen werden.

Die Ereignisanzeige gibt Aufschluss über Fehler im Netzwerk. Zudem können Sie gefilterte Ereignislisten erstellen: z.B. eine Liste aller Application Control-Ereignisse, die in den letzten 24 Stunden von einem bestimmten Benutzer ausgelöst wurden.

Im Dashboard wird die Anzahl der Computer angezeigt, deren Ereignisanzahl in den letzten 24 Stunden einen festgelegten Höchstwert überschritten hat. Nähere Informationen zum Festlegen des Höchstwerts finden Sie im Abschnitt [Konfiguration des Dashboards](#) (Seite 9).

Sie können einstellen, dass die von Ihnen ausgewählten Empfänger bei Ereignissen benachrichtigt werden. Weitere Informationen finden Sie unter [Einrichten von Antivirus- und HIPS-Benachrichtigungen](#) (Seite 45).

### 9.2 Anzeigen von Application Control-Ereignissen

So können Sie sich Application Control-Ereignisse anzeigen lassen:

1. Klicken Sie im Menü **Ansicht** auf **Application Control-Ereignisse**.  
Oder klicken Sie auf dem Dashboard auf den Link **Application Control**.  
Das Dialogfeld **Application Control – Ereignisanzeige** wird angezeigt.
2. Wählen Sie im Dropdown-Menü **Suchperiode** den Zeitraum aus, für den Ereignisse angezeigt werden sollen.  
Sie können einen festen Zeitraum, etwa **24 Std.**, festlegen oder über die Option **Benutzerdefiniert** durch Auswahl von Start- und Endzeitpunkt ihren eigenen Zeitraum bestimmen.
3. Klicken Sie zur Anzeige einer Ereignisliste auf **Suche**.

Sie können die Liste mit Application Control-Ereignissen in eine Datei exportieren. Mehr dazu erfahren Sie unter [Exportieren der Ereignisliste in eine Datei](#) (Seite 23).

Sie können Ereignisse auch in die Zwischenablage kopieren. Mehr dazu erfahren Sie unter [Kopieren von Ereignissen in die Zwischenablage](#) (Seite 23).

### 9.3 Anzeige von Device Control-Ereignissen

So können Sie sich Device Control-Ereignisse anzeigen lassen:

1. Wählen Sie im Menü **Ansicht** die Option **Device Control-Ereignisse**.  
Oder klicken Sie auf dem Dashboard auf den Link **Device Control**.  
Das Dialogfenster **Device Control – Ereignisanzeige** wird geöffnet.

2. Wählen Sie im Dropdown-Menü **Suchperiode** den Zeitraum aus, für den Ereignisse angezeigt werden sollen.  
Sie können einen festen Zeitraum, etwa **24 Std.**, festlegen oder über die Option **Benutzerdefiniert** durch Auswahl von Start- und Endzeitpunkt ihren eigenen Zeitraum bestimmen.
3. Wenn Sie Ereignisse für einen bestimmten Gerätetyp aufrufen möchten, wählen Sie im Dropdown-Menü **Gerätetyp** den Gerätetyp aus.  
Standardmäßig werden in der Ereignisanzeige Ereignisse für alle Gerätetypen angezeigt.
4. Wenn Sie Ereignisse für einen bestimmten Benutzer oder Computer aufrufen möchten, geben Sie den entsprechenden Namen in das zugehörige Feld ein.  
Wenn Sie keine spezifischen Angaben machen, werden Ereignisse für alle Benutzer und Computer angezeigt.
5. Klicken Sie zur Anzeige einer Ereignisliste auf **Suche**.

Im Dialogfeld **Device Control – Ereignisanzeige** können Sie ein Gerät von Device Control-Richtlinien ausschließen. Mehr dazu erfahren Sie unter [Geräte-Ausschlüsse](#) (Seite 44).

Sie können die Liste von Device Control-Ereignissen in eine Datei exportieren. Weitere Informationen erhalten Sie unter [Exportieren der Ereignisliste in eine Datei](#) (Seite 23).

Sie können Ereignisse auch in die Zwischenablage kopieren. Weitere Informationen erhalten Sie unter [Kopieren von Ereignissen in die Zwischenablage](#) (Seite 23).

## 9.4 Anzeige von Firewall-Ereignissen

So können Sie Firewall-Ereignisse anzeigen:

1. Klicken Sie im Menü **Ansicht** auf **Firewall-Ereignisse**.  
Oder klicken Sie auf dem Dashboard auf den Link **Firewall**.  
Das Dialogfeld **Firewall – Ereignisanzeige** wird angezeigt.
2. Wählen Sie im Dropdown-Menü **Suchperiode** den Zeitraum aus, für den Ereignisse angezeigt werden sollen.  
Sie können einen festen Zeitraum, etwa **24 Std.**, festlegen oder über die Option **Benutzerdefiniert** durch Auswahl von Start- und Endzeitpunkt ihren eigenen Zeitraum bestimmen.
3. Klicken Sie zur Anzeige einer Ereignisliste auf **Suche**.

Im Dialogfeld **Firewall – Ereignisanzeige** können Sie anhand der Anweisungen im Abschnitt [Einrichten der Firewall](#) (Seite 36) eine Firewall-Regel an Ihre Bedürfnisse anpassen.

Sie können die Liste mit Firewall-Ereignissen in eine Datei exportieren. Mehr dazu erfahren Sie unter [Exportieren der Ereignisliste in eine Datei](#) (Seite 23).

Sie können Ereignisse auch in die Zwischenablage kopieren. Mehr dazu erfahren Sie unter [Kopieren von Ereignissen in die Zwischenablage](#) (Seite 23).

## 9.5 Exportieren der Ereignisliste in eine Datei

Sie können Application Control-, Firewall- und Device Control-Ereignisse in eine CSV-Datei exportieren.

1. Klicken Sie im Menü **Ansicht** auf die „Ereignis“-Option, die der zu exportierenden Liste entspricht.

Das Dialogfeld **Ereignisanzeige** wird angezeigt.

2. Wenn nur ausgewählte Ereignisse angezeigt werden sollen, legen Sie im Feld **Suchkriterien** Filter fest und klicken Sie zur Anzeige der Ereignisse auf **Suchen**.

Mehr dazu erfahren Sie unter [Anzeigen von Application Control-Ereignissen](#) (Seite 21), [Anzeige von Device Control-Ereignissen](#) (Seite 21) und [Anzeige von Firewall-Ereignissen](#) (Seite 22).

3. Klicken Sie auf **Exportieren**.
4. Geben Sie der Datei im Dialogfeld **Speichern unter** einen Namen und wählen Sie einen Speicherort für die Datei aus.

## 9.6 Kopieren von Ereignissen in die Zwischenablage

Sie können Application Control-, Firewall- oder Device Control-Ereignisse in die Zwischenablage kopieren und in ein anderes Dokument im TSV-Format einfügen. Sie können die gesamte Ereignisliste oder auch nur ein einzelnes Ereignis kopieren.

1. Klicken Sie im Menü **Ansicht** auf die „Ereignis“-Option, die der zu exportierenden Liste entspricht.

Das Dialogfeld **Ereignisanzeige** wird angezeigt.

2. Wenn nur ausgewählte Ereignisse angezeigt werden sollen, legen Sie im Feld **Suchkriterien** Filter fest und klicken Sie zur Anzeige der Ereignisse auf **Suchen**.

Mehr dazu erfahren Sie unter [Anzeigen von Application Control-Ereignissen](#) (Seite 21), [Anzeige von Device Control-Ereignissen](#) (Seite 21) und [Anzeige von Firewall-Ereignissen](#) (Seite 22).

3. Klicken Sie im Dialogfeld **Ereignisanzeige** auf **Kopieren**, um die Ereignisliste in die Zwischenablage zu kopieren.

Wenn Sie ein einzelnes Ereignis kopieren möchten, wählen Sie dieses aus und klicken Sie auf **Kopieren**.

## 10 Konfigurieren eines Scans

### 10.1 Scannen auf Viren, Trojaner, Spyware und Würmer

Standardmäßig erkennt Sophos Anti-Virus bekannte und unbekannt Viren, Trojaner, Spyware und Würmer automatisch, wenn ein Anwender versucht, auf Dateien zuzugreifen, in denen Sie enthalten sind.

So scannen Sie Ihren Computer:

1. Klicken Sie auf der linken Seite unter **Konfiguration** auf **Scans konfigurieren**.
2. Überprüfen Sie, ob im Dialogfeld **Scans konfigurieren** unter **Antivirus- und HIPS-Konfiguration** das Kontrollkästchen **On-Access-Scans aktivieren** ausgewählt ist.

### 10.2 Scannen auf potenziell unerwünschte Anwendungen

Standardmäßig erkennt Sophos Anti-Virus Viren, Trojaner, Spyware und Würmer. Sie können die Software auch dazu konfigurieren, potenziell unerwünschte Anwendungen zu erkennen.

**Hinweis:** Die Option beschränkt sich auf Sophos Endpoint Security and Control für Windows 2000 oder höher.

Es empfiehlt sich, die Suche nach potenziell unerwünschten Anwendungen über einen geplanten Scan zu starten. So wird der sichere Umgang mit Anwendungen gewährleistet, die bereits im Netzwerk laufen. Sie können dann die On-Access-Erkennung aktivieren, um Ihre Computer in Zukunft zu schützen.

So können Sie auf potenziell unerwünschte Anwendungen scannen:

1. Klicken Sie links unter **Konfiguration** auf **Scans konfigurieren**.
2. Klicken Sie im Fenster **Scans konfigurieren** unter **Geplante Scans** auf **Hinzufügen**, um einen neuen Scan zu erstellen. Wenn Sie einen Scan bearbeiten möchten, wählen Sie ihn aus der Liste aus und klicken Sie auf **Ändern**.
3. Im Dialogfeld **Einstellungen zu geplanten Scans** klicken Sie auf **Konfigurieren** (unten im Fenster).
4. Klicken Sie im Dialogfeld **Einstellungen zu Scans und Bereinigung** auf die Registerkarte **Scans**. Im Feld **Scan-Optionen** muss **Adware und PUA einbeziehen** ausgewählt werden. Klicken Sie auf **OK**.
5. Im Verlauf der Scans meldet Sophos Anti-Virus unter Umständen **potenziell unerwünschte Anwendungen**.

Wenn Ihr Computer die Anwendungen starten soll, müssen Sie diese zulassen. Informationen zur Zulassung der Anwendungen entnehmen Sie bitte dem Abschnitt [Zulassen von Anwendungen](#) (Seite 29).

6. Wenn On-Access-Scans aktiviert werden sollen, klicken Sie im Dialogfeld **Scans konfigurieren** auf **On-Access-Scans**.

Das Dialogfeld **On-Access-Scan-Einstellungen** wird angezeigt. Wählen Sie darin im Bereich **Scan-Optionen** die Option **Adware und PUA einbeziehen**.

Einige Anwendungen „überwachen“ Dateien und versuchen regelmäßig, auf sie zuzugreifen. Wenn die On-Access-Scans aktiviert sind, werden alle Zugriffe erkannt und mehrere Alerts ausgegeben. Mehr zu diesem Thema erfahren Sie unter [Hohe Alert-Anzahl aufgrund potenziell unerwünschter Anwendungen](#) (Seite 54).

## 10.3 Konfigurieren von On-Access-Scans

So können Sie die gewünschten Optionen für On-Access-Scans auswählen:

1. Klicken Sie links unter **Konfiguration** auf **Scans konfigurieren**.
2. Klicken Sie im Fenster **Scans konfigurieren** auf **On-Access-Scans**.
3. Wählen Sie im Dialogfeld **On-Access-Scan-Einstellungen** die gewünschten Optionen aus.

### ■ Scannen von Archivdateien

Die Software kann Archivdateien scannen. Beachten Sie hierbei jedoch folgende Hinweise:

- Die On-Access-Scanfunktion scannt beim Zugriff auf Archivdateien diese Dateien automatisch. Das Scannen von Archivdateien ist daher fakultativ.
- Das Scannen von Archivdateien kann die Systemgeschwindigkeit beeinträchtigen und sollte nicht mit On-Access-Scans kombiniert werden.

### ■ Macintosh-Viren einbeziehen

Wählen Sie diese Option aus, um auf Windows-Computern gespeicherte Macintosh-Dateien in On-Access-Scans einzubeziehen.

### ■ Scannen auf Adware und PUA

Standardmäßig erkennt Sophos Endpoint Security and Control Viren, Trojaner und Würmer. Sie können die Software auch dazu konfigurieren, potenziell unerwünschte Anwendungen zu erkennen.

### ■ Scannen auf verdächtige Dateien (HIPS)

Wählen Sie diese Option aus, um verdächtige Dateien in On-Access-Scans einzubeziehen.

4. Wählen Sie unter **Auslöser für On-Access-Scans** aus, welche Dateien gescannt werden sollen, wenn der Benutzer Arbeitsschritte durchführt.

- **Lesezugriff:** Sophos Anti-Virus scannt Dateien automatisch bei Zugriff. In der Regel entspricht dies dem Zeitpunkt, zu dem der Benutzer die Datei öffnet.
- **Schreibzugriff:** Dateien werden beim Schließen gescannt.
- **Umbenennen von:** Dateien werden gescannt, wenn Sie umbenannt werden.

Diese Option bieten einen verbesserten Schutz vor Viren, die auf die Festplatte des Computers schreiben und/oder Dateien umbenennen. Die Nutzung dieser Optionen kann jedoch die Systemleistung beeinträchtigen.

5. Wählen Sie unter **Wechseldatenträger** die Option **Zugriff auf Laufwerke mit infizierten Bootsektoren erlauben** aus, um den Zugriff zu ermöglichen. Dies ist beispielsweise erforderlich, wenn Dateien von einer Diskette kopiert werden sollen, auf der sich ein Bootsektorvirus befindet.

Sophos Anti-Virus verhindert standardmäßig den Zugriff auf Wechseldatenträger mit infiziertem Bootsektor.

## 10.4 Ändern der Scan-Objekte

Die standardmäßig gescannten Dateitypen sind vom Betriebssystem abhängig und ändern sich bei Produkt-Updates.

### ■ Macintosh

Änderungen an Mac OS X-Systemen können Sie über Sophos Update Manager vornehmen, einem mit Sophos Anti-Virus ausgelieferten Tool. Zum Starten von Sophos Update Manager unter Mac OS X öffnen Sie ein **Finder**-Fenster und suchen den Ordner „Sophos Anti-Virus:ESOSX“. Doppelklicken Sie auf **Sophos Update Manager**. Weitere Details werden in der Sophos Update Manager-Hilfe aufgeführt.

### ■ Windows

Standardmäßig scannt Sophos Anti-Virus Dateitypen, die für Viren anfällig sind. Sie können weitere Dateitypen (Scan-Objekte) scannen lassen oder auch bestimmte Dateitypen von Scans ausschließen. Sie können eine Liste der Dateitypen ansehen, wenn Sie zu einem Computer mit dem entsprechenden Betriebssystem gehen, das Sophos Anti-Virus-Fenster öffnen und dort die Konfigurationsseite mit den Erweiterungen aufrufen.

**Hinweis:** Unter Windows 98 gelten Änderungen der Einstellungen für „geplante Scans“ auch für On-Access-Scans.

So lassen sich die Scan-Objekte ändern:

1. Klicken Sie links unter **Konfiguration** auf **Scans konfigurieren**. Das Dialogfeld **Scans konfigurieren** wird angezeigt.
  - Klicken Sie zur Konfiguration von On-Access-Scans im Bereich **Antivirus- und HIPS-Konfiguration** auf **On-Access-Scans**.
  - Klicken Sie zur Konfiguration von geplanten Scans im Bereich **Geplante Scans** auf **Erweiterungen und Ausschlüsse**.
2. Klicken Sie auf die Registerkarte **Erweiterungen**:
  - Um weitere Dateitypen zu scannen, klicken Sie auf **Hinzufügen** und geben im Feld **Erweiterung** die entsprechende Dateinamenserweiterung ein, z.B. PDF.
  - **Dateien ohne Erweiterung scannen**. Standardmäßig werden Dateien ohne Erweiterung gescannt.
  - Um standardmäßig gescannte Dateitypen auszuschließen, klicken Sie auf **Ausschließen**. Das Dialogfeld **Erweiterungen ausschließen** wird angezeigt. Geben Sie die Dateierweiterung ein.

## 10.5 Aktivieren von Web-Scanning

Web-Scanning überprüft Daten und Dateien, die mit Internet Explorer heruntergeladen werden. Web-Scanning ist standardmäßig deaktiviert.

So aktivieren Sie Web-Scanning:

1. Klicken Sie links unter **Konfiguration** auf **Scans konfigurieren**.
2. Wählen Sie im Dialogfeld **Scans konfigurieren** neben der Option **Web-Scanning: Ein** aus.

Sie können auch die Option **Wie On-Access** auswählen, wenn On-Access-Scans und Web-Scanning gleichzeitig aktiviert werden sollen.

## 10.6 Ausschließen von Objekten von On-Access-Scans

Im Folgenden wird erläutert, wie Objekte (z.B. Laufwerke, Ordner oder Dateien) von On-Access-Scans ausgeschlossen werden können.

Dateitypen, die nicht gescannt werden sollen, müssen unter **Folgende Dateitypen nicht scannen**: in die Ausschlussliste aufgenommen werden. Anweisungen hierzu entnehmen Sie bitte dem Abschnitt *Ändern der Scan-Objekte* (Seite 26).

- Die genannten Optionen beschränken sich auf Windows 2000 und höher sowie Mac OS X.
  - Anweisungen zum Ausschließen von Objekten unter Windows 98 finden Sie im Abschnitt *Ausschließen von Objekten von geplanten Scans* (Seite 31).
1. Klicken Sie links unter **Konfiguration** auf **Scans konfigurieren**.
  2. Klicken Sie im Fenster **Scans konfigurieren** auf **On-Access-Scans**.
  3. Klicken Sie im Dialogfeld **Einstellungen für On-Access-Scans** auf die Registerkarte **Windows-Ausschlüsse** bzw. **Mac-Ausschlüsse**.
    - Um weitere Objekte in die Liste aufzunehmen, klicken Sie auf **Hinzufügen** und geben den vollständigen Pfad im Dialogfeld **Objekt ausschließen** ein.
    - Wenn Sie die Option **Remote-Dateien ausschließen** auswählen, scannt Sophos Anti-Virus keine Dateien auf Netzlaufwerken.

## 10.7 Einrichten der automatischen Bereinigung

### 10.7.1 Automatische Bereinigung

Computer können automatisch bereinigt werden, wenn ein Virus gefunden wird. Ändern Sie hierzu die Scan-Einstellungen anhand der Anweisungen im entsprechenden Abschnitt.

**Hinweis:** Potenziell unerwünschte Anwendungen (PUA) werden bei On-Access-Scans nicht bereinigt. Sie können jedoch die automatische Bereinigung nicht zugelassener Anwendungen für geplante Scans aktivieren, wie nachfolgend erläutert wird.

## 10.7.2 Automatische Bereinigung von Viren

Viren können im Verlauf von On-Access-Scans und geplanten Scans automatisch bereinigt werden.

Verfahren Sie hierzu wie folgt:

1. Klicken Sie links unter **Konfiguration** auf **Scans konfigurieren**.
2. Klicken Sie zum Ändern der Einstellungen von On-Access-Scans im Dialogfeld **Scans konfigurieren** auf die Schaltfläche **On-Access-Scans**. Klicken Sie im Dialogfeld **Einstellungen für On-Access-Scans** auf die Registerkarte **Bereinigung**.
3. Wählen Sie zum Ändern der Einstellungen eines geplanten Scans im Dialogfeld **Scans konfigurieren** unter **Geplante Scans** einen geplanten Scan aus und klicken Sie auf **Ändern**.

Klicken Sie dann im Dialogfeld **Einstellungen zu geplanten Scans** auf **Konfigurieren**. Klicken Sie im Dialogfeld **Scan- und Bereinigungs-Einstellungen** auf die Registerkarte **Bereinigung**.

4. Wählen Sie **Objekte mit Virus/Spyware automatisch bereinigen**.
5. Sie können außerdem festlegen, wie verfahren werden soll, wenn die Bereinigung fehlschlägt: Folgende Optionen stehen zur Verfügung:
  - Zugriff verweigern
  - Löschen
  - Zugriff verweigern und in das Standardverzeichnis verschieben
  - Zugriff verweigern und in UNC-Pfad verschieben

**Hinweis:** Wenn Sie **Verschieben nach** auswählen und einen Speicherort angeben, verschieben Mac OS X Computer infizierte Objekte in das Standardverzeichnis.

## 10.7.3 Automatische Bereinigung potenziell unerwünschter Anwendungen

**Hinweis:** Diese Option beschränkt sich auf Sophos Endpoint Security and Control unter Windows 2000 und aufwärts.

Die automatische Bereinigung potenziell unerwünschter Anwendungen ist nur bei geplanten Scans möglich.

So werden potenziell unerwünschte Anwendungen automatisch bereinigt:

1. Klicken Sie links unter **Konfiguration** auf **Scans konfigurieren**.
2. Wählen Sie im Dialogfeld **Scans konfigurieren** im Bereich **Geplante Scans** einen Scan aus und klicken Sie auf **Ändern**.
3. Klicken Sie dann im Dialogfeld **Einstellungen zu geplanten Scans** auf **Konfigurieren**.
4. Klicken Sie im Dialogfeld **Scan- und Bereinigungs-Einstellungen** auf die Registerkarte **Bereinigung**.

5. Wählen Sie im Bereich **Adware und PUA** die Option **Adware und PUA automatisch bereinigen**.

Jetzt kann **Sophos Anti-Virus** potenziell unerwünschte Anwendungen vom Computer entfernen.

6. Sie können auch angeben, wie mit verdächtigen Dateien verfahren werden soll. Folgende Optionen stehen zur Verfügung:
  - Zugriff verweigern
  - Löschen
  - Zugriff verweigern und in das Standardverzeichnis verschieben
  - Zugriff verweigern und in UNC-Pfad verschieben

**Hinweis:** Wenn Sie **Verschieben nach** wählen und einen Speicherort angeben, verschieben Mac OS X-Computer infizierte Objekte trotzdem in den Standard-Speicherort.

## 10.8 Zulassen von Anwendungen

Wenn Sie die Erkennung von potenziell unerwünschten Anwendungen in Sophos Anti-Virus aktiviert haben, werden unter Umständen Anwendungen gesperrt, die Sie nutzen möchten.

So können Sie Anwendungen zulassen:

1. Klicken Sie auf der linken Seite unter **Konfiguration** auf **Scans konfigurieren**.
2. Klicken Sie im Fenster **Scans konfigurieren** auf **Autorisierungen**.
3. Wählen Sie im Dialogfeld **Authorization Manager** unter **Bekannte Adware/PUA** die Anwendung aus, die zugelassen werden soll. Klicken Sie auf **Hinzufügen**, um die gewünschte Anwendung in die Liste der zugelassenen Anwendungen aufzunehmen. Wiederholen Sie die genannten Schritte für alle Anwendungen, die zugelassen werden sollen. Klicken Sie auf **OK**.
4. Wenn die zuzulassende Anwendung nicht angezeigt wird, klicken Sie auf **Neuer Eintrag**. Geben Sie in das Dialogfeld **Neue Adware/PUA** den Namen der gewünschten Adware oder PUA ein und klicken Sie auf **OK**.

## 10.9 Scannen von Computern zu bestimmten Zeiten

Computer können zu festgesetzten Zeiten gescannt werden.

So können Sie Scans zu bestimmten Zeiten einrichten:

1. Klicken Sie auf der linken Seite unter **Konfiguration** auf **Scans konfigurieren**.
2. Klicken Sie im Dialogfeld **Scans konfigurieren** im Feld **Geplante Scans** auf **Hinzufügen**.
3. Geben Sie im Dialogfeld **Einstellungen zu geplanten Scans** einen Namen für den geplanten Scan ein.
4. Wählen Sie die Scan-Objekte aus:
  - Lokale Festplatten

- Diskettenlaufwerke und Wechsellaufwerke
- CD-Laufwerke

Standardmäßig werden alle lokalen Festplatten gescannt.

5. Wählen Sie den gewünschten Scanzeitpunkt (Datum und Uhrzeit) aus.

Klicken Sie zum Ändern der Standard-Scan- und Bereinigungsoptionen des Scans auf **Konfigurieren** im unteren Bereich des Dialogfelds **Einstellungen zu geplanten Scans**. Mehr dazu erfahren Sie unter [Konfigurieren von geplanten Scans](#) (Seite 30) und [Automatische Bereinigung von Viren](#) (Seite 28).

Unter [Ändern der Scan-Objekte](#) (Seite 26) oder [Ausschließen von Objekten von geplanten Scans](#) (Seite 31) können Sie nachlesen, wie die Scan-Objekte geändert und Objekte von geplanten Scans ausgeschlossen werden können.

## 10.10 Konfigurieren von geplanten Scans

Sie können die Einstellungen für geplante Scans konfigurieren.

So können Sie die Einstellungen eines geplanten Scans konfigurieren:

1. Klicken Sie links unter **Konfiguration** auf **Scans konfigurieren**.
2. Wählen Sie im Dialogfeld **Scans konfigurieren** einen geplanten Scan aus und klicken Sie auf **Ändern**.
3. Klicken Sie dann im Dialogfeld **Einstellungen zu geplanten Scans** auf **Konfigurieren**.

4. Rufen Sie im Dialogfeld **Scan- und Bereinigungs-Einstellungen** die Registerkarte **Scans** auf und wählen Sie die gewünschten Optionen aus.

- **Scannen von Archivdateien**

Die Software kann Archivdateien scannen. Beachten Sie hierbei jedoch folgende Hinweise:

- Die On-Access-Scanfunktion scannt beim Zugriff auf Archivdateien diese Dateien automatisch. Das Scannen von Archivdateien ist daher fakultativ.
- Das Scannen von Archivdateien kann die Systemgeschwindigkeit beeinträchtigen und sollte nicht mit On-Access-Scans kombiniert werden.

- **Macintosh-Viren einbeziehen**

Wählen Sie diese Option aus, um auf Windows-Computern gespeicherte Macintosh-Dateien in geplante Scans einzubeziehen.

- **Scannen auf Adware und PUA**

Standardmäßig erkennt Sophos Endpoint Security and Control Viren, Trojaner und Würmer. Sie können die Software auch dazu konfigurieren, potenziell unerwünschte Anwendungen zu erkennen. Diese Option ist bei geplanten Scans standardmäßig aktiviert.

- **Scannen auf verdächtige Dateien (HIPS)**

Standardmäßig werden verdächtige Dateien von geplanten Scans erfasst.

- **Aktivieren von Rootkit-Scans**

Beim Durchführen einer **vollständigen Systemüberprüfung** wird auch auf Rootkits gescannt. Diese Option kann auch bei geplanten Scans ausgewählt werden.

Nähere Informationen zu den Bereinigungsoptionen finden Sie im Abschnitt [Automatische Bereinigung](#) (Seite 27) und den Abschnitten zum Einrichten der automatischen Bereinigung.

## 10.11 Ausschließen von Objekten von geplanten Scans

Im Folgenden wird erläutert, wie Objekte (z.B. Laufwerke, Ordner oder Dateien) von geplanten Scans ausgeschlossen werden können.

Dateitypen, die nicht gescannt werden sollen, müssen unter **Folgende Dateitypen nicht scannen:** in die Ausschlussliste aufgenommen werden. Anweisungen hierzu entnehmen Sie bitte dem Abschnitt [Ändern der Scan-Objekte](#) (Seite 26).

**Hinweis:** Unter Windows 98 werden Änderungen an den Einstellungen für geplante Scans auch für On-Access-Scans übernommen.

So können Sie Objekte von geplanten Scans ausschließen:

1. Klicken Sie links unter **Konfiguration** auf **Scans konfigurieren**. Das Dialogfeld **Scans konfigurieren** wird angezeigt.
2. Klicken Sie im Fensterbereich **Geplante Scans** auf **Erweiterungen und Ausschlüsse**.

3. Öffnen Sie im Fenster **Erweiterungen und Ausschlüsse für geplante Scans** je nach dem auszuschließenden Betriebssystem jeweils die Registerkarte **Windows-Ausschlüsse** oder **Macintosh-Ausschlüsse**. Um Objekte zu der Liste hinzuzufügen, klicken Sie auf **Hinzufügen** und geben den vollständigen Pfad im Dialogfeld **Objekt ausschließen** ein.

## 10.12 Konfigurieren von Scans auf Einzelcomputern

Sie können festlegen, dass bestimmte Computer von der zentralen Konfiguration in Sophos Control Center abweichen.

So können Sie Scans auf Einzelcomputern konfigurieren:

1. Markieren Sie den/die Computer in der Computerliste. Rechtsklicken Sie darauf und deaktivieren Sie die Option **Zentrale Konfiguration übernehmen**.
2. Gehen Sie anschließend zu den gewünschten Computern und konfigurieren Sie die Virenschutzoptionen.

Rechtsklicken Sie zum Konfigurieren von Scans auf einem bestimmten Computer auf das Symbol von **Sophos Endpoint Security and Control** in der Taskleiste .

3. Klicken Sie auf **Sophos Endpoint Security and Control öffnen**. Klicken Sie im Fenster von **Sophos Endpoint Security and Control** auf **Antivirus- und HIPS-Konfiguration**. Klicken Sie im Bereich **Konfigurieren** auf **On-Access-Scans** und nehmen Sie die gewünschten Änderungen an den Einstellungen vor.

Nähere Informationen zur Konfiguration von Scans auf Einzelcomputern entnehmen Sie bitte der **Hilfe** zu *Sophos Endpoint Security and Control*.

## 11 Konfigurieren von Updates

### 11.1 Ändern des Update-Umfangs

Sie können die Software, die upgedatet wird, ändern. Dies kann unter folgenden Voraussetzungen erforderlich sein:

- Computer mit einem anderen Betriebssystem, z.B. Mac OS X, für die Sophos Anti-Virus erforderlich ist, werden ins Netzwerk aufgenommen.
- Alle Computer eines bestimmten Betriebssystems werden aus dem Netzwerk entfernt.

So können Sie die heruntergeladene Software ändern:

1. Klicken Sie auf der linken Seite unter **Konfiguration** auf **Updates konfigurieren**.
2. Klicken Sie im Dialogfeld **Update-Konfiguration** auf die Registerkarte **Software**. Wählen Sie das/die Betriebssystem(e) aus, für die Sophos Anti-Virus erforderlich ist und klicken Sie auf **OK**.

Wenn für die gewählten Betriebssysteme noch kein Schutz vorhanden war (Windows 98 oder Mac OS X), fahren Sie mit Schritt 3 und 4 fort.

3. Rufen Sie wieder das Hauptfenster von Sophos Control Center auf. Klicken Sie im Menü **Maßnahme** auf **Jetzt updaten**, um die neue Software herunterzuladen.
4. Gehen Sie zu allen Computern des neuen Typs und installieren Sie Sophos Anti-Virus. Weitere Informationen zur manuellen Installation können Sie der **Startup-Anleitung** zu *Sophos Control Center* entnehmen.

### 11.2 Updates über einen Proxyserver

Wenn Sie über einen Proxyserver auf das Internet zugreifen, müssen Sie Sophos Control Center so konfigurieren, dass Updates über den Proxyserver heruntergeladen werden.

Verfahren Sie hierzu wie folgt:

1. Klicken Sie auf der linken Seite unter **Konfiguration** auf **Updates konfigurieren**.
2. Klicken Sie im Dialogfeld **Update-Konfiguration** auf die Registerkarte **Proxyserver**. Geben Sie die Adresse des Proxyservers und die Portnummer ein. Geben Sie den Benutzernamen und das Kennwort eines Benutzerkontos mit Zugriff auf den Proxyserver ein (diese Daten erhalten Sie bei Bedarf von Ihrem Netzwerkadministrator).

### 11.3 Ändern der Benutzerdetails für Updates

Sie können die Benutzerdetails zum Herunterladen von Updates ändern.

Verfahren Sie hierzu wie folgt:

1. Klicken Sie auf der linken Seite unter **Konfiguration** auf **Updates konfigurieren**.
2. Klicken Sie im Dialogfeld **Update-Konfiguration** auf die Registerkarte **Benutzerdetails**. Geben Sie den Benutzernamen und das Kennwort ein, das Sie von Sophos erhalten haben.

## 11.4 Deaktivieren automatischer Updates

Wenn Sie automatische Updates deaktivieren möchten (weil Sie beispielsweise über eine Einwahlverbindung auf das Internet zugreifen), verfahren Sie wie folgt:

**Hinweis:** Wenn Sie automatische Updates deaktivieren, stellen Sie sicher, dass Sie regelmäßig auf Updates prüfen. Im Abschnitt *Manuelle Updates* (Seite 13) wird die manuelle Update-Suche erläutert.

So können Sie automatische Updates deaktivieren:

1. Klicken Sie auf der linken Seite unter **Konfiguration** auf **Updates konfigurieren**.
2. Klicken Sie im Dialogfeld **Update-Konfiguration** auf die Registerkarte **Zeitplan**. Deaktivieren Sie das Kontrollkästchen **Sophos Updates automatisch herunterladen**.

## 11.5 Ändern der Update-Häufigkeit

Standardmäßig suchen Computer alle 10 Minuten nach Sicherheitssoftware-Updates.

So können Sie die Update-Häufigkeit ändern:

1. Klicken Sie auf der linken Seite unter **Konfiguration** auf **Updates konfigurieren**.
2. Klicken Sie im Dialogfeld **Update-Konfiguration** auf die Registerkarte **Zeitplan**. Stellen Sie sicher, dass das Kontrollkästchen **Netzwerkcomputer können Sophos Updates automatisch herunterladen** aktiviert ist. Geben Sie ein Zeitintervall in Minuten in das Feld unter dem Kontrollkästchen ein.

## 11.6 Updaten von Computern ohne permanente Netzwerkverbindung

Standardmäßig laden Computer Updates aus einem Update-Ordner auf dem Computer herunter, auf dem Sophos Control Center ausgeführt wird. Wenn der Ordner auf dem Computer nicht mehr verfügbar ist (z.B. wenn der Computer nicht mit dem Unternehmensnetzwerk, jedoch mit dem Internet verbunden ist), bezieht der Computer Updates direkt von Sophos.

So können Sie Computer ohne permanente Netzwerkverbindung updaten:

1. Klicken Sie auf der linken Seite unter **Konfiguration** auf **Updates konfigurieren**.
2. Klicken Sie im Dialogfeld **Updates konfigurieren** auf die Registerkarte **Alternativquelle**. Die folgenden Optionen werden angezeigt:

■ **Sophos**

Diese Option bietet sich an, wenn Computer nicht immer mit dem Unternehmensnetzwerk verbunden sind, z.B. Laptops. Die Zugangsdaten für diese Computer entsprechen den Zugangsdaten für Sophos Control Center.

■ **Keine**

Diese Option ist voreingestellt. Eine Alternativquelle wird hierbei nicht angegeben.

■ **Ihr Unternehmen**

Wählen Sie diese Option aus, wenn die Computer Updates von einer Website oder einem Verzeichnis im Unternehmen beziehen sollen, wenn die primäre Update-Quelle nicht verfügbar ist. Geben Sie die Adresse des Netzwerkordners (UNC-Pfad) oder der Website (HTTP-Adresse) ein.

Geben Sie bei Bedarf die Zugangsdaten eines Kontos an, die den Zugriff auf den Ordner oder die Website ermöglichen. Dieses Konto benötigt Leserechte für das Verzeichnis, das Sie in das Adressfeld eingegeben haben. Wenn der Benutzername die Domäne enthalten muss, verwenden Sie die Form Domäne\Benutzername.

**Hinweis:** Achten Sie bei Angabe eines Ordners oder einer Website darauf, dass die Sicherheitssoftware in dem entsprechenden Ordner regelmäßig aktualisiert wird. Installieren Sie hierzu Sophos Control Center. Sie können auch Kopien des Update-Ordners veröffentlichen.

## 12 Konfigurieren der Firewall

### 12.1 Einrichten der Firewall

Sie können die Firewall so konfigurieren, dass Datenverkehr in Einklang mit Ihren Bedürfnissen gesperrt oder zugelassen wird. Die Firewall sperrt standardmäßig unnötigen Datenverkehr.

Eine umfassende Übersicht über die Werkseinstellungen der Firewall finden Sie unter:  
<http://www.sophos.de/support/knowledgebase/article/16608.html>

So können Sie die Firewall konfigurieren:

1. Klicken Sie auf der linken Seite unter **Konfiguration** auf **Firewall konfigurieren**.
2. Klicken Sie im Firewall-Konfigurationsassistenten auf **Weiter**.
3. Wählen Sie auf der Seite **Firewall konfigurieren** die gewünschten Optionen aus:
  - Wählen Sie die Option **Gesamten Verkehr zulassen**, wenn Sie die Firewall deaktivieren und den gesamten Datenverkehr zulassen möchten.
  - Wählen Sie **Ein Standort**, wenn sich Computer immer im Netzwerk befinden, z.B. Desktop Computer.
  - Wählen Sie **Zwei Standorte**, wenn die Firewall unterschiedliche Einstellungen je nach Standort des Computers aufweisen soll, z.B. im Büro (im Firmennetzwerk) oder extern. Bei Notebooks bietet sich die Option „Zwei Standorte“ an.
4. Wenn Sie auf der vorherigen Seite die Option **Zwei Standorte** ausgewählt haben, konfigurieren Sie auf der Seite **Netzwerkidentifizierung** DNS- oder Gateway-Netzwerkerkennung.

**Hinweis:** Die Seite **Netzwerkidentifizierung** wird nur bei Auswahl der Option **Zwei Standorte** angezeigt.

Sophos Control Center wendet unterschiedliche Einstellungen auf Computer an, je nachdem, ob Computer mit dem Netzwerk verbunden sind oder nicht.

5. Geben Sie auf der Seite **Arbeitsmodus** an, wie die Firewall eingehenden und ausgehenden Datenfluss behandeln soll.
  - **Lernmodus**  
Die Computer können auf das Netzwerk und das Internet zugreifen, und Informationen werden an die Konsole übermittelt.
  - **Eingehenden Datenfluss blockieren, ausgehenden Datenfluss erlauben**  
Die Computer können auf das Netzwerk und das Internet zugreifen. Eingehender Datenfluss wird jedoch gesperrt.
  - **Eingehenden und ausgehenden Datenfluss blockieren**  
Bei Auswahl dieser Option sperrt die Firewall den gesamten ausgehenden Datenfluss mit Ausnahme von Anwendungen, die Sie durch Klicken auf **Zulassen** auf der rechten Seite erlauben. Bei „zugelassenen“ Anwendungen unterliegt die Netzwerkaktivität keinerlei Beschränkungen.

6. Klicken Sie zum Öffnen der erweiterten Firewall-Konfigurationsoptionen auf **Erweitert**.  
**Hinweis:** Sie sollten nur Änderungen an den erweiterten Optionen vornehmen, wenn Sie wissen, wie sich dies auswirkt.  
Informationen zur erweiterten Firewall-Konfigurationen können Sie der **Hilfe** zu *Sophos Endpoint Security and Control* entnehmen.
7. Wählen Sie auf der Seite **Datei- und Druckerfreigabe** die Option **Datei- und Druckerfreigabe zulassen**, wenn Sie anderen Computern im Netzwerk den Zugriff auf Drucker und Freigaben auf dem Computer ermöglichen möchten.
8. Wenn Sie die Option **Zwei Standorte** ausgewählt haben, werden Sie zur Konfiguration von eingehendem und ausgehendem Datenfluss und der Datei- und Druckerfreigabe für den zweiten Standort (nicht im Netzwerk) aufgefordert.

Nach dem Einrichten der Firewall können Sie sich Firewall-Ereignisse in der **Firewall – Ereignisanzeige** anzeigen lassen (z.B. Anwendungen, die von der Firewall gesperrt wurden). Mehr dazu erfahren Sie unter [Anzeige von Firewall-Ereignissen](#) (Seite 22).

Sie können den Assistenten erneut ausführen, wenn Sie bestimmte Einstellungen zu einem späteren Zeitpunkt ändern.

Im Dashboard wird außerdem die Anzahl der Computer angezeigt, deren Ereignisanzahl in den letzten 24 Stunden einen festgelegten Höchstwert überschritten hat.

## 12.2 Ausschalten der Firewall

### 12.2.1 Deaktivieren der Firewall in Sophos Control Center

Sie können die Firewall auf allen in Sophos Control Center verwalteten Computern deaktivieren.

Es empfiehlt sich jedoch, die Firewall für den Normalgebrauch aktiviert zu lassen.

So können Sie die Firewall in Sophos Control Center deaktivieren:

1. Klicken Sie links unter **Konfiguration** auf **Firewall konfigurieren**.  
Der **Firewall-Konfigurationsassistent** wird geöffnet.
2. Rufen Sie im **Firewall-Konfigurationsassistent** die Seite **Firewall konfigurieren** aus und aktivieren Sie die Option **Gesamten Verkehr zulassen**.

### 12.2.2 Deaktivieren der Firewall auf Einzelcomputern

Sie können die Firewall für die gewählten Computer deaktivieren.

Verfahren Sie hierzu wie folgt:

1. Markieren Sie den/die Computer in der Computerliste. Rechtsklicken Sie darauf und deaktivieren Sie die Option **Zentrale Konfiguration übernehmen**.

**Hinweis:** Wenn die zentrale Konfiguration (und die Firewall) für den Computer nicht übernommen wurde, kann Sophos Anti-Virus auch lokal konfiguriert werden.

2. Gehen Sie zu dem/den Einzelcomputer(n) und deaktivieren Sie die Firewall wie folgt:  
Suchen Sie das Schildsymbol von Sophos Endpoint Security and Control.
  - a) Rechtsklicken Sie auf das Symbol. Wählen Sie im angezeigten Kontextmenü die Option **Sophos Endpoint Security and Control öffnen**.
  - b) Klicken Sie im Bereich **Firewall** auf **Firewall konfigurieren**.  
Das Fenster zur Firewall-Konfiguration wird geöffnet.
  - c) Klicken Sie auf die Registerkarte **Allgemein** und wählen Sie **Gesamten Verkehr zulassen**.  
Klicken Sie auf **OK**.

## 12.3 Zulassen von gesperrten Anwendungen

Wenn die Firewall eine Anwendung auf Ihren Netzwerkcomputern sperrt, wird dies im Firewall-Protokoll festgehalten.

So können Sie Informationen zu gesperrten Anwendungen aufrufen, diese zulassen oder neue Regeln dafür erstellen:

1. Richten Sie den Mauszeiger im Menü **Ansicht** auf **Ereignisse** und klicken Sie anschließend auf **Firewall-Ereignisse**.
2. Wählen Sie im Dialogfeld **Firewall – Ereignisanzeige** den Eintrag für die Anwendung aus, die Sie zulassen möchten oder für die Sie eine Regel erstellen möchten. Klicken Sie auf **Regel erstellen**.
3. Wählen Sie im Dialogfeld aus, ob Sie die Anwendung zulassen möchten oder eine Regel dafür erstellen möchten.
4. Wählen Sie aus der Liste der Firewall-Richtlinien die Richtlinien aus, die Sie in die Regel aufnehmen möchten. Klicken Sie zur Übernahme der Regel für alle Richtlinien auf **Alles markieren** und klicken Sie anschließend auf **OK**.

## 12.4 Konfigurieren der Firewall auf Einzelcomputern

Wenn bestimmte Computer von der zentralen Konfiguration von Sophos Control Center abweichen sollen, verfahren Sie wie folgt:

1. Markieren Sie den/die Computer in der Computerliste. Rechtsklicken Sie darauf und deaktivieren Sie die Option **Zentrale Konfiguration übernehmen**.
2. Gehen Sie zu dem/den Einzelcomputer(n) und konfigurieren Sie die Firewall wie folgt:
  - a) Rechtsklicken Sie auf das Schildsymbol von Sophos Endpoint Security.
  - b) Rechtsklicken Sie auf das Symbol. Wählen Sie im angezeigten Kontextmenü die Option **Sophos Endpoint Security and Control öffnen**.
  - c) Klicken Sie im Bereich **Firewall** auf **Firewall konfigurieren**.  
Das Fenster zur Firewall-Konfiguration wird geöffnet.

## 13 Konfigurieren von Application Control

### 13.1 Application Control

Mit Sophos Control Center können Sie Controlled Applications erkennen und sperren, d.h. legitime Anwendungen, die zwar kein Sicherheitsrisiko darstellen, die aber für Ihre Unternehmensumgebung ungeeignet sind. Zu solchen Anwendungen gehören Instant Messaging (IM) Clients, Voice Over Internet Protocol (VoIP) Clients, Digital Imaging Software, Medienplayer, Browser Plug-Ins usw.

**Hinweis:** Die Option beschränkt sich auf Sophos Endpoint Security and Control für Windows 2000 und aufwärts.

Die Liste der Controlled Applications wird von Sophos zur Verfügung gestellt und regelmäßig aktualisiert. Sie können keine neuen Anwendungen in die Liste aufnehmen. Auf Wunsch können Sie jedoch bei Sophos die Aufnahme einer Anwendung, die im Netzwerk kontrolliert werden soll, in die Liste beantragen. Nähere Informationen finden Sie im Support-Artikel **35330** (<http://www.sophos.de/support/knowledgebase/article/35330.html>).

#### Application Control-Ereignisse

Application Control-Ereignisse (z.B. eine erkannte Controlled Application im Netzwerk) werden im Application Control-Ereignisprotokoll verzeichnet und können in Sophos Control Center aufgerufen werden. Mehr dazu erfahren Sie unter [Anzeigen von Application Control-Ereignissen](#) (Seite 21).

Standardmäßig wird im Dashboard die Anzahl der Computer angezeigt, deren Ereignisanzahl in den letzten 24 Stunden einen festgelegten Höchstwert überschritten hat.

Sie können einstellen, dass die von Ihnen ausgewählten Empfänger über Application Control-Ereignisse benachrichtigt werden. Mehr dazu erfahren Sie unter [Einrichten von Application Control-Alerts](#) (Seite 47).

### 13.2 Konfigurieren von Application Control

Sie können Sophos Control Center dazu konfigurieren, bei Zugriff auf Controlled Applications in Ihrem Netzwerk zu scannen.

1. Klicken Sie auf der linken Seite unter **Konfiguration** auf **Application Control konfigurieren**.  
Das Dialogfeld **Application Control konfigurieren** wird angezeigt.
2. Stellen Sie auf der Registerkarte **Scans** die Optionen folgendermaßen ein:
  - Aktivieren Sie zur Aktivierung von On-Access-Scans das Kontrollkästchen **On-Access-Scans aktivieren**. Wenn die Anwendungen bei Zugriff erkannt jedoch nicht blockiert werden sollen, wählen Sie das Kontrollkästchen **Erkennen, aber laufen lassen**.
  - Zum Aktivieren von On-Demand-Scans aktivieren Sie das Kontrollkästchen **On-Demand-Scans und geplante Scans aktivieren**.

**Hinweis:** Ihre Einstellungen für Antivirus- und HIPS-Richtlinien bestimmen, welche Dateien überprüft werden (d.h. die Erweiterungen und Ausnahmen).

3. Klicken Sie auf die Registerkarte **Autorisierungen** und wählen Sie die Anwendungen aus, die überwacht werden sollen.

Informationen zur Auswahl der Anwendungen entnehmen Sie bitte dem Abschnitt [Auswahl der Controlled Applications](#) (Seite 40).

Wenn Sie Controlled Applications entfernen möchten, die auf Ihren Netzwerkcomputern gefunden wurden, folgen Sie den Anweisungen im Abschnitt [Deinstallieren von Controlled Applications](#) (Seite 40).

Sie können auch Alerts an bestimmte Benutzer senden, wenn auf einem der Computer in der Gruppe eine Controlled Application entdeckt wurde. Nähere Informationen hierzu finden Sie unter [Einrichten von Application Control-Alerts](#) (Seite 47).

### 13.3 Auswahl der Controlled Applications

Standardmäßig sind alle Anwendungen zugelassen. Sie können die Anwendungen, die Sie kontrollieren möchten, folgendermaßen wählen:

1. Klicken Sie auf der linken Seite unter **Konfiguration** auf **Application Control konfigurieren**.
2. Klicken Sie im Dialogfeld **Application Control konfigurieren** auf die Registerkarte **Autorisierungen**.
3. Wählen Sie einen **Anwendungstyp**, z.B. **Dateifreigabe**.

Eine vollständige Liste der Anwendungen in dieser Gruppe wird in der Liste **Zugelassen** angezeigt.

- Um eine Anwendung zu sperren, wählen Sie sie und verschieben Sie sie in die Liste **Gesperrt**, indem Sie auf die Schaltfläche **Hinzufügen** klicken.



- Um neue Anwendungen zu sperren, die Sophos diesem Typ in Zukunft hinzufügt, verschieben Sie **Neue Anwendungen** in die Liste **Gesperrt**.
- Um alle Anwendungen dieses Typs zu blockieren, verschieben Sie alle Anwendungen aus der Liste **Zugelassen** in die Liste **Gesperrt**, indem Sie auf die Schaltfläche **Alle hinzufügen** klicken.



### 13.4 Deinstallieren von Controlled Applications

Vor der Deinstallation von Controlled Applications müssen Sie sicherstellen, dass On-Access-Scans für Controlled Applications deaktiviert sind. Bei On-Access-Scans werden Programme gesperrt, die zur Installation und Deinstallation von Anwendungen benötigt werden. Diese Scan-Funktion kann daher die Deinstallation beeinträchtigen.

Es gibt zwei Möglichkeiten, eine Anwendung zu entfernen:

- Führen Sie an das Deinstallationsprogramm für das Produkt auf allen Computern aus. Dies erfolgt gewöhnlich über das Dienstprogramm „Software“ in der Windows-Systemsteuerung.
- Auf dem Server können Sie das Deinstallationsprogramm für das Produkt auf Ihren Computern im Netzwerk über Ihr übliches Skript- oder Administrationstool ausführen.

Sie können die On-Access-Scans für Controlled Applications nun aktivieren.

## 14 Konfigurieren von Device Control

### 14.1 Device Control

**Wichtig:** Es ist davon abzuraten, Sophos Device Control mit Gerätesteuerungssoftware anderer Anbieter zu kombinieren.

Mit **Device Control** können Sie verhindern, dass Benutzer nicht zugelassene externe Hardware, Wechselmedien und Wireless-Geräte auf dem Computer einsetzen. So wird das Risiko unerwünschter Datenverluste minimiert. Zudem wird die unzulässige Installation unternehmensfremder Software unterbunden.

Wechselmedien, optische Disk-Laufwerke und Diskettenlaufwerke können auch schreibgeschützt werden.

Device Control ist standardmäßig deaktiviert und alle Geräte sind zugelassen.

Für den ersten Einsatz von Device Control empfiehlt Sophos:

- Wählen Sie Gerätearten aus, die überwacht werden sollen.
- Lassen Sie Geräte zwar erkennen, jedoch nicht blockieren.
- Richten Sie Device Control-Alerts ein.
- Lassen Sie Device Control Speichermedien erkennen und blockieren oder schreibschützen Sie sie.

#### Device Control-Ereignisse

Device Control-Ereignisse (z.B. das Sperren eines Wechselmediums) werden im Device Control-Ereignisprotokoll verzeichnet und können in Sophos Control Center aufgerufen werden. Mehr dazu erfahren Sie unter [Anzeige von Device Control-Ereignissen](#) (Seite 21).

Standardmäßig wird im Dashboard die Anzahl der Computer angezeigt, deren Ereignisanzahl in den letzten 24 Stunden einen festgelegten Höchstwert überschritten hat.

Zudem können Sie festlegen, dass die gewählten Empfänger über Device Control-Ereignisse benachrichtigt werden. Mehr dazu erfahren Sie unter [Einrichten von Device Control-Alerts](#) (Seite 48).

### 14.2 Welche Geräte kann Device Control kontrollieren?

Mit Device Control können Sie drei Gerätetypen sperren: *Speicher, Netzwerk und kurze Reichweite*.

#### Speichermedien

- Wechselmedien (z.B. USB-Flash-Laufwerke, PC-Kartenlesegeräte und externe Festplatten)
- Optische Laufwerke (CD-ROM/DVD-Laufwerke/Blu-ray-Laufwerke)
- Diskettenlaufwerke

- Sichere Wechselmedien (z.B. USB-Flash-Laufwerke mit Hardware-Verschlüsselung (SanDisk Cruzer Enterprise, SanDisk Cruzer Enterprise FIPS Edition, Kingston Data Traveler Vault – Privacy Edition, Kingston Data Traveler BlackBox und IronKey Enterprise Basic Edition)

Bei Bedarf können Sie auch unterstützte sichere Wechselmedien zulassen und andere Wechselmedien sperren. Auf der Sophos Website ([www.sophos.de](http://www.sophos.de)) finden Sie eine aktuelle Liste unterstützter sicherer Wechselmedien.

### Netzwerkgeräte

- Modems
- Wireless-Geräte (Wi-Fi-Schnittstellen, 802.11-Standard)

Bei Netzwerkschnittstellen können Sie zudem die Zugangsstufe „Netzwerkbrücken sperren“ einstellen. Hierdurch können Netzwerkgeräte (d.h. Wi-Fi-Adapter) aktiviert werden, wenn der Computer physisch vom Netzwerk abgetrennt wird. Wählen Sie die Option **Netzwerkbrücken sperren** aus, wenn Sie die Zugriffsstufen für Netzwerkgeräte festlegen.

**Hinweis:** Im Modus „Netzwerkbrücken sperren“ sind Netzwerkbrücken nicht möglich (beispielsweise zwischen einem Unternehmensnetzwerk und einem unternehmensexternen Netzwerk). Der Modus „Netzwerkbrücken sperren“ steht für Wireless-Geräte und Modems zur Verfügung. Hierbei werden Wireless- oder Modemnetzwerkadapter deaktiviert, wenn ein Endpoint an ein physisches Netzwerk angeschlossen wird (in der Regel per Ethernet-Verbindung). Wenn der Endpoint von dem physischen Netzwerk getrennt wird, wird der Wireless- oder Modemnetzwerkadapter wieder aktiviert.

### Kurze Reichweite

- Bluetooth-Schnittstellen
- Infrarot-Schnittstellen (IrDA)

Device Control sperrt interne und externe Geräte und Schnittstellen. Wenn Bluetooth-Schnittstellen gesperrt werden, werden folgende Komponenten blockiert:

- Die integrierte Bluetooth-Schnittstelle im Computer
- USB-Bluetooth-Adapter, die an den Computer angeschlossen werden

## 14.3 Konfigurieren von Device Control

Sie können Sophos Control Center dazu konfigurieren, bei Zugriff auf Geräte in Ihrem Netzwerk, die überwacht werden sollen, zu scannen.

1. Klicken Sie auf der linken Seite unter **Konfiguration** auf **Device Control konfigurieren**.  
Das Dialogfeld **Device Control-Richtlinie** wird angezeigt.

2. Nehmen Sie auf der Registerkarte **Konfiguration** die folgenden Einstellungen vor:
  - Aktivieren Sie zum Aktivieren von Device Control das Kontrollkästchen **Device Control-Scans aktivieren**. Wenn die Geräte bei Zugriff erkannt jedoch nicht blockiert werden sollen, wählen Sie das Kontrollkästchen **Geräte erkennen, aber nicht sperren**.
  - So können Sie die Zugriffsstufe für die einzelnen Gerätetypen festlegen: Klicken Sie in der Spalte **Status** neben den Gerätetyp und klicken Sie dann auf den Dropdown-Pfeil. Legen Sie eine Zugriffsart für die Geräte fest.

Standardmäßig besitzen die Geräte Vollzugriff. Wechselmedien, optische Laufwerke und Diskettenlaufwerke können gesperrt oder mit Lesezugriff ausgestattet werden. Sichere Wechselmedien können gesperrt werden.

## 14.4 Geräte-Ausschlüsse

Sie können Geräte von Device Control-Richtlinien ausschließen.

Sie können ein einzelnes Gerät („nur dieses Gerät“) oder einen Gerätetyp („alle Geräte des Typs“) ausschließen. Schließen Sie nicht ein bestimmtes Gerät und den entsprechenden Gerätetyp gleichzeitig aus. Wenn Ausschlüsse für beides festgelegt werden, hat das Einzelgerät Vorrang.

So können Sie ein Gerät ausschließen:

1. Klicken Sie im Menü **Ansicht** auf **Device Control-Ereignisse**.

Das Dialogfeld **Device Control – Ereignisanzeige** wird angezeigt.
2. Wenn nur ausgewählte Ereignisse angezeigt werden sollen, legen Sie im Feld **Suchkriterien** Filter fest und klicken Sie zur Anzeige der Ereignisse auf **Suchen**.

Weitere Informationen finden Sie unter [Anzeige von Device Control-Ereignissen](#) (Seite 21).
3. Wählen Sie das Gerät aus, das ausgeschlossen werden soll, und klicken Sie anschließend auf **Gerät ausschließen**.

Das Dialogfeld **Gerät ausschließen** wird angezeigt. Im Dialogfeld **Geräte-Details** werden Typ, Modell und ID des Geräts angezeigt.

## 15 Verwalten von Benachrichtigungen

### 15.1 Konfigurieren von Benachrichtigungen

Sie können Sophos Control Center zur Ausgabe von Alerts bei Erkennung von Threats im Netzwerk und/oder bei Änderungen des Netzwerkstatus konfigurieren. Zudem können Sie festlegen, wie Sophos Control Center mit alten Alerts umgeht.

E-Mail-Benachrichtigungen von Sophos Control Center fallen in zwei Kategorien:

- Die gewählten Empfänger werden bei Viren, verdächtigem Verhalten, unerwünschten Anwendungen oder Fehlern in einem der Computer im Netzwerk benachrichtigt. Solche Alerts werden über die Option **Scans konfigurieren > Benachrichtigungen** konfiguriert. Nähere Informationen hierzu finden Sie unter [Einrichten von Antivirus- und HIPS-Benachrichtigungen](#) (Seite 45).
- Die gewählten Empfänger werden benachrichtigt, wenn ein im Dashboard festgelegter Schwellenwert überschritten wurde. Sie können Alerts anhand einer der folgenden Methoden konfigurieren:
  - **Extras > E-Mail-Benachrichtigungen konfigurieren**
  - **Extras > Dashboard konfigurieren > E-Mail-Benachrichtigungen**

Nähere Informationen hierzu finden Sie unter [Einrichten von Netzwerkstatus-E-Mail-Benachrichtigungen](#) (Seite 46).

### 15.2 Einrichten von Antivirus- und HIPS-Benachrichtigungen

Sophos Control Center kann bei Erkennung von Viren oder potenziell unerwünschten Anwendungen im Netzwerk einen Alert auf dem Desktop anzeigen oder eine E-Mail-Benachrichtigung versenden.

So können Sie die Scan-Alerts einrichten:

1. Klicken Sie links unter **Konfiguration** auf **Scans konfigurieren**.
2. Klicken Sie im Fenster **Scans konfigurieren** auf **Benachrichtigungen**.
3. Standardmäßig sind im Feld **Benachrichtigungen** die Optionen **Desktop-Benachrichtigungen aktivieren** sowie alle Optionen im Feld **Bei folgenden Ereignissen eine Benachrichtigung senden**: aktiviert. Sie können diese Einstellungen bei Bedarf ändern.

Sie können im Textfeld **Benutzerdefinierter Text** eine Benachrichtigung eingeben, die an das Ende der Standard-Desktop-Benachrichtigung angehängt wird.

4. Wählen Sie auf der Registerkarte **E-Mail-Benachrichtigungen** die Option **E-Mail-Benachrichtigungen zulassen**, um E-Mail-Benachrichtigungen zu erhalten.

**Hinweis:** Zu von der Firewall gesperrten Objekten werden keine Alerts gesendet.

5. Wählen Sie unter **Bei folgenden Ereignissen eine Benachrichtigung senden:** die Ereignisse aus, zu denen jeweils eine E-Mail-Benachrichtigung gesendet werden soll.

**Hinweis:** Die Einstellungen zur Erkennung verdächtigen Verhaltens, Erkennung verdächtiger Dateien und zur Erkennung und Bereinigung von Adware und PUA gelten nur für Windows 2000 und aufwärts. Die Einstellung für Sonstige Fehler trifft nur für Windows zu.

6. Sie können im Bereich **Empfänger** durch Klicken auf **Hinzufügen** oder **Entfernen** die E-Mail-Adressen bestimmen, an die Benachrichtigungen gesendet werden sollen. Klicken Sie auf **Umbenennen**, um die E-Mail-Adresse zu ändern, die Sie hinzugefügt haben.

**Hinweis:** Mac OS X-Computer senden Benachrichtigungen nur an den ersten Empfänger in der Liste.

7. Klicken Sie auf die Schaltfläche **SMTP konfigurieren**, um die Einstellungen für den SMTP-Server und die Sprache der E-Mail-Benachrichtigungen zu ändern.
8. Geben Sie im Dialogfeld **SMTP-Einstellungen konfigurieren** die nachfolgend beschriebenen Details ein.

- Geben Sie in das Textfeld **SMTP-Server** den Hostnamen oder die IP-Adresse des SMTP-Servers ein. Klicken Sie auf **Test**, um eine Test-E-Mail-Benachrichtigung zu senden.
- Geben Sie in das Textfeld **SMTP-Absenderadresse** eine E-Mail-Adresse ein, an die nicht zustellbare Benachrichtigungen und Nicht-Zustellbarkeitsmeldungen gesendet werden sollen.
- Im Textfeld **SMTP-Adresse für Rückantworten:** können Sie eine E-Mail-Adresse angeben, an die Antworten auf E-Mail-Benachrichtigungen gesendet werden können. E-Mail-Benachrichtigungen werden von einem Systemkonto gesendet.  
**Hinweis:** Linux- und UNIX-Computer ignorieren „SMTP-Absender“- und „Rückantwort“-Adressen und verwenden die Adresse root@<hostname>.
- Klicken Sie im Bereich **Sprache** auf den Drop-Down-Pfeil und wählen Sie die Sprache, in der die E-Mail-Benachrichtigungen gesendet werden sollen.

## 15.3 Einrichten von Netzwerkstatus-E-Mail-Benachrichtigungen

Sie können einstellen, dass die von Ihnen ausgewählten Empfänger per E-Mail darüber benachrichtigt werden, wenn im Dashboard ein festgelegter Grenzwert erreicht wurde.

So können Sie E-Mail-Benachrichtigungen einrichten:

1. Wählen Sie im Menü **Extras** die Option **E-Mail-Benachrichtigungen konfigurieren**.

Das Dialogfeld **E-Mail-Benachrichtigungen konfigurieren** wird angezeigt.

2. Wenn die SMTP-Einstellungen nicht konfiguriert wurden oder wenn Sie die Einstellungen ansehen oder ändern möchten, klicken Sie auf **Konfigurieren**. Geben Sie in das Dialogfeld **SMTP-Einstellungen konfigurieren** Folgendes ein:
  - a) Geben Sie in das Textfeld **Serveradresse** den Hostnamen oder die IP-Adresse des SMTP-Servers ein.
  - b) Geben Sie in das Textfeld **Absender** eine E-Mail-Adresse ein, an die nicht zustellbare Benachrichtigungen und Nicht-Zustellbarkeitsmeldungen gesendet werden können.
  - c) Klicken Sie auf **Test**, um die Verbindung zu testen.
3. Klicken Sie im Bereich **Empfänger** auf **Hinzufügen**.  
Das Dialogfeld **Neuer E-Mail-Benachrichtigungsempfänger** wird angezeigt.
4. Geben Sie im Feld **E-Mail-Adresse** die Adresse des Empfängers ein.
5. Wählen Sie im Feld **Sprache** die Sprache, in der E-Mail-Benachrichtigungen gesendet werden sollen.
6. Wählen Sie im Feld **Abonnements** die Optionen für die E-Mail-Benachrichtigungen aus, wenn ein Schwellenwert überschritten wird.

Nähere Informationen zum Ändern der Grenzwerte entnehmen Sie bitte dem Abschnitt [Konfiguration des Dashboards](#) (Seite 9).

## 15.4 Einrichten von Application Control-Alerts

Sie können Benachrichtigungen an bestimmte Benutzer senden, wenn eine Controlled Application gefunden wird.

1. Klicken Sie links unter **Konfiguration** auf **Application Control konfigurieren**.  
Das Dialogfenster **Application Control konfigurieren** wird geöffnet.
2. Nehmen Sie auf der Registerkarte **Benachrichtigungen** die folgenden Einstellungen vor:
  - a) Im Bereich **Benachrichtigung** ist das Kontrollkästchen **Desktop-Benachrichtigung aktivieren** standardmäßig aktiviert.  
Wenn eine nicht zugelassene Controlled Application von On-Access-Scans erkannt und blockiert wird, wird eine Desktop-Benachrichtigung angezeigt, die den Benutzer darüber informiert, dass die Anwendung gesperrt wurde.
  - b) Sie können im Feld **Text** eine Meldung eingeben, die an eine Desktop-Benachrichtigung angehängt wird.
  - c) Aktivieren Sie das Kontrollkästchen **E-Mail-Benachrichtigungen aktivieren**, damit **Sophos Anti-Virus** E-Mail-Benachrichtigungen versendet. Nähere Informationen zu E-Mail-Benachrichtigungen können Sie dem Abschnitt [Einrichten von Antivirus- und HIPS-Benachrichtigungen](#) (Seite 45) entnehmen.

## 15.5 Einrichten von Device Control-Alerts

Ausgewählte Benutzer können über Device Control-Ereignisse benachrichtigt werden.

1. Klicken Sie auf der linken Seite unter **Konfiguration** auf **Device Control konfigurieren**.

Das Dialogfeld **Device Control konfigurieren** wird angezeigt.

2. Nehmen Sie auf der Registerkarte **Benachrichtigungen** die folgenden Einstellungen vor:

- a) Im Bereich **Benachrichtigung** ist das Kontrollkästchen **Desktop-Benachrichtigung aktivieren** standardmäßig aktiviert.

Wenn ein nicht zugelassenes Gerät von On-Access-Scans erkannt und blockiert wird, wird eine Desktop-Benachrichtigung angezeigt, die den Benutzer darüber informiert.

- b) Sie können im Feld **Text** eine Meldung eingeben, die an eine Desktop-Benachrichtigung angehängt wird.

- c) Aktivieren Sie das Kontrollkästchen **E-Mail-Benachrichtigungen aktivieren**, damit Sophos Control Center E-Mail-Benachrichtigungen versendet.

Geben Sie in das Feld **E-Mail-Empfänger** die E-Mail-Adressen der gewünschten Empfänger ein.

## 15.6 Löschen alter Alerts

Sie können Sophos Control Center so konfigurieren, dass alte Alerts automatisch gelöscht werden. Standardmäßig werden Alerts 12 Monate lang in der Datenbank gespeichert und anschließend gelöscht.

**Hinweis:** Ausstehende Alerts werden nicht gelöscht.

So werden alte Alerts gelöscht:

1. Wählen Sie im Menü **Extras** die Option **Reporting konfigurieren**.

Es öffnet sich das Dialogfeld **Reporting konfigurieren**.

2. Klicken Sie auf die Registerkarte **Löschen**.

Wählen Sie je nach Ihren Report-Anforderungen, wie Sie mit alten Alerts umgehen wollen.

- **Alte Alerts nicht löschen.**
- **Alerts löschen, die älter sind als  $n$  Monate** ( $n$  ist die von Ihnen gewählte Anzahl).

## 16 Report-Verwaltung

### 16.1 Erstellen eines Reports

Mit dem Report Manager können Sie verfügbare Reports erstellen.

So können Sie einen Report erstellen:

1. Klicken Sie im Fenster von Sophos Control Center in der Symbolleiste auf **Reports**.  
Der **Report Manager** wird angezeigt.
2. Wählen Sie die gewünschte Reportart aus.  
Nähere Informationen zum Erstellen eines neuen Reports finden Sie im Abschnitt [Erstellen eines neuen Reports](#) (Seite 49).
3. Klicken Sie auf **Ausführen**.  
Ein Report wird erstellt. Darin werden die Kriterien zusammengefasst, die der Erstellung zugrunde liegen.
4. Wählen Sie das gewünschte Anzeigeformat durch Klicken auf die entsprechende Registerkarte aus:  
**Hinweis:** Je nach Typ ist ggf. nur ein Anzeigeformat verfügbar:
  - **Diagramm**
  - **Tabelle**

### 16.2 Erstellen eines neuen Reports

Sie können Reports im Report Manager erstellen.

So können Sie einen Report erstellen:

1. Klicken Sie im Fenster von Sophos Control Center in der Symbolleiste auf **Reports**.  
Der **Report Manager** wird angezeigt.
2. Klicken Sie auf **Erstellen**.  
Das Fenster **Neuer Report** wird angezeigt.
  - Über den Assistenten: Wählen Sie die gewünschte Report-Vorlage aus dem Dropdown-Menü aus und klicken Sie auf **OK**.  
Der Assistent leitet Sie durch die Reporterstellung auf der Basis der gewählten Vorlage.
  - Über das Fenster „Eigenschaften“: Deaktivieren Sie die Option **Report mit Assistent erstellen** und klicken Sie auf **OK**.  
Das Fenster **Eigenschaften** wird geöffnet, in dem Sie die gewünschten Einstellungen vornehmen können.

## 16.3 Einrichten regelmäßiger Reports

Sophos Control Center kann Reports mit Angaben zur Anzahl und Art der erkannten Threats in einem bestimmten Zeitraum versenden.

Die Empfänger erhalten Reports mit den folgenden Informationen per E-Mail:

- Report-Datum
- Unternehmensname (Klicken Sie auf **Extras Reporting konfigurieren** und geben den Unternehmensnamen ein).
- Anzahl verdächtiger Dateien/Verhaltensmuster
- Anzahl der erkannten potenziell unerwünschten Anwendungen
- Anzahl erkannter Viren/Spyware.
- Liste der erkannten Threats in chronologischer Reihenfolge mit Anzeige des Threat-Namens und der Anzahl der Infektionen
- Liste der gesperrten Anwendungen in chronologischer Reihenfolge mit Anzeige des Namens der Anwendung und der Anzahl der betroffenen Computer. Sie können auch folgende Alerts einbeziehen: „Von Firewall blockiert“, „Controlled Applications“ und „Device Control“.

So können Sie regelmäßige Reports einrichten:

1. Klicken Sie im Fenster von Sophos Control Center in der Symbolleiste auf **Reports**.  
Der **Report Manager** wird angezeigt.
2. Wählen Sie einen vorhandenen Report aus und klicken Sie auf **Zeitplan**.  
Das Eigenschaftfenster **Reportname** wird angezeigt (wobei *Reportname* der Name des Reports ist).
3. Passen Sie auf der Registerkarte **Zeitplan** die Optionen an Ihre Bedürfnisse an:
  - a) Wählen Sie **Zeitplan für diesen Report erstellen** aus.
  - b) Geben Sie in den Feldern **Start** und **am** den Zeitpunkt (Datum und Uhrzeit) ein, zu dem der Report erstellt werden soll.  
Geben Sie im Dropdown-Menü **Wiederh.:** an, wie oft Reports erstellt werden sollen.
  - c) Geben Sie im Abschnitt **Ausgabe** das **Format** des E-Mail-Anhangs an.
  - d) Wählen Sie die **Sprache** aus, in der der Report erstellt werden soll.
  - e) Geben Sie die E-Mail-Adressen der gewünschten Empfänger ein und nehmen Sie sie in die Empfängerliste auf.  
Sie müssen die SMTP-Server-Einstellungen zum Versenden von E-Mails konfigurieren. Nähere Informationen hierzu können Sie dem Abschnitt [Einrichten von Netzwerkstatus-E-Mail-Benachrichtigungen](#) (Seite 46) entnehmen.

## 16.4 Ändern von Reports

Sie können einen vorhandenen Report ändern und Daten generieren.

So können Sie einen vorhandenen Report ändern:

1. Klicken Sie im Fenster von Sophos Control Center in der Symbolleiste auf **Reports**.
2. Wählen Sie im Dialogfeld **Report Manager** den gewünschten Report aus und klicken Sie auf **Eigenschaften**.

**Hinweis:** Je nach den gewählten Kriterien umfassen die Registerkarten möglicherweise nicht alle Optionen.

3. Wählen Sie auf der Registerkarte **Konfiguration** die gewünschten Optionen aus:

### ■ Report-Details

Geben Sie einen **Namen** ein, unter dem Sie den Report speichern möchten. Das Feld **Beschreibung** beinhaltet standardmäßig eine Beschreibung, die sich nach den von Ihnen gewählten Kriterien richtet.

### ■ Reporting-Zeitraum

Wählen Sie im Dropdown-Menü **Zeitraum** den gewünschten Zeitraum aus. Wählen Sie die Option **Benutzerdefiniert** und füllen Sie die Felder **Start** und **Ende** aus.

### ■ Speicherort für Reports

Wählen Sie zur Angabe des Computernamens das Dropdown-Menü **Alle Computer** oder **Einzelcomputer** aus.

### ■ Einzubeziehende Alerts

Wählen Sie die Alert-Arten aus, die in Reports berücksichtigt werden sollen.

Sie können den Report auch so konfigurieren, dass nur Computer angegeben werden, auf denen ein bestimmter Alert gemeldet wurde. Klicken Sie zur Angabe eines bestimmten Threats auf **Erweitert**.

Wählen Sie im Fenster **Erweiterte Konfiguration** aus, welche Alerts einbezogen werden sollen. Sie können in das Feld **Ausschluss** den Namen eines Threats eingeben. Durch die Verwendung von Wildcards können Sie mehrere Threats angeben. ? steht für ein einzelnes Zeichen im Namen und \* für eine Zeichenfolge. Zum Beispiel steht W32/\* für alle Viren, deren Namen mit W32/ beginnen.

4. Wählen Sie auf der Registerkarte **Anzeigeoptionen** die gewünschten Optionen aus:
  - Standardmäßig sind alle Einträge in der Liste **Anzeigeoptionen** ausgewählt. Sie können den Report auch dazu konfigurieren, nur Folgendes anzuzeigen:
    - Nur die ersten  $n$  Alerts (wobei  $n$  eine von Ihnen festgelegte Anzahl ist).
    - Nur Alerts, die  $n$ -mal oder öfter vorkommen.
  - **Ergebnisse pro**  
Standardmäßig werden Ergebnisse pro **Tag** angezeigt. Sie können den Wert jedoch auch in **Stunde**, **Woche** oder **Monat** ändern.
  - **Ergebnisse als**  
Standardmäßig werden die Ergebnisse als **Prozentsätze** angegeben. Die Ergebnisse können jedoch auch als **Zahlen** dargestellt werden.
  - **Geordnet nach**  
Als Standard listet der Report Threats absteigend nach der Anzahl der zugehörigen Alerts auf. Es kann jedoch auch nach **Alert-Name**, **Computername** oder **Datum und Uhrzeit** sortiert werden.
5. Wählen Sie auf der Registerkarte „Zeitplan“ die zu ändernden Optionen aus:
  - a) Wählen Sie **Zeitplan für diesen Report erstellen** aus.
  - b) Geben Sie in den Feldern **Start** und **am** den Zeitpunkt (Datum und Uhrzeit) ein, zu dem der Report erstellt werden soll.  
  
Sie können im Dropdown-Menü **Wiederh.** die gewünschte Wiederholungsfrequenz angeben.
  - c) Geben Sie im Abschnitt **Ausgabe** das **Dateiformat** des E-Mail-Anhangs an.
  - d) Wählen Sie die **Sprache** aus, in der der Report erstellt werden soll.
  - e) Geben Sie die E-Mail-Adressen der gewünschten Empfänger ein und nehmen Sie sie in die Empfängerliste auf.  
Weitere Informationen zur Konfiguration oder zum Hinzufügen von E-Mail-Adressen finden Sie unter [Einrichten von Netzwerkstatus-E-Mail-Benachrichtigungen](#) (Seite 46).

## 16.5 Exportieren eines Reports in eine Datei

Reports können nach der Erstellung in verschiedenen Formaten exportiert werden.

So exportieren Sie einen Report in eine Datei:

1. Klicken Sie im Fenster von Sophos Control Center in der Symbolleiste auf **Reports**.  
Der **Report Manager** wird angezeigt.
2. Wählen Sie einen Report aus, den Sie exportieren möchten und klicken Sie auf **Ausführen**.

3. Klicken Sie im Fenster **Reports** auf das **Exportsymbol** in der Symbolleiste.



4. Wählen Sie im Dialogfeld **Export-Report** den Dokument- oder Tabellentyp für den exportierten Report aus.
5. Klicken Sie auf die Schaltfläche neben dem Feld **Dateiname**, um einen Speicherort auszuwählen.
6. Wählen Sie im Dialogfeld **Speichern unter** den gewünschten Report-Speicherort aus, geben Sie einen Report-Namen ein und klicken Sie auf **Speichern**.
7. Klicken Sie im Dialogfeld **Export-Report** auf **OK**.

## 16.6 Ändern des Report-Layouts

Sie können das Seitenlayout von Reports ändern. Sie können sich beispielsweise einen Report im Querformat anzeigen lassen.

So können Sie das Report-Layout ändern:

1. Klicken Sie im Fenster von Sophos Control Center in der Symbolleiste auf **Reports**.  
Der **Report Manager** wird angezeigt.
2. Wählen Sie einen Report aus und klicken Sie auf **Ausführen**.
3. Klicken Sie im Fenster **Reports** auf das **Seitenlayoutsymbol** in der Symbolleiste.



4. Geben Sie im Dialogfeld **Seite einrichten** das Seitenformat, die Ausrichtung und die Ränder ein. Klicken Sie auf **OK**. Der Report wird im gewählten Format angezeigt.
5. Das Format wird auch beim Drucken oder Exportieren von Reports übernommen.

## 17 Fehlersuche

### 17.1 Bereinigung fehlgeschlagen

Wenn sich Threats nicht zentral entfernen lassen, gehen Sie zu dem betroffenen Computer und führen Sie die Bereinigung manuell durch.

Wenn der Threat nicht beseitigt wurde und Sie Unterstützung zur Problembeseitigung benötigen, verfahren Sie wie folgt:

1. Schreiben Sie sich den Threat-Namen auf.
2. Klicken Sie auf der linken Seite unter **Informationen** auf **Threat-Daten**, um die Threat-Analysen auf der Sophos Website aufzurufen.
3. Suchen Sie auf der Analyseseite nach dem Threat. Über die Links erhalten Sie Anweisungen zur Bereinigung.

Wenn Sie den Threat nicht beseitigen können, klicken Sie unter **Informationen** auf **Technischer Support**.

Geben Sie den Threat-Namen und Details zu dem/den betroffenen Computer(n) in der E-Mail an.

### 17.2 Hohe Alert-Anzahl aufgrund potenziell unerwünschter Anwendungen

Es kann vorkommen, dass zahlreiche Alerts aufgrund potenziell unerwünschter Anwendungen ausgegeben werden, die sich unter Umständen jedoch auf die gleiche Anwendung beziehen.

Dies kann daran liegen, dass bestimmte potenziell unerwünschte Anwendungen Dateien „überwachen“ und versuchen, häufig auf sie zuzugreifen. Wenn On-Access-Scans aktiviert sind, werden alle Dateizugriffe von Sophos Anti-Virus erkannt und mehrere Alerts ausgegeben.

Führen Sie einen der folgenden Schritte durch:

- Deaktivieren Sie On-Access-Scans für potenziell unerwünschte Anwendungen. Sie können stattdessen eine geplante Scan verwenden.
- Lassen Sie die Anwendung zu, wenn sie auf Ihren Computern ausgeführt werden soll. Nähere Informationen hierzu finden Sie unter [Zulassen von Anwendungen](#) (Seite 29).
- Bereinigen Sie Anwendungen, die Sie nicht zugelassen haben. Nähere Informationen hierzu finden Sie unter [Computer-Bereinigung](#) (Seite 14).

## 18 Technischer Support

Technischen Support zu Sophos Produkten können Sie wie folgt abrufen:

- Rufen Sie das SophosTalk-Forum unter <http://community.sophos.com/> auf und suchen Sie nach Benutzern mit dem gleichen Problem.
- Durchsuchen Sie die Sophos Support-Knowledgebase unter <http://www.sophos.de/support/>.
- Laden Sie Dokumentation zu den Produkten unter <http://www.sophos.de/support/docs/> herunter.
- Senden Sie eine E-Mail an den technischen Support [support@sophos.de](mailto: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.

## 19 Copyright

Copyright © 2010 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 von Sophos Plc und Sophos Group. Alle anderen erwähnten Produkt- und Unternehmensnamen sind Marken oder eingetragene Marken der jeweiligen Inhaber.

Die in dieser Anleitung beschriebene Sophos Software kann Programme enthalten, die unter der Common Public License (CPL) laufen, die u.a. den Quellcode frei zugänglich macht. Für jede Software, die unter den Bedingungen der CPL lizenziert und als Objektcode veröffentlicht wird, muss außerdem den Lizenzinhabern auch der Quellcode zur Verfügung gestellt werden. 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](mailto:support@sophos.de) or via the web at <http://www.sophos.de/support/queries/enterprise.html>. A copy of the license agreement for any such included software can be found at <http://opensource.org/licenses/cpl1.0.php>

### **ACE™, TAO™, CIAO™, and CoSMIC™**

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

Since DOC software is open-source<sup>10</sup>, 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<sup>11</sup> know so we can promote your project in the DOC software success stories<sup>12</sup>.

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<sup>13</sup> 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<sup>14</sup>, TAO<sup>15</sup>, CIAO<sup>16</sup>, and CoSMIC<sup>17</sup> web sites are maintained by the DOC Group<sup>18</sup> at the Institute for Software Integrated Systems (ISIS)<sup>19</sup> and the Center for Distributed Object Computing of Washington University, St. Louis<sup>20</sup> for the development of open-source software as part of the open-source software community<sup>21</sup>. 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, Washington University, 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<sup>22</sup> know.

Douglas C. Schmidt<sup>23</sup>

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](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

- Aktivieren von On-Access-Scans 24
- Alerts
  - Anti-Virus 45
  - Application Control 47
  - Dashboard 46
  - Device Control 48
  - HIPS 45
  - Konfigurieren 45
  - Löschen 48
  - Netzwerkstatus 46
- Ändern
  - Benutzererkennung 33
  - Proxyserver 33
  - Reports 51
- Anzeigen von Computern 19
- Application Control 39
  - Alerts 47
  - Ereignisse 21
- Assistent zum Schützen von Computern 10
- Auffinden gelöschter Computer 19
- Ausschließen von geplanten Scans 31
- Ausschließen von Objekten 27
- automatische Bereinigung 27
  - PUA 28
  - Viren 28

### B

- Benutzeroberfläche
  - Endpoint-Ansicht 4
  - Update Manager-Ansicht 4
- Benutzeroberfläche von Sophos Control Center 4
- Bereinigen
  - Alerts 16
  - Fehler 16
  - Threats 14
- Bereinigung 14
  - fehlgeschlagen 54

### C

- Computerstatus 19
- Controlled Applications
  - Auswählen von Anwendungen 40

- Controlled Applications (*Fortsetzung*)
  - sperren 39

### D

- Dashboard
  - Konfigurieren 9
  - Überblick 8
- Deaktivieren
  - Automatische Updates 34
  - Firewall
    - Einzelcomputer 37
    - Sophos Control Center 37
- Deinstallieren
  - Controlled Applications 40
- Deinstallieren von Controlled Applications 40
- Desinfektion/Beseitigung 14
- Desktop-Benachrichtigung 45
- Device Control
  - Aktivieren von Device Control 43
  - Alerts 48
  - Ereignisse 21
  - Geräte-Ausschlüsse 44
  - Gerätetypen 42
  - Netzwerk
    - kurze Reichweite 42
  - Netzwerkbrücken sperren 42
  - Speicher 42
  - Übersicht 42
- Druckübersicht 20

### E

- Endpoint-Ansicht 4
- Ereignisse 21
  - Application Control 21
  - Device Control 21
  - Exportieren in eine Datei 23
  - Firewall 22
  - Kopieren von Ereignissen in die Zwischenablage 23
- Erneuter Schutz von Computern 17
- Erstellen
  - Reports 49
- Exportieren
  - Reports 52

## F

### Fehlersuche

- Bereinigung 54
- Hohe Alert-Anzahl 54
- PUA 54

### fehlgeschlagene Bereinigung 54

### Firewall

- Deaktivieren der Firewall auf einzelnen Computern 37
- Deaktivieren von Sophos Control Center 37
- Einrichten 36
- Ereignisse 22
- Individuelle Konfiguration 38
- Zulassen von Anwendungen 38

## G

### Geplante Scans 24, 29

### geschützte Computer 19

### geschütztes Netzwerk 19

## I

### Informationen zu Threats 16

## K

### Konfigurieren des Dashboards 9

### Konfigurieren von Dateien

- Mac 26
- Windows 26

### Konfigurieren von On-Access-Scans 24

## L

### Layout

- Reports 53

### Letztes Update 12

### Lokale Konfigurationen 18

### Löschen

- Alerts 16
- Fehler 16

## M

### manuelle Updates 13

## N

### Netzwerk-Updates 13

### Neübernahme der zentralen Konfiguration 18

### Nicht aktuelle Computer

- Updates 13

## O

### On-Access-Scan-Optionen 25

## P

### Priorität von Alerts 7

### PUA

- Hohe Alert-Anzahl 54

## R

### Reports

- Ändern 51
- Erstellen 49
- Exportieren 52
- Layout 53
- Zeitplan 50

## S

### Scan-Konfiguration 32

### Scan-Optionen

- ausgeschlossene Datei 26
- Ausschließen von Erweiterungen 26

### Scannen

- On-Access 24, 25
- PUA 24

### Scannen einzelner Computer 32

### Schützen von Betriebssystemen 11

### Schützen von Computern

- Assistent zum Schützen von Computern 10

### Sofort-Updates 13

### Sophos Control Center 3, 4

### sperren

- Controlled Applications 39

### Symbole 5

## U

### Übernahme der Konfigurationseinstellungen 18

### Überprüfen des Netzwerks 19

### Überprüfung des Updates 12

Update-Vorgang 12

Updates

    Auswählen von Anwendungen 33

    automatisch 34

    Benutzerkennung 33

    Intervall 34

    ohne Netzwerk 34

    Proxyserver 33

Updates auf einzelnen Computern 13

## V

verdächtige Dateien 28

verwaltete Computer 5

vom Netzwerk getrennte Computer 5

## W

Warnsymbole 5

Web-Scanning 27

## Z

Zeitplan

    Reports 50

Zeitplanoptionen 30

zentrale Konfiguration 18

Zulassen von Anwendungen 29