

SOPHOS

Sophos Enterprise Console Hilfe

Produktversion: 4.5
Stand: Juni 2010



Inhalt

1	Sophos Enterprise Console.....	4
2	Einführung in Enterprise Console.....	5
3	Vorbereitung.....	10
4	Verwalten von Rollen und Teilverwaltungseinheiten.....	13
5	Erstellen und Einsatz von Gruppen.....	23
6	Erstellen und Einsatz von Richtlinien.....	26
7	Computersuche im Netzwerk.....	32
8	Synchronisierung mit Active Directory.....	36
9	Schützen von Computern.....	43
10	Ermitteln des Netzwerkschutzes.....	48
11	Benachrichtigungen, Alerts und Fehlermeldungen.....	54
12	Bereinigen von Computern.....	58
13	Ereignisanzeige.....	62
14	Scannen von Computern.....	67
15	Updates.....	68
16	Konfigurieren von Software-Abonnements.....	70
17	Konfigurieren des Update Managers.....	73
18	Konfigurieren der Antivirus- und HIPS-Richtlinie.....	83
19	Konfigurieren der Update-Richtlinie.....	103
20	Alte Update-Richtlinien.....	110
21	Konfigurieren der Firewall-Richtlinie.....	120
22	Konfigurieren der Application Control-Richtlinie.....	130
23	Konfigurieren der Data Control-Richtlinie.....	133
24	Konfigurieren der Device Control-Richtlinie.....	149
25	Konfigurieren der NAC-Richtlinie.....	157
26	Konfigurieren der Manipulationsschutz-Richtlinie.....	160
27	Alerts.....	163
28	Erstellen von Reports.....	173

29 Kopieren und Drucken von Daten mit Enterprise Console.....	185
30 Wie kann ein anderer Anwender Enterprise Console nutzen?.....	187
31 Aktivieren/Deaktivieren von Reports an Sophos.....	188
32 Fehlerbehebung.....	189
33 Glossar.....	197
34 Technischer Support.....	204
35 Rechtlicher Hinweis.....	205

1 Sophos Enterprise Console

Bei Sophos Enterprise Console, Version 4.5, handelt es sich um eine eigenständige, automatisierte Konsole, mit der Sophos Sicherheitssoftware unter Windows, Mac, Linux und UNIX zentral installiert und verwaltet wird. Enterprise Console umfasst die folgenden Funktionen:

- Schutz des Netzwerks vor Viren, Trojanern, Würmern, Spyware, schädlichen Websites, unbekanntem Threats, Adware und sonstigen potenziell unerwünschten Anwendungen.
- Kontrolle der Anwendungen, die im Netzwerk ausgeführt werden dürfen.
- Verwalten des Client Firewall-Schutzes auf Endpoints.
- Bewerten der Konformität von Computern mit den festgelegten Bedingungen vor der Anmeldung im Netzwerk und Richtliniendurchsetzung.
- Verhindern unerwünschter Datenverluste von Endpoints (z.B. versehentliche Übertragung sensibler Daten).
- Verhindern, dass Benutzer nicht zugelassene externe Speichermedien und Wireless-Geräte auf Endpoints einsetzen.
- Verhindern, dass Benutzer Sophos Sicherheitssoftware umkonfigurieren, deaktivieren oder deinstallieren.

Wenn Sie noch nicht mit Enterprise Console gearbeitet haben, bietet der Abschnitt [Vorbereitung](#) (Seite 10) eine Einführung.

2 Einführung in Enterprise Console

2.1 Die Benutzeroberfläche

Sie können Sicherheitssoftware von Sophos über die Benutzeroberfläche von Sophos Enterprise Console nutzen und konfigurieren. Die Hauptfunktionen werden im Folgenden ausgeführt.

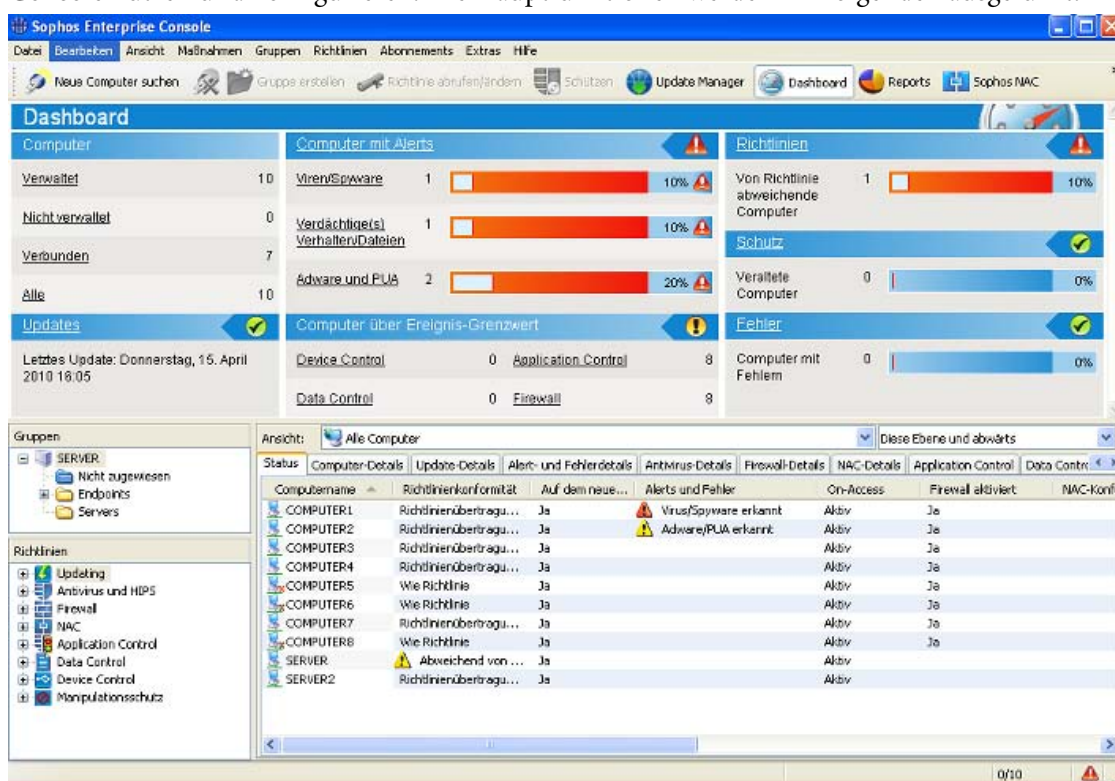


Abbildung 1: Enterprise Console – Ansicht „Endpoints“

Das 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**. Nähere Informationen zum Dashboard können Sie dem Abschnitt [Übersicht über das Dashboard](#) (Seite 48) entnehmen.

Die Computerliste

Die Computerliste auf der rechten Seite bietet zwei Ansichten, die Ansicht **Endpoints** und die Ansicht **Update Manager**. Sie können in eine andere Ansicht wechseln, indem Sie in der Symbolleiste auf **Update Manager** bzw. **Endpoints** klicken.

Die Ansicht **Endpoints** zeigt die Computer der gewählten Gruppe an. Die Ansicht umfasst diverse Registerkarten. Aus der Registerkarte **Status** geht hervor, bei welchen Computern On-Access-Scans aktiviert sind, ob die Computer mit den Gruppenrichtlinien konform sind, welche Funktionen aktiviert sind und ob sich die Software auf dem neuesten Stand befindet. Außerdem werden hier ggf. Alerts angezeigt. Auf den anderen Registerkarten finden Sie weitere Details zu den genannten Themen.

Im Abschnitt *Was bedeuten die Symbole?* (Seite 8) werden die Symbole in der Computerliste näher erläutert.

Die Informationen der Computerliste in der Ansicht **Endpoints** können Sie kopieren oder ausdrucken. Mehr dazu erfahren Sie im Abschnitt „Kopieren und Drucken von Daten mit Enterprise Console“.

Auf der Registerkarte **Update Manager** werden die Computer angezeigt, auf denen Sophos Update Manager installiert ist. In dieser Ansicht können Sie automatische Updates für Sophos Sicherheitssoftware von der Sophos Website einrichten und den Status sowie weitere Informationen zu den Update Managern aufrufen.

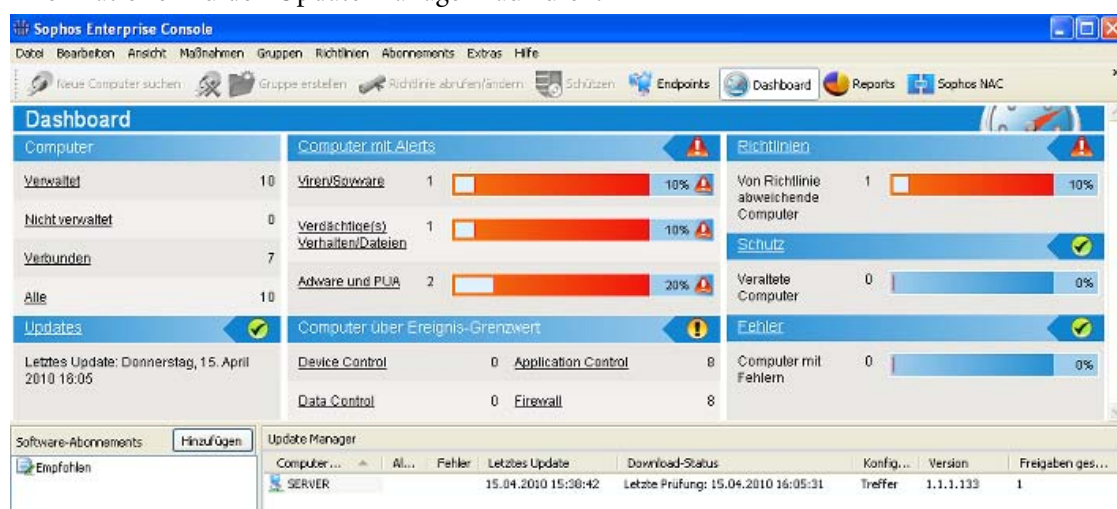


Abbildung 2: Enterprise Console – Ansicht „Update Manager“

Der Fensterbereich „Gruppen“

Der Fensterbereich **Gruppen** wird in der Ansicht **Endpoints** angezeigt. Im Fensterbereich **Gruppen** können Sie Gruppen erstellen und diesen Netzwerkcomputern zuweisen. Sie können selbst Gruppen erstellen oder Active Directory-Container mit oder ohne Computer importieren und als Enterprise Console-Computergruppen einsetzen.

Die Gruppe **Nicht zugewiesen** ist für Computer bestimmt, die sich noch nicht in einer von Ihnen erstellten Gruppe befinden. Rechtsklicken Sie auf eine Gruppe, die Sie konfigurieren möchten.

Fensterbereich „Richtlinien“

Der Fensterbereich **Richtlinien** wird in der Ansicht **Endpoints** angezeigt. Im Fensterbereich **Richtlinien** erstellen oder ändern Sie die Richtlinien, die auf Computergruppen übertragen werden. Rechtsklicken Sie auf eine Richtlinie, die Sie konfigurieren möchten.

Fensterbereich „Software-Abonnements“

Der Fensterbereich **Software-Abonnements** wird in der Ansicht **Update Manager** angezeigt. Im Fensterbereich **Software-Abonnements** können Sie Software-Abonnements erstellen oder ändern und so angeben, welche Versionen der Endpoint-Software für das jeweilige System von Sophos heruntergeladen werden.

Die Symbolleiste

Computer suchen sucht nach Computern im Netzwerk und fügt sie zur Konsole hinzu.

Gruppe erstellen erstellt eine neue Gruppe für Computer.

Mit **Richtlinie ansehen/bearbeiten** können Sie eine Richtlinie öffnen und ändern, die im Fensterbereich **Richtlinien** ausgewählt wurde.

Mit **Schützen** können Sie Virenschutz- und Firewall-Software auf Computern installieren, die in der Computerliste ausgewählt wurden.

Über die Option **Update Manager/Endpoints** können Sie die Ansicht der Computerliste ändern.

Mit **Reports** können Sie Reports zu Meldungen und Ereignissen im Netzwerk erstellen.

Dashboard öffnet die Dashboard-Ansicht, die Ihnen einen Überblick über den Netzwerksicherheitsstatus verschafft.

Sophos NAC öffnet Sophos NAC Manager, mit dem Sie NAC-Richtlinien ändern können.

2.2 Was ist eine Gruppe?

Eine Gruppe  ist ein Ordner mit mehreren Computern.

Sie können selbst Gruppen erstellen oder Active Directory-Container mit oder ohne Computer importieren und als Enterprise Console Computergruppen einsetzen. Sie können außerdem eine Synchronisierung mit Active Directory einstellen, damit neue Computer und Container sowie andere Änderungen in Active Directory automatisch auf Enterprise Console übertragen werden.

Jede Gruppe hat eigene Einstellungen für Updates, Viren- und HIPS-Schutz, Firewall-Schutz usw. Alle Computer einer Gruppe sollten in der Regel mit diesen Einstellungen („Richtlinie“) arbeiten.

Eine Gruppe kann Untergruppen enthalten.

2.3 Was ist eine Richtlinie?

In einer Richtlinie werden Einstellungen zusammengefasst, die für alle Computer in einer Gruppe gelten.

Bei der Installation von Enterprise Console werden Standardrichtlinien erstellt, die für einen Basisschutz sorgen. Diese Richtlinien werden auf neu erstellte Gruppen übertragen. Sie können die Standardrichtlinien ändern oder neue Richtlinien erstellen.

Nähere Informationen über die unterschiedlichen Richtlinienarten finden Sie im Abschnitt [Wofür gibt es Richtlinien?](#) (Seite 26).

2.4 Wozu dient die Gruppe „Nicht zugewiesen“?

Enterprise Console legt Computer vor der Einteilung in der Gruppe **Nicht zugewiesen** ab.

Sie können nicht:



- Richtlinien auf die Gruppe **Nicht zugewiesen** übertragen.
- Weitere Gruppen in der Gruppe **Nicht zugewiesen** erstellen.
- Die Gruppe **Nicht zugewiesen** verschieben oder löschen.

2.5 Was bedeuten die Symbole?

Symbole in der Computerliste in der Ansicht **Endpoints** weisen auf Folgendes hin:

- Alerts.
- Schutz deaktiviert oder nicht aktuell.
- Status aller Computer, z.B. ob Software installiert wird.




Alerts

Symbol	Erklärung
	Ein rotes Warnsymbol auf der Registerkarte Status in der Spalte Alerts und Fehler deutet darauf hin, dass ein Virus, Wurm, Trojaner, Spyware oder verdächtiges Verhalten erkannt wurde.
	Ein gelbes Warnsymbol auf der Registerkarte Status in der Spalte Alerts und Fehler deutet auf eins der folgenden Probleme hin: <ul style="list-style-type: none"> ■ Eine verdächtige Datei wurde erkannt. ■ Adware oder eine andere potenziell unerwünschte Anwendung wurde erkannt. ■ Ein Fehler ist aufgetreten. Ein gelbes Warnsymbol in der Spalte Richtlinienkonformität weist darauf hin, dass die Richtlinie(n) des Computers von den anderen Computern der Gruppe abweichen.







Wenn für einen Computer mehrere Alerts oder Fehler vorhanden sind, wird in der Spalte **Alerts und Fehler** 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)

Schutz deaktiviert oder nicht aktuell

Symbol	Erklärung
	Ein graues Schildsymbol bedeutet, dass On-Access-Scans nicht aktiviert sind.
	Ein graues Firewall-Symbol bedeutet, dass die Firewall deaktiviert ist.
	Ein Uhrensymbolsymbol bedeutet, dass die Software nicht aktuell ist.

Computerstatus

Symbol	Erklärung
	Ein blaues Computer-Symbol bedeutet, dass der Computer von der Enterprise Console 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 bedeutet, dass die Komponente der Endpoint-Schutz-Software für automatische Updates installiert wurde und nun die neueste Version des Produkts herunterlädt.
	Ein graues Computer-Symbol bedeutet, dass der Computer nicht von Enterprise Console verwaltet wird.
	Ein Computersymbol, neben dem sich ein rotes Kreuz befindet, weist darauf hin, dass ein Computer, der von Enterprise Console verwaltet wird, nicht mit dem Netzwerk verbunden ist. (Nicht verwaltete Computer, die nicht mit dem Netzwerk verbunden sind, werden nicht angezeigt).

3 Vorbereitung

Im Folgenden werden die Schritte zusammengefasst, die Sie nach der Installation von Enterprise Console und dem Ausführen des **Download-Assistenten für Sicherheitssoftware** durchführen müssen, um Ihr Netzwerk zu schützen. Nähere Informationen zu Enterprise Console finden Sie im Begleitmaterial und den genannten Abschnitten.

Praxistipps zum Einsatz und zur Verwaltung von Sophos Sicherheitssoftware finden Sie in der *Sophos Endpoint Security and Control Richtlinienanleitung*. Begleitmaterial zu Sophos Software finden Sie hier: www.sophos.de/support/docs/.

Wenn Sie den **Download-Assistenten für Sicherheitssoftware** nicht ausgeführt haben, lesen Sie den Abschnitt *Ausführen des Download-Assistenten für Sicherheitssoftware* (Seite 72).

Verfahren Sie wie folgt, um Ihr Netzwerk zu schützen:

1. Erstellen Sie Gruppen.

Sie können selbst Gruppen erstellen oder Gruppen aus Active Directory-Containern mit oder ohne Computer importieren und als Enterprise Console Computer-Gruppen einsetzen.

Anweisungen zum Importieren von Active Directory-Containern finden Sie unter *Importieren von Containern und Computern aus Active Directory* (Seite 32). Es empfiehlt sich, Active Directory-Container zunächst ohne Computer zu importieren, den Gruppen dann Gruppenrichtlinien zuzuweisen und Computer in die Gruppen (z.B. durch Synchronisieren der Gruppen mit Active Directory) aufzunehmen.

Nähere Informationen zur manuellen Erstellung von Gruppen finden Sie im Abschnitt „Erstellen und Einsatz von Gruppen“.

2. Erstellen/Konfigurieren Sie Richtlinien.

Enterprise Console bietet diverse Standardrichtlinien, die für den Netzwerkschutz unerlässlich sind. Die Standard-**Update-** und **Antivirus- und HIPS-**Richtlinie können Sie ohne Vornahme weiterer Einstellungen übernehmen. Die Firewall-Richtlinie muss mit dem **Firewall-Richtlinienassistenten** konfiguriert werden. Mehr dazu erfahren Sie unter *Einrichten der Firewall* (Seite 120).

3. Suchen Sie Computer im Netzwerk und fügen Sie sie zur Konsole hinzu.

Wenn Sie bereits in Schritt 1 Container und Computer aus Active Directory importiert haben, können Sie diesen Schritt überspringen. Wenn dies nicht der Fall ist, entnehmen Sie bitte dem Abschnitt „Computersuche im Netzwerk“ weitere Anweisungen.

4. Schützen Sie die Computer.

Sie können zwischen zwei Methoden zum Schutz Ihrer Computer im Netzwerk wählen:

■ **Der Assistent zum Schutz für Computer**

Wenn Sie einen Computer aus der Gruppe **Nicht zugewiesen** in eine andere Gruppe ziehen, wird ein Assistent gestartet, mit dessen Hilfe Sie die Computer schützen können. Details hierzu finden Sie im Abschnitt „Schützen neuer Computer“.

■ **Automatischer Schutz von Computern bei der Synchronisierung mit Active Directory**

Wenn Sie mit Active Directory synchronisieren möchten, können Sie auch Ihre Computer mit Windows 2000 und höher automatisch schützen. Dies stellen Sie im **Assistenten zur Synchronisierung mit Active Directory** oder im Dialogfeld **Synchronisierungseigenschaften** ein. Anweisungen hierzu finden Sie unter [Automatisches Schützen von Computern über Synchronisierung](#) (Seite 40).

5. Überprüfen Sie, ob die Computer geschützt sind.

Wenn die Installation abgeschlossen ist, sehen Sie sich noch einmal die Computerliste in der neuen Gruppe an. In der Spalte **On-Access** sollte „aktiv“ stehen: Das bedeutet, dass der Computer durch die On-Access-Scanfunktion geschützt und von Enterprise Console verwaltet wird. Weitere Informationen finden Sie unter [So überprüfen Sie, ob Ihr Netzwerk geschützt ist](#) (Seite 48).

6. Führen Sie eine Bereinigung der Computer durch.

Wenn ein Virus, ein sonstiges Objekt oder eine unerwünschte Anwendung im Netzwerk erkannt wird, bereinigen Sie die betroffenen Computer anhand der Anweisungen im Abschnitt „Bereinigen von Computern“.

Weitere Schutz- und Verwaltungsoptionen

Standardmäßig erkennt Sophos Endpoint Security and Control Viren, Trojaner, Würmer und Spyware. Sophos Anti-Virus 7 und höher für Windows 2000 und höher analysiert außerdem das Verhalten der Programme, die auf dem System ausgeführt werden. Sie können weitere Schutzmechanismen hinzufügen, z.B. Schutz vor Adware, potenziell unerwünschten Anwendungen (PUA), verdächtigem oder unerwünschtem Verhalten oder ungewollten Datenverlusten über Computer. In den folgenden Abschnitten finden Sie weitere Informationen:

- [Die Antivirus- und HIPS-Richtlinie](#) (Seite 83)
- [Einrichten der Firewall](#) (Seite 120)
- [Application Control](#) (Seite 130)
- [Data Control](#) (Seite 133)
- [Device Control](#) (Seite 149)
- [NAC](#) (Seite 157)
- [Allgemeine Informationen](#) (Seite 160)

In Enterprise Console können Sie verschiedene *Rollen* erstellen und diesen Rechte und Windows-Benutzer und -Gruppen zuweisen. Die Rolle „Systemadministrator“, zu der auch die Windows-Gruppe „Sophos Full Administrators“ zählt, besitzt uneingeschränkte

Zugriffsrechte und muss nicht eigens eingerichtet werden. Näheres zu den einzelnen Rollen entnehmen Sie bitte dem Abschnitt „Verwalten von Rollen und Teilverwaltungseinheiten“.

Sie können Ihre IT-Verwaltungseinheit in *Teilverwaltungseinheiten* aufgliedern und den Teilverwaltungseinheiten Enterprise Console-Computergruppen zuweisen. Sie können den Zugriff auf die Teilverwaltungseinheiten regeln, indem Sie ihnen Windows-Benutzer und -Gruppen zuweisen. Die Teilverwaltungseinheit **Standard** umfasst alle Enterprise Console-Gruppen und die Gruppe **Nicht zugewiesen**. Näheres zu Teilverwaltungseinheiten entnehmen Sie bitte dem Abschnitt „Verwalten von Rollen und Teilverwaltungseinheiten“.

4 Verwalten von Rollen und Teilverwaltungseinheiten

4.1 Rollen und Teilverwaltungseinheiten

Wichtig: Wenn Sie bereits mit rollenbasierter Verwaltung arbeiten, müssen Sie zum Einrichten von Rollen und Teilverwaltungseinheiten über die Berechtigung **Rollenbasierte Verwaltung** verfügen. Die Rolle „Systemadministrator“, zu der auch die Windows-Gruppe „Sophos Full Administrators“ zählt, besitzt uneingeschränkte Zugriffsrechte und muss nicht eigens eingerichtet werden. Mehr dazu erfahren Sie unter [Vordefinierte Rollen](#) (Seite 14) und [Aufgabenbereich der Berechtigungen](#) (Seite 18).

Wenn Sie rollenbasierten Zugriff zur Konsole einrichten möchten, können Sie Rollen erstellen, ihnen Rechte zuweisen und ihnen Windows-Benutzer und -Gruppen zuteilen. Zum Beispiel kann ein Helpdesk-Techniker Computer updaten und bereinigen, jedoch keine Richtlinien konfigurieren, da dies die Aufgabe eines Administrators ist.

Zum Öffnen von Enterprise Console muss ein Benutzer der Gruppe „Sophos Console Administrators“ angehören und mindestens einer Enterprise Console-Rolle und -Teilverwaltungseinheit zugewiesen worden sein. Mitglieder der Gruppe „Sophos Full Administrators“ besitzen uneingeschränkten Zugriff auf Enterprise Console.

Hinweis: Nähere Informationen zum Gewähren des Zugriffs auf eine Remote-Enterprise Console oder weitere Instanz von Enterprise Console finden Sie unter [Wie kann ein anderer Anwender Enterprise Console nutzen?](#) (Seite 187).

Sie können selbst Rollen erstellen oder die Voreinstellungen übernehmen.

Benutzer können beliebig viele Rollen erhalten: Weisen Sie die Rolle dem Benutzer oder einer Windows-Gruppe zu, der er angehört.

Wenn ein Benutzer eine bestimmte Aufgabe von der Konsole aus nicht ausführen darf, besitzt er dennoch Lesezugriff auf die entsprechenden Konfigurationseinstellungen. Benutzer, denen keine Rollen zugewiesen wurden, können Enterprise Console nicht öffnen.

Sie können außerdem die Computer und Gruppen beschränken, auf die Benutzer zugreifen können. Sie können Ihre IT-Verwaltungseinheit in Teilverwaltungseinheiten aufgliedern und den Teilverwaltungseinheiten Enterprise Console-Computergruppen zuweisen. Sie können den Zugriff auf die Teilverwaltungseinheiten regeln, indem Sie ihnen Windows-Benutzer und -Gruppen zuweisen. Die Teilverwaltungseinheit **Standard** umfasst alle Enterprise Console-Gruppen und die Gruppe **Nicht zugewiesen**.

Benutzer können nur die Teilverwaltungseinheiten aufrufen, wenn sie ihnen zugewiesen wurden. Benutzer, die mehreren Teilverwaltungseinheiten zugewiesen wurden, können bestimmen, welche Teilverwaltungseinheit angezeigt werden soll. Es kann jeweils nur eine Teilverwaltungseinheit aufgerufen werden. Die in Enterprise Console geöffnete Teilverwaltungseinheit wird als *aktive Teilverwaltungseinheit* bezeichnet. Benutzer können keine Änderungen an Richtlinien vornehmen, die sich nicht in ihrer aktiven Teilverwaltungseinheit befinden.

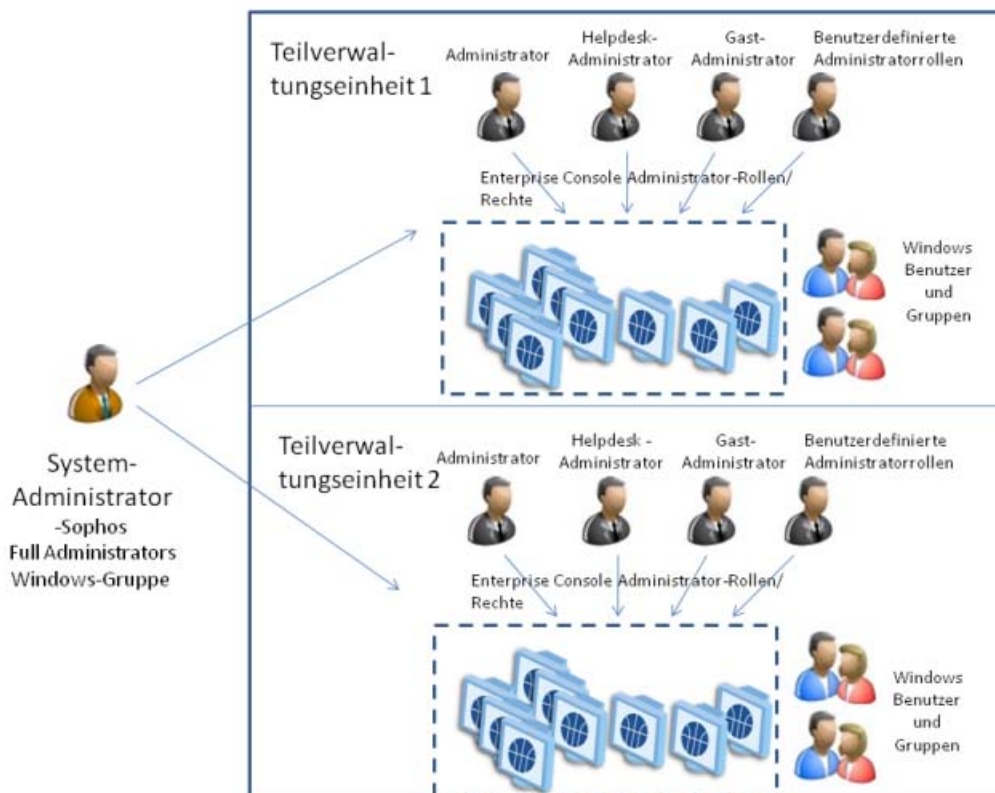


Abbildung 3: Rollen und Teilverwaltungseinheiten

4.2 Vordefinierte Rollen

Enterprise Console bietet vier vordefinierte Rollen:

Rolle	Beschreibung
Systemadministrator	Eine vorkonfigurierte Rolle für die Verwaltung von Sophos Sicherheitssoftware im Netzwerk und Rollen in Enterprise Console. Sie können die Rolle „Systemadministrator“ nicht modifizieren oder löschen.
Administrator	Ein vorkonfiguriertes Berechtigungsklasse für die Verwaltung von Sophos Sicherheitssoftware im Netzwerk, jedoch nicht zur Verwaltung von Berechtigungsklassen in Enterprise Console. Sie können der Rolle „Administrator“ einen neuen Namen geben, die Rolle modifizieren oder löschen.
Helpdesk	Eine vorkonfigurierte Berechtigungsklasse, die nur über Korrekturrechte verfügt, z.B. zum Bereinigen oder Aktualisieren von Computern. Sie können die Rolle „Helpdesk“ umbenennen, modifizieren und löschen.

Rolle	Beschreibung
Gast	Eine vorkonfigurierte Berechtigungsklasse mit Lesezugriff auf Enterprise Console. Sie können die Rolle „Gast“ umbenennen, modifizieren und löschen.

Sie können die Rollen „Administrator“, „Helpdesk“ und „Gast“ an Ihre Bedürfnisse anpassen oder anhand der Anweisungen im Abschnitt [Erstellen einer Rolle](#) (Seite 15) eigene Rollen erstellen.

4.3 Erstellen einer Rolle

Bei rollenbasierter Verwaltung müssen Sie hierzu über die Berechtigung **Rollenbasierte Verwaltung** verfügen. Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

1. Klicken Sie im Menü **Extras** auf **Rollen und Teilverwaltungseinheiten verwalten**.
2. Rufen Sie im Dialogfeld **Rollen und Teilverwaltungseinheiten verwalten** die Registerkarte **Rollen verwalten** auf und klicken Sie auf **Erstellen**.

Das Dialogfeld **Rolle erstellen** wird angezeigt.

3. Geben Sie einen Namen für die Funktion in das Feld **Name** ein.
4. Wählen Sie im Fenster **Berechtigungen** die Berechtigung(en) aus, die der Funktion zugewiesen werden sollen und klicken Sie auf **Hinzufügen**.
5. Klicken Sie im Fenster **Benutzer und Gruppen** auf **Hinzufügen**.
6. Geben Sie in das Dialogfeld **Benutzer oder Gruppe auswählen** den Namen eines Windows-Benutzers oder einer -Gruppe ein, dem/der Sie eine Funktion zuweisen möchten. Klicken Sie auf **OK**.

Bei Bedarf können Sie der Rolle mehr Benutzer oder Gruppen zuweisen. Anweisungen hierzu finden Sie in Schritt 5 und 6.

4.4 Löschen einer Rolle

Bei rollenbasierter Verwaltung müssen Sie hierzu über die Berechtigung **Rollenbasierte Verwaltung** verfügen. Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

1. Klicken Sie im Menü **Extras** auf **Rollen und Teilverwaltungseinheiten verwalten**.
2. Wählen Sie im Dialogfeld **Rollen und Teilverwaltungseinheiten verwalten** auf der Registerkarte **Rollen verwalten** die zu löschende Funktion aus und klicken Sie auf **Löschen**.

Hinweis: Sie können die vordefinierte Funktion „Systemadministrator“ nicht löschen.

4.5 Ändern einer Rolle

Bei rollenbasierter Verwaltung müssen Sie hierzu über die Berechtigung **Rollenbasierte Verwaltung** verfügen. Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

1. Klicken Sie im Menü **Extras** auf **Rollen und Teilverwaltungseinheiten verwalten**.
2. Wählen Sie im Dialogfeld **Rollen und Teilverwaltungseinheiten verwalten** auf der Registerkarte **Rollen verwalten** die gewünschte Rolle aus und klicken Sie auf **Ändern**.
Das Dialogfeld **Rolle ändern** wird angezeigt.
3. Weisen Sie im Fenster **Berechtigungen** den Rollen Berechtigungen zu oder entfernen Sie vorhandene Berechtigungen.
4. Fügen Sie im Fenster **Benutzer und Gruppen** Windows-Benutzer und -Gruppen zu der Rolle hinzu oder löschen Sie vorhandene Benutzer oder Gruppen.

4.6 Zuweisen von Berechtigungen zu Rollen

Bei rollenbasierter Verwaltung müssen Sie hierzu über die Berechtigung **Rollenbasierte Verwaltung** verfügen. Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

1. Klicken Sie im Menü **Extras** auf **Rollen und Teilverwaltungseinheiten verwalten**.
2. Wählen Sie im Dialogfeld **Rollen und Teilverwaltungseinheiten verwalten** auf der Registerkarte **Rollen verwalten** die gewünschte Rolle aus und klicken Sie auf **Ändern**.
Das Dialogfeld **Rolle ändern** wird angezeigt.
3. Wählen Sie im Fenster **Berechtigungen** aus der **Berechtigungsliste** eine Berechtigung aus und klicken Sie auf **Hinzufügen**.

4.7 Erstellen einer Teilverwaltungseinheit

Bei rollenbasierter Verwaltung müssen Sie hierzu über die Berechtigung **Rollenbasierte Verwaltung** verfügen. Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

1. Klicken Sie im Menü **Extras** auf **Rollen und Teilverwaltungseinheiten verwalten**.
2. Rufen Sie im Dialogfeld **Rollen und Teilverwaltungseinheiten verwalten** die Registerkarte **Teilverwaltungseinheiten verwalten** auf und klicken Sie auf **Erstellen**.
Das Dialogfeld **Teilverwaltungseinheit erstellen** wird angezeigt.
3. Geben Sie einen Namen für die Teilverwaltungseinheit in das Feld **Name** ein.
4. Wählen Sie im Fenster **Enterprise Console-Gruppen** die Gruppen aus, die Sie in die Teilverwaltungseinheit aufnehmen möchten.
5. Klicken Sie im Fenster **Benutzer und Gruppen** auf **Hinzufügen**, um Windows-Benutzer und -Gruppen in die Teilverwaltungseinheit aufzunehmen.

4.8 Ändern der aktiven Teilverwaltungseinheit

Wenn Ihnen mehrere Teilverwaltungseinheiten zugewiesen wurden, können Sie festlegen, welche Teilverwaltungseinheiten beim Öffnen von Enterprise Console angezeigt werden und in Enterprise Console zu einer anderen Teilverwaltungseinheit wechseln.

Es kann jeweils nur eine Teilverwaltungseinheit angezeigt werden. Wenn Sie die aktive Teilverwaltungseinheit ändern, wird Enterprise Console mit der neuen Teilverwaltungseinheit neu geladen.

So können Sie die aktive Teilverwaltungseinheit ändern:

1. Klicken Sie im Menü **Extras** auf **Aktive Teilverwaltungseinheit auswählen**.
2. Wählen Sie im Dialogfeld **Aktive Teilverwaltungseinheit auswählen** die Teilverwaltungseinheit aus, die Sie öffnen möchten, und klicken Sie auf **OK**.

4.9 Ändern einer Teilverwaltungseinheit

Bei rollenbasierter Verwaltung müssen Sie hierzu über die Berechtigung **Rollenbasierte Verwaltung** verfügen. Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

1. Klicken Sie im Menü **Extras** auf **Rollen und Teilverwaltungseinheiten verwalten**.
2. Wählen Sie im Dialogfeld **Rollen und Teilverwaltungseinheiten verwalten** auf der Registerkarte **Teilverwaltungseinheiten verwalten** die zu ändernde Teilverwaltungseinheit aus und klicken Sie auf **Ändern**.
3. Im Dialogfeld **Teilverwaltungseinheit ändern** können Sie den Namen der Teilverwaltungseinheit, die Enterprise Console-Gruppen der Teilverwaltungseinheit und die Windows-Benutzer und -Gruppen ändern, die Zugriff auf die Teilverwaltungseinheit besitzen. Klicken Sie auf **OK**.

4.10 Kopieren einer Teilverwaltungseinheit

Bei rollenbasierter Verwaltung müssen Sie hierzu über die Berechtigung **Rollenbasierte Verwaltung** verfügen. Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

1. Klicken Sie im Menü **Extras** auf **Rollen und Teilverwaltungseinheiten verwalten**.
2. Wählen Sie im Dialogfeld **Rollen und Teilverwaltungseinheiten verwalten** auf der Registerkarte **Teilverwaltungseinheiten verwalten** die gewünschte Teilverwaltungseinheit aus und klicken Sie auf **Kopieren**.

In der Liste der Teilverwaltungseinheiten erscheint nun eine Kopie der Teilverwaltungseinheit.

3. Wählen Sie die neue Teilverwaltungseinheit aus und klicken Sie auf **Ändern**. Benennen Sie die Teilverwaltungseinheit um. Auf Wunsch können Sie die Gruppen der Teilverwaltungseinheit sowie die Windows-Benutzer und -Gruppen ändern, die darauf zugreifen können.

4.11 Löschen einer Teilverwaltungseinheit

Bei rollenbasierter Verwaltung müssen Sie hierzu über die Berechtigung **Rollenbasierte Verwaltung** verfügen. Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

1. Klicken Sie im Menü **Extras** auf **Rollen und Teilverwaltungseinheiten verwalten**.
2. Wählen Sie im Dialogfeld **Rollen und Teilverwaltungseinheiten verwalten** auf der Registerkarte **Teilverwaltungseinheiten verwalten** die zu löschende Teilverwaltungseinheit aus und klicken Sie auf **Löschen**.

Die Teilverwaltungseinheit **Default** kann nicht gelöscht werden.

4.12 Anzeigen von Rollen und Teilverwaltungseinheiten von Benutzern und Gruppen

So können Sie die Rollen und Teilverwaltungseinheiten von Windows-Benutzern und -Gruppen aufrufen:

1. Klicken Sie im Menü **Extras** auf **Rollen und Teilverwaltungseinheiten verwalten**.
2. Rufen Sie im Dialogfeld **Rollen und Teilverwaltungseinheiten verwalten** die Registerkarte **Benutzer-/Gruppenansicht** auf und klicken Sie auf die Schaltfläche **Benutzer/Gruppe auswählen**.
3. Wählen Sie im Dialogfeld **Benutzer/Gruppe auswählen** einen Benutzer oder eine Gruppe aus, dessen/deren Rollen und Teilverwaltungseinheiten angezeigt werden sollen und klicken Sie auf **OK**.

4.13 Aufgabenbereich der Berechtigungen

Berechtigung	Aufgaben
Computersuche, -schutz und -gruppen	Suche starten, Suche anhalten und Suche nach Domänen (Netzwerksuche, IP-Bereichsuche und Active Directory-Suche)
	Importieren von Computern und Gruppen aus Active Directory, Importieren von Gruppen aus Active Directory
	Importieren von Computern aus einer Datei
	Löschen eines Computers
	Schützen eines Computers
	Synchronisierung von Gruppen mit Active Directory
	Ändern der Synchronisierungseigenschaften von Gruppen
	Gruppensynchronisierung entfernen

Berechtigung	Aufgaben
	Verschieben eines Computers Erstellen einer Gruppe Umbenennen einer Gruppe Verschieben einer Gruppe Löschen einer Gruppe Übertragen einer Richtlinie auf eine Gruppe
Anpassung von Data Control	Erstellen einer Data Control-Regel Ändern einer Data Control-Regel Kopieren einer Data Control-Regel Löschen einer Data Control-Regel Ausschließen von Dateien von Data Control-Scans Erstellen einer Content Control List Ändern einer Content Control List Kopieren einer Content Control List Löschen einer Content Control List
Richtlinieneinstellung – Antivirus und HIPS	Erstellen einer Antivirus- und HIPS-Richtlinie Duplizieren einer Antivirus- und HIPS-Richtlinie Umbenennen einer Antivirus- und HIPS-Richtlinie Ändern einer Antivirus- und HIPS-Richtlinie Wiederherstellen der Standardeinstellungen von Antivirus und HIPS Löschen einer Antivirus- und HIPS-Richtlinie Hinzufügen oder Entfernen von Einträgen aus einer Threat-Masterliste
Richtlinieneinstellung – Application Control	Erstellen einer Application Control-Richtlinie Duplizieren einer Application Control-Richtlinie Umbenennen einer Application Control-Richtlinie Ändern einer Application Control-Richtlinie

Berechtigung	Aufgaben
	Wiederherstellung der Standardeinstellungen von Application Control
	Löschen einer Application Control-Richtlinie
Richtlinieneinstellung – Data Control	Erstellen einer Data Control-Richtlinie
	Duplizieren einer Data Control-Richtlinie
	Umbenennen einer Data Control-Richtlinie
	Ändern einer Data Control-Richtlinie
	Wiederherstellen der Data Control-Einstellungen
	Löschen einer Data Control-Richtlinie
Richtlinieneinstellung – Device Control	Erstellen einer Device Control-Richtlinie
	Duplizieren einer Device Control-Richtlinie
	Umbenennen einer Device Control-Richtlinie
	Ändern einer Device Control-Richtlinie
	Wiederherstellen der Standardeinstellungen von Device Control
	Löschen einer Device Control-Richtlinie
Richtlinieneinstellung – Firewall	Erstellen einer Firewall-Richtlinie
	Duplizieren einer Firewall-Richtlinie
	Umbenennen einer Firewall-Richtlinie
	Ändern einer Firewall-Richtlinie
	Wiederherstellen der Standardeinstellungen der Firewall
	Löschen einer Firewall-Richtlinie
Richtlinieneinstellung – NAC	Anzeige einer NAC-Richtlinie
Richtlinieneinstellung – Manipulationsschutz	Erstellen einer Manipulationsschutz-Richtlinie
	Duplizieren einer Manipulationsschutz-Richtlinie
	Umbenennen einer Manipulationsschutz-Richtlinie
	Bearbeiten einer Manipulationsschutz-Richtlinie
	Wiederherstellen der Standardeinstellungen des Manipulationsschutzes

Berechtigung	Aufgaben
	Löschen einer Manipulationsschutz-Richtlinie
Richtlinieneinstellung – Updates	Erstellen einer Update-Richtlinie
	Duplizieren einer Update-Richtlinie
	Umbenennen einer Update-Richtlinie
	Ändern einer Update-Richtlinie
	Wiederherstellen der Standard-Update-Einstellungen
	Löschen einer Update-Richtlinie
	Erstellen von Abonnements
	Ändern von Abonnements
	Umbenennen von Abonnements
	Duplizieren von Abonnements
	Löschen von Abonnements
	Konfigurieren von Update Managern
	Korrektur – Bereinigung
Alerts löschen	
Fehler löschen	
Korrektur – Updates und Scans	Computer jetzt updaten
	Durchführen einer vollständigen Systemüberprüfung
	Durchsetzen von Gruppenrichtlinien
Report-Konfiguration	Erstellen, Bearbeiten und Löschen eines Reports
Rollenbasierte Verwaltung	Erstellen einer Rolle
	Umbenennen einer Rolle
	Löschen einer Rolle
	Ändern der Berechtigungen einer Rolle
	Hinzufügen von Benutzern/Gruppen zur Rolle
	Entfernen eines Benutzers/einer Gruppe von einer Funktion
	Verwaltung von Teilverwaltungseinheiten: Erstellen einer Teilverwaltungseinheit; Umbenennen einer Teilverwaltungseinheit; Löschen einer Teilverwaltungseinheit;

Berechtigung	Aufgaben
	Hinzufügen einer Teilverwaltungseinheit; Entfernen einer Stammgruppe einer Teilverwaltungseinheit, Hinzufügen von Benutzern/Gruppen zu einer Teilverwaltungseinheit, Entfernen von Benutzern/Gruppen von einer Teilverwaltungseinheit
Systemkonfiguration	Ändern der SMTP-Servereinstellungen; Testen der SMTP-Servereinstellungen; Hinzufügen von Empfängern von E-Mail-Benachrichtigungen
	Konfigurieren von Höchstwerten für das Dashboard
	Konfigurieren von Reports: Konfigurieren der Datenbank-Alert-Bereinigung; Einstellen des in Reports angezeigten Firmennamens
	Konfigurieren der Benachrichtigungen an Sophos: Aktivieren/Deaktivieren der Benachrichtigungen an Sophos; Ändern des Benutzernamens; Ändern der Kontakt-E-Mail-Adresse
	Konfigurieren der NAC-URL

5 Erstellen und Einsatz von Gruppen

5.1 Wofür gibt es Gruppen?

Sie müssen Gruppen erstellen und ihnen Computer zuordnen, bevor Sie diese Computer schützen und verwalten können.

Gruppen bieten die folgenden Vorteile:

- Updaten von Computern in unterschiedlichen Gruppen von verschiedenen Quellen oder über verschiedene Zeitpläne.
- Einsatz unterschiedlicher Antivirus- und HIPS-, Application Control-, Firewall- oder sonstiger Richtlinien für die einzelnen Gruppen.
- Einfachere Computerverwaltung.

Tipp: Erstellen von Gruppen in Gruppen und Übertragen von Richtlinien auf alle Gruppen und Untergruppen.

5.2 Erstellen einer Gruppe

Bei rollenbasierter Verwaltung ist hierzu die Berechtigung **Computersuche, -schutz und -gruppen** erforderlich. Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

So können Sie eine neue Gruppe für Computer erstellen:

1. Wählen Sie in der Ansicht **Endpoints** im Fensterbereich **Gruppen** (links in der Konsole), wo Sie die Gruppe erstellen möchten.
Klicken Sie auf den Computernamen oben, wenn Sie eine neue Top-Level-Gruppe erstellen möchten. Klicken Sie auf eine bestehende Gruppe, wenn Sie eine Untergruppe erstellen möchten.
2. Klicken Sie in der Symbolleiste auf das Symbol **Gruppe erstellen**.
Eine „Neue Gruppe“ wird in die Liste aufgenommen. Der Name der Gruppe ist markiert.
3. Geben Sie einen Namen für die Gruppe ein.

Update-, Anti-Virus- und HIPS-, Application Control-, Firewall-, NAC- (Network Access Control), Data Control- und Device Control-Richtlinien werden automatisch auf die neue Gruppe übertragen. Sie können diese Richtlinien ändern oder andere Richtlinien anwenden. Nähere Informationen [Ändern einer Richtlinie](#) (Seite 30) und [Übertragen einer Richtlinie auf eine Gruppe](#) (Seite 29).

Hinweis: Wenn es sich bei der neuen Gruppe um eine Untergruppe handelt, verwendet die Untergruppe anfangs dieselben Einstellungen wie die Gruppe, in der sie sich befindet.

5.3 Zuweisen von Computern zu einer Gruppe

Bei rollenbasierter Verwaltung ist hierzu die Berechtigung **Computersuche, -schutz und -gruppen** erforderlich. Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

1. Markieren Sie die Computer, die Sie in eine Gruppe aufnehmen möchten. Klicken Sie z.B. auf die Gruppe **Nicht zugewiesen** und markieren Sie dort Computer.
2. Ziehen Sie die Computer mittels Drag-and-Drop in die neue Gruppe.

Wenn Sie ungeschützte Computer aus der Gruppe **Nicht zugewiesen** in eine Gruppe verschieben, für die automatische Updates eingerichtet sind, wird ein Assistent gestartet, der Ihnen dabei hilft, diese Computer zu schützen.

Wenn Sie Computer von einer Gruppe in eine andere verschieben, verwenden Sie die gleichen Richtlinien wie die Computer, die sich bereits in der Gruppe befinden, in die sie verschoben wurden.

5.4 Löschen von Computern aus einer Gruppe

Bei rollenbasierter Verwaltung ist hierzu die Berechtigung **Computersuche, -schutz und -gruppen** erforderlich. Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Sie können Computer aus einer Gruppe löschen, z.B. wenn Sie Einträge für Computer entfernen möchten, die sich nicht mehr im Netzwerk befinden.

Wichtig: Wenn Sie Computer löschen, die sich noch im Netzwerk befinden, werden sie nicht mehr in der Konsole aufgelistet oder von ihr verwaltet.

So löschen Sie Computer:

1. Markieren Sie die Computer, die Sie löschen möchten.
2. Rechtsklicken Sie auf die Auswahl und wählen Sie **Löschen**.

Wenn Sie die Computer erneut sehen möchten, klicken Sie in der Symbolleiste auf das Symbol **Computersuche**. Die Computer werden bis zum nächsten Neustart nicht als verwaltet angezeigt.

5.5 Verschieben einer Gruppe

Bei rollenbasierter Verwaltung ist hierzu die Berechtigung **Computersuche, -schutz und -gruppen** erforderlich. Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

1. Markieren Sie die Gruppe, die Sie verschieben möchten. Klicken Sie im Menü **Bearbeiten** auf **Ausschneiden**.
2. Markieren Sie die Gruppe, in die Sie die Gruppe einfügen möchten. Klicken Sie im Menü **Bearbeiten** auf **Einfügen**.

5.6 Löschen einer Gruppe

Bei rollenbasierter Verwaltung ist hierzu die Berechtigung **Computersuche, -schutz und -gruppen** erforderlich. Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Alle Computer, die sich in der gelöschten Gruppe befanden, werden in der Gruppe **Nicht zugewiesen** abgelegt.

1. Markieren Sie die Gruppe, die Sie löschen möchten.
2. Rechtsklicken Sie auf die Auswahl und wählen Sie **Löschen**. Bestätigen Sie bei entsprechender Aufforderung, dass Sie die Gruppe und gegebenenfalls deren Untergruppen löschen möchten.

5.7 Umbenennen einer Gruppe

Bei rollenbasierter Verwaltung ist hierzu die Berechtigung **Computersuche, -schutz und -gruppen** erforderlich. Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

1. Markieren Sie die Gruppe, die Sie umbenennen möchten.
2. Rechtsklicken Sie auf die Auswahl und wählen Sie **Umbenennen**.

5.8 Übertragen einer Richtlinie auf eine Gruppe

Bei rollenbasierter Verwaltung ist hierzu die Berechtigung **Computersuche, -schutz und -gruppen** erforderlich. Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

1. Markieren Sie im Fensterbereich **Richtlinien** die Richtlinie.
2. Klicken Sie auf die Richtlinie und ziehen Sie sie auf die Gruppe, auf die sie übertragen werden soll. Bestätigen Sie bei entsprechender Aufforderung, dass Sie den Vorgang fortsetzen möchten.

Hinweis: Sie können auch auf eine Gruppe rechtsklicken und die Option **Gruppenrichtliniendetails öffnen** wählen. Anschließend können Sie Richtlinien für die Gruppe aus den Dropdown-Menüs auswählen.

5.9 Welche Richtlinien sind einer Gruppe zugewiesen?

So können Sie feststellen, welche Richtlinien einer Gruppe zugewiesen wurden:

- Rechtsklicken Sie im Fensterbereich **Gruppen** auf die Gruppe. Wählen Sie **Gruppenrichtliniendetails öffnen**.

Im Dialogfeld „Gruppendetails“ können Sie die Richtlinien ansehen, die derzeit verwendet werden.

6 Erstellen und Einsatz von Richtlinien

6.1 Wofür gibt es Richtlinien?

In einer Richtlinie werden Einstellungen zusammengefasst, die für alle Computer in einer Gruppe gelten.

- Die **Update**-Richtlinie gibt an, wie Computer mit neuer Sicherheitssoftware upgedatet werden.

Hinweis: Wenn Sie ein Upgrade von Enterprise Console 3.x durchgeführt haben, Ihre Update-Einstellungen jedoch noch nicht migriert haben, finden Sie neben der **Update-Richtlinie alte Update-Richtlinien**. Weitere Informationen finden Sie im Abschnitt „Alte Updates“.

- In der **Anti-Virus- und HIPS**-Richtlinie ist festgelegt, wie die Sicherheitssoftware Computer auf Viren, Trojaner, Würmer, Spyware, Adware, potenziell unerwünschte Anwendungen, verdächtige Dateien und Verhaltensmuster scannt und sie davon bereinigt.
- In der **Application Control**-Richtlinie ist festgelegt, welche Anwendungen auf Ihren Computern gesperrt und welche zugelassen sind.
- Die **Firewall**-Richtlinie gibt an, wie die Firewall Computer schützt.
- Die **Data Control**-Richtlinie umfasst Regeln zum Überwachen bzw. Beschränken von Dateiübertragungen auf der Basis des Inhalts, Namens und Typs von Dateien.
- In der **Device Control**-Richtlinie werden die Speichermedien und Netzwerkgeräte festgelegt, die nicht auf Arbeitsplatzrechnern verwendet werden dürfen.
- Die **NAC**-Richtlinie enthält die von Computern zu erfüllenden Bedingungen für den Netzwerkzugriff.
- Die **Manipulationsschutz**-Richtlinie umfasst das Kennwort, über das autorisierte Endpoint-Benutzer Sophos Sicherheitssoftware konfigurieren, deaktivieren oder deinstallieren können.

Sie können mehr als eine Richtlinie von jedem Typ erstellen.

Sie können die gleiche Richtlinie auf mehr als eine Gruppe übertragen.

6.2 Standardrichtlinien

Bei der Installation von Enterprise Console werden Standard-Richtlinien erstellt.

Update-Richtlinie

Die Standard-Update-Richtlinie bietet Folgendes:

- Fünfminütliche Updates der Computer vom Standardverzeichnis. Das Standardverzeichnis lautet: UNC-Freigabe \\<Computername>\SophosUpdate. Dabei ist „Computername“ der Name des Computers, auf dem der Update Manager installiert ist.

Hinweis: Wenn Sie ein Upgrade von Enterprise Console 3.x durchgeführt haben, Ihre Update-Einstellungen jedoch noch nicht migriert haben, finden Sie neben der **Update-Richtlinie alte Update-Richtlinien**. Weitere Informationen finden Sie im Abschnitt „Alte Updates“.

Antivirus- und HIPS-Richtlinie

Die Standard-Antivirus- und HIPS-Richtlinie bietet Folgendes:

- On-Access-Scans auf Viren und Spyware (jedoch nicht verdächtige Dateien und Adware oder andere potenziell unerwünschte Anwendungen).
- Analyse der auf dem System laufenden Programme (Sophos Anti-Virus und Sophos Endpoint Security and Control für Windows 2000 und höher).
- Sicherheits-Alerts, die auf dem Desktop des betroffenen Computers angezeigt und zum Ereignisprotokoll hinzugefügt werden.

Application Control-Richtlinie

Standardmäßig werden alle Anwendungen und Anwendungstypen zugelassen. On-Access-Scans auf Anwendungen, die Sie eventuell überwachen möchten, ist nicht aktiviert.

Firewall-Richtlinie

Standardmäßig ist die Sophos Client Firewall aktiviert und sperrt unnötigen Datenfluss. Konfigurieren Sie die zunächst Firewall so, dass gewünschte Anwendungen zugelassen werden, bevor Sie sie im gesamten Netzwerk einsetzen. Mehr zu diesem Thema erfahren Sie unter *Einrichten der Firewall* (Seite 120).

Eine vollständige Beschreibung der Firewall-Einstellungen ist dem Sophos Support-Artikel 57757 (<http://www.sophos.de/support/knowledgebase/article/57757.html>) zu entnehmen.

Data Control-Richtlinie

Standardmäßig ist Data Control deaktiviert und es sind keine Regeln zur Überwachung oder Einschränkung der Übertragung von Dateien auf das Internet oder auf Speichermedien festgelegt.

Device Control-Richtlinie

Device Control ist standardmäßig deaktiviert und alle Geräte sind zugelassen.

NAC-Richtlinie

Wenn Sie die Standardrichtlinie oder den Richtlinien-Modus im NAC-Server nicht geändert haben, besitzen alle Computer über Netzwerkzugriffsrechte.

Manipulationsschutz-Richtlinie

Standardmäßig ist der Manipulationsschutz deaktiviert und für die Konfiguration, Deaktivierung oder Deinstallation von Sophos Sicherheitssoftware ist kein Kennwort festgelegt.

6.3 Muss ich meine eigenen Richtlinien erstellen?

Bei der Installation von Enterprise Console werden Standard-Richtlinien erstellt. Diese Richtlinien werden auf neu erstellte Gruppen übertragen.

Die Standardrichtlinien bieten Ihnen grundlegenden Schutz. Wenn Sie jedoch Funktionen wie Network Access Control oder Application Control nutzen möchten, müssen Sie neue Richtlinien erstellen oder zumindest die Standardrichtlinien ändern.

Hinweis: Wenn Sie die Standardrichtlinie ändern, wirken sich die Änderungen auf alle neu erstellten Richtlinien aus.

Hinweis: Bei rollenbasierter Verwaltung müssen Sie zum Konfigurieren einer NAC-Richtlinie über die Berechtigung **Richtlinieneinstellung** verfügen. Wenn Sie beispielsweise eine Antivirus- und HIPS-Richtlinie erstellen oder ändern möchten, benötigen Sie die Berechtigung **Richtlinieneinstellung – Anti-Virus und HIPS**. Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Update-Richtlinie

In der Standardrichtlinie ist festgelegt, dass Computer alle fünf Minuten über das Standardverzeichnis Updates beziehen. Das Standardverzeichnis lautet: UNC-Freigabe \\<Computername>\SophosUpdate. Dabei ist „Computername“ der Name des Computers, auf dem der Update Manager installiert ist. Sie können eine andere Freigabe angeben, die über das benötigte Software-Abonnement verfügt. Mehr dazu erfahren Sie im Abschnitt „Konfigurieren der Update-Richtlinie“.

Antivirus und HIPS

Die Antivirus- und HIPS-Standardrichtlinie schützt Computer vor Viren und sonstiger Malware. Wenn auch unerwünschte Anwendungen oder Verhaltensmuster erkannt werden sollen, können Sie entweder die Standardrichtlinie ändern oder eine neue Richtlinie erstellen. Mehr zu diesem Thema erfahren Sie unter [Die Antivirus- und HIPS-Richtlinie](#) (Seite 83).

Application Control

Konfigurieren Sie zum Festlegen und Sperren nicht zulässiger Anwendungen **Application Control**-Richtlinien. Anweisungen hierzu finden Sie unter [Application Control](#) (Seite 130).

Firewall-Richtlinie

Konfigurieren Sie **Firewall**-Richtlinien, um vertrauenswürdigen Anwendungen Netzwerkzugang zu gewähren. Anweisungen hierzu finden Sie unter [Einrichten der Firewall](#) (Seite 120).

Data Control

Data Control ist standardmäßig deaktiviert. Konfigurieren Sie zum Schutz vor ungewollten Datenverlusten **Data Control**-Richtlinien, um ungewollte Datenverluste zu verhindern. Anweisungen hierzu finden Sie unter [Data Control](#) (Seite 133).

Device Control

Device Control ist standardmäßig deaktiviert. Konfigurieren Sie zur Beschränkung zulässiger Hardware-Geräte **Device Control**-Richtlinien. Anweisungen hierzu finden Sie unter [Device Control](#) (Seite 149).

NAC

Network Access Control ist standardmäßig deaktiviert. Konfigurieren Sie NAC-Richtlinien, um den Computerzugriff bestimmten Bedingungen zu unterwerfen. Anweisungen hierzu finden Sie unter [Ändern einer NAC-Richtlinie](#) (Seite 159).

Manipulationsschutz

Der Manipulationsschutz ist standardmäßig deaktiviert. Konfigurieren Sie zum Aktivieren des Manipulationsschutzes **Manipulationsschutz-Richtlinien**. Anweisungen hierzu finden Sie unter [Allgemeine Informationen](#) (Seite 160).

6.4 Erstellen einer Richtlinie

Bei rollenbasierter Verwaltung müssen Sie hierzu über die Berechtigung **Richtlinieneinstellung** verfügen. Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

So können Sie eine Richtlinie erstellen:

Hinweis: Sie können keine NAC-Richtlinien erstellen. NAC-Richtlinien können nur bearbeitet werden. Mehr dazu erfahren Sie unter [Ändern einer NAC-Richtlinie](#) (Seite 159).

1. Rechtsklicken Sie in der Ansicht **Endpoints** im Fensterbereich **Richtlinien** auf den Richtlinientyp, den Sie erstellen möchten (z.B. „Update-Richtlinie“), und wählen Sie **Richtlinie erstellen**.

Eine „Neue Richtlinie“, deren Name markiert ist, wird zur Liste hinzugefügt.

2. Geben Sie der Richtlinie einen neuen Namen.
3. Doppelklicken Sie auf die neue Richtlinie. Geben Sie die gewünschten Einstellungen ein.
Anweisungen zur Auswahl der Einstellungen finden Sie im Abschnitt zum Konfigurieren der entsprechenden Richtlinie.

Sie haben eine Richtlinie erstellt, die nun auf Gruppen übertragen werden kann.

6.5 Übertragen einer Richtlinie auf eine Gruppe

Bei rollenbasierter Verwaltung ist hierzu die Berechtigung **Computersuche, -schutz und -gruppen** erforderlich. Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

1. Markieren Sie im Fensterbereich **Richtlinien** die Richtlinie.
2. Klicken Sie auf die Richtlinie und ziehen Sie sie auf die Gruppe, auf die Sie die Richtlinie übertragen möchten. Bestätigen Sie bei entsprechender Aufforderung, dass Sie den Vorgang fortsetzen möchten.

Hinweis: Sie können auch auf eine Gruppe rechtsklicken und die Option **Gruppenrichtliniendetails öffnen** wählen. Anschließend können Sie Richtlinien für die Gruppe aus den Dropdown-Menüs auswählen.

6.6 Ändern einer Richtlinie

Bei rollenbasierter Verwaltung:

- Hierzu müssen Sie zum Ändern der entsprechenden **Richtlinieneinstellung** berechtigt sein.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

So ändern Sie eine Richtlinie für eine Gruppe oder Gruppen von Computern:

1. Doppelklicken Sie im Fensterbereich **Richtlinien** auf die Richtlinie, die Sie bearbeiten möchten.
2. Bearbeiten Sie die Einstellungen.

Anweisungen zum Konfigurieren unterschiedlicher Richtlinien finden Sie in den entsprechenden Abschnitten.

6.7 Umbenennen einer Richtlinie

Bei rollenbasierter Verwaltung:

- Hierzu müssen Sie zum Ändern der entsprechenden **Richtlinieneinstellung** berechtigt sein.
- Sie können keine Richtlinien umbenennen, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Hinweis: Die „Standardrichtlinie“ kann nicht umbenannt werden.

So können Sie eine Richtlinie umbenennen:

1. Wählen Sie im Fensterbereich **Richtlinien** die Richtlinie, die Sie umbenennen möchten.
2. Rechtsklicken Sie darauf und wählen Sie **Richtlinie umbenennen**.

6.8 Löschen einer Richtlinie

Bei rollenbasierter Verwaltung:

- Hierzu müssen Sie zum Ändern der entsprechenden **Richtlinieneinstellung** berechtigt sein.
- Sie können keine Richtlinien löschen, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Hinweis: Sie können keine „Standard“-Richtlinie löschen.

So können Sie eine Richtlinie löschen:

1. Rechtsklicken Sie im Fensterbereich **Richtlinien** auf die Richtlinie, die Sie löschen möchten, und wählen Sie **Richtlinie löschen**.
2. Alle Gruppen, die die gelöschte Richtlinie verwenden, werden auf die Standardrichtlinie zurückgestellt.

6.9 Anzeige der Gruppen einer Richtlinie

Verfahren Sie wie folgt, um festzustellen, auf welche Gruppen eine bestimmte Richtlinie übertragen wurde:

- Rechtsklicken Sie im Fensterbereich **Richtlinie** auf die Richtlinie und wählen Sie **Gruppen anzeigen, denen diese Richtlinie zugeordnet wurde**

Eine Liste der Gruppen wird angezeigt, die diese Richtlinie verwenden.

6.10 Prüfen, ob Computer die Gruppenrichtlinie verwenden

Sie können prüfen, ob alle Computer in einer Gruppe mit der entsprechenden Gruppenrichtlinie konform sind.

1. Markieren Sie die Gruppe, die Sie prüfen möchten.
2. Wechseln Sie in der Computerliste in die Ansicht **Endpoints** und betrachten Sie auf der Registerkarte **Status** die Spalte **Richtlinienkonformität**.
 - Wenn „Wie Richtlinie“ angezeigt wird, ist der Computer mit den Richtlinien der Gruppe konform.
 - Wenn ein gelbes Warnsymbol und der Text „Weicht von Richtlinie ab“ angezeigt werden, verwendet der Computer eine andere Richtlinie als die übrigen Computer in der Gruppe.

Nähere Informationen zum Status der Sicherheitsfunktionen des Computers und der ihm zugewiesenen Richtlinien finden Sie im entsprechenden Abschnitt in der Ansicht **Endpoints** (z.B. Registerkarte **Antivirus-Details**).

Wenn Computer mit den Gruppenrichtlinien konform sein sollen, verfahren Sie anhand der Anweisungen im Abschnitt [Durchsetzen von Gruppenrichtlinien](#) (Seite 31).

6.11 Durchsetzen von Gruppenrichtlinien

Bei rollenbasierter Verwaltung müssen Sie hierzu über die Berechtigung **Korrektur – Updates und Scans** verfügen. Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Wenn Computer gefunden werden, die nicht mit den Richtlinien Ihrer Gruppe konform sind, können Sie Gruppenrichtlinien für diese Computer übernehmen.

1. Markieren Sie die Computer, die von der Gruppenrichtlinie abweichen.
2. Rechtsklicken Sie auf die Auswahl und wählen Sie **Konformität mit**. Wählen Sie dann den passenden Richtlinientyp aus, z.B. **Antivirus- und HIPS-Gruppenrichtlinie**.

7 Computersuche im Netzwerk

7.1 Auffinden von Computern

Sie können die Funktion „Computersuche“ verwenden und eine von mehreren Optionen wählen, mit denen Sie Computer im Netzwerk suchen und zur Enterprise Console hinzufügen können. Folgende Optionen stehen zur Auswahl:

- [Importieren von Containern und Computern aus Active Directory](#) (Seite 32)
- [Suchen nach Computern mit Active Directory](#) (Seite 33)
- [Computersuche im Netzwerk](#) (Seite 33)
- [Suchen nach Computern in einem IP-Bereich](#) (Seite 34)
- [Importieren von Computern aus einer Datei](#) (Seite 34)

Bei rollenbasierter Verwaltung ist die Berechtigung **Computersuche, -schutz und -gruppen** erforderlich, um Computer zur Konsole hinzuzufügen. Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

7.2 Importieren von Containern und Computern aus Active Directory

Bei rollenbasierter Verwaltung ist hierzu die Berechtigung **Computersuche, -schutz und -gruppen** erforderlich. Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Beim Importieren von Gruppen aus Active Directory wird die Active Directory-Containerstruktur abgerufen und in Enterprise Console als Computergruppenstruktur übernommen. Sie können entweder nur die Gruppenstruktur oder Gruppen und Computer importieren. Bei letzterer Option werden in Active Directory gefundene Computer in ihrer jeweiligen Gruppe statt in der Gruppe **Nicht zugewiesen** gespeichert.

Sie können Gruppen selbst erstellen und verwalten oder aus Active Directory importieren. Sie können die importierten Gruppen auch mit Active Directory synchronisieren.

So werden Gruppen aus Active Directory importiert:

1. Klicken Sie in der Symbolleiste auf das Symbol zur **Computersuche**.
2. Wählen Sie im Dialogfeld **Computersuche** unter **Import aus Active Directory** die Option **Import** aus und klicken Sie auf **OK**.

Sie können auch auf eine Gruppe rechtsklicken und Active Directory-Container über die Option **Import aus Active Directory** importieren.

Der **Assistent zum Import aus Active Directory** wird gestartet.

3. Befolgen Sie die Anweisungen des Assistenten. Geben Sie bei entsprechender Aufforderung an, ob **Computer und Gruppen** oder **Nur Gruppen** importiert werden sollen.

Nach dem Import von Containern aus Active Directory können Sie Richtlinien auf die Gruppen übertragen. Lesen Sie dazu den Abschnitt „Erstellen und Einsatz von Richtlinien“.

Nach dem Zuweisen der Richtlinien können Sie die Gruppen bei Bedarf mit Active Directory synchronisieren. Anweisungen hierzu finden Sie unter [Synchronisierung mit Active Directory](#) (Seite 38).

7.3 Suchen nach Computern mit Active Directory

Bei rollenbasierter Verwaltung ist hierzu die Berechtigung **Computersuche, -schutz und -gruppen** erforderlich. Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Mit Active Directory können Sie Netzwerkcomputer suchen und in der Gruppe **Nicht zugewiesen** auflisten lassen.

1. Klicken Sie in der Symbolleiste auf das Symbol zur **Computersuche**.
2. Wählen Sie im Dialogfeld **Computersuche** die Option **Active Directory** und klicken Sie auf **OK**.
3. Nun müssen Sie einen Benutzernamen und ein Kennwort eingeben. Dies ist notwendig, wenn eine Anmeldung auf Ihren Computern erforderlich ist (z.B. Windows XP Service Pack 2).

Bei dem Benutzerkonto muss es sich um ein Domänen-Administratorkonto oder ein Konto mit Vollzugriff auf die XP-Zielcomputer handeln.

Wenn Sie ein Domäne-Konto verwenden, *müssen* Sie den Benutzernamen in der Form Domäne\Benutzer eingeben.

4. Wählen Sie im Dialogfeld **Computersuche** die Domänen, die Sie durchsuchen möchten. Klicken Sie auf **OK**.
5. Klicken Sie auf die Gruppe **Nicht zugewiesen**, um die aufgefundenen Computer anzuzeigen.

Um die Computer zu verwalten, ziehen Sie sie in eine Gruppe.

7.4 Computersuche im Netzwerk

Bei rollenbasierter Verwaltung ist hierzu die Berechtigung **Computersuche, -schutz und -gruppen** erforderlich. Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

So können Sie eine Liste von Computern, die in Windows-Domänen und Arbeitsgruppen gefunden wurden, in die Gruppe **Nicht zugewiesen** aufnehmen:

1. Klicken Sie in der Symbolleiste auf das Symbol **Neue Computer suchen**.
2. Wählen Sie im Dialogfeld **Computersuche** die Option **Im Netzwerk suchen** und klicken Sie auf **OK**.

3. Geben Sie in das Dialogfeld **Zugangsdaten** den Benutzernamen und das Kennwort eines Benutzerkontos mit den erforderlichen Rechten zum Abrufen der Computerinformationen ein.

Bei dem Benutzerkonto muss es sich um ein Domänen-Administratorkonto oder ein Konto mit Vollzugriff auf die Zielcomputer handeln. Wenn Sie sich über ein Domänen-Konto anmelden müssen Sie den Benutzernamen in folgender Form eingeben: Domäne/Benutzer. Sie können diesen Schritt überspringen, wenn auf den Zielcomputern keine Anmeldung erforderlich ist.

4. Wählen Sie im Dialogfeld **Computersuche** die Domänen oder Arbeitsgruppen aus, die Sie suchen möchten. Klicken Sie auf **OK**.
5. Klicken Sie auf die Gruppe **Nicht zugewiesen**, um die aufgefundenen Computer anzuzeigen.

Um die Computer zu verwalten, ziehen Sie sie in eine Gruppe.

7.5 Suchen nach Computern in einem IP-Bereich

Bei rollenbasierter Verwaltung ist hierzu die Berechtigung **Computersuche, -schutz und -gruppen** erforderlich. Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Sie können Netzwerkcomputer über einen IP-Adressen-Bereich suchen und in der Gruppe **Nicht zugewiesen** auflisten lassen.

Hinweis: Sie können keine IPv6-Adressen verwenden.

1. Klicken Sie in der Symbolleiste auf das Symbol zur **Computersuche**.
2. Wählen Sie im Dialogfeld **Computersuche** die Option **IP-Bereich** und klicken Sie auf **OK**.
3. Geben Sie Ihren Benutzernamen und Ihr Kennwort ins Dialogfeld **Zugangsdaten** ein. Dies ist notwendig, wenn eine Anmeldung auf Ihren Computern erforderlich ist (z.B. Windows XP Service Pack 2).

Bei dem Benutzerkonto muss es sich um ein Domänen-Administratorkonto oder ein Konto mit Vollzugriff auf die XP-Zielcomputer handeln.

Wenn Sie ein Domäne-Konto verwenden, *müssen* Sie den Benutzernamen in der Form Domäne\Benutzer eingeben.

In das Feld **SNMP** können Sie den Namen der SNMP-Community eingeben.

4. Geben Sie im Dialogfeld **Computersuche** den **Beginn des IP-Bereichs** und das **Ende des IP-Bereichs** ein. Klicken Sie auf **OK**.
5. Klicken Sie auf die Gruppe **Nicht zugewiesen**, um die aufgefundenen Computer anzuzeigen.

Um die Computer zu verwalten, ziehen Sie sie in eine Gruppe.

7.6 Importieren von Computern aus einer Datei

Bei rollenbasierter Verwaltung ist hierzu die Berechtigung **Computersuche, -schutz und -gruppen** erforderlich. Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Damit Enterprise Console Ihre Computer auflistet, können Sie die Computernamen aus einer Datei importieren.

Die Datei mit den Computernamen muss eines der folgenden Kriterien erfüllen:

- eine Datei, die folgenden Konventionen entspricht.
- eine aus SAVAdmin exportierte SGR-Datei

Sie können eine Datei erstellen, die Einträge wie folgt verwendet:

```
[GroupName1 ]  
Domain1 | Windows2000 | ComputerName1  
Domain1 | Windows2000Server | ComputerName2
```

Hinweis: Sie müssen die Gruppe, in die die Computer aufgenommen werden sollen, nicht angeben. Bei Eingabe von [] (ohne Leerzeichen zwischen den Klammern) als Gruppenname werden Computer in die Gruppe **Nicht zugewiesen** gestellt.

Hinweis: Die folgenden Betriebssystemsnamen sind möglich: Windows95, Windows98, Windows9x, WindowsMe, WindowsNT, WindowsNTServer, Windows2000, Windows2000Server, WindowsXP, Windows2003, WindowsVista, Windows7, WindowsServer2008, WindowsServer2008R2, MACOS9, MACOSX, Linux und Unix.

Sowohl der Domänenname als auch das Betriebssystem sind optional. Ein solcher Eintrag kann folgendermaßen aussehen:

```
[GroupName1 ]  
ComputerName1
```

Computernamen werden folgendermaßen importiert:

1. Klicken Sie im Menü **Datei** auf **Computer aus Datei importieren**.
2. Markieren Sie die Datei im Browser-Fenster.
3. Klicken Sie auf die Gruppe **Nicht zugewiesen**, um die aufgefundenen Computer anzuzeigen.
4. Um die Computer zu verwalten, ziehen Sie sie in eine Gruppe.

8 Synchronisierung mit Active Directory

8.1 Informationen zur Synchronisierung mit Active Directory

In diesem Abschnitt wird die Synchronisierung mit Active Directory zusammengefasst.

Welche Vorteile bietet die Synchronisierung mit Active Directory?

Mithilfe der Synchronisierung mit Active Directory können Sie Enterprise Console-Gruppen mit Active Directory-Containern synchronisieren. Neue Computer und Container, die in Active Directory erkannt wurden, werden automatisch in Enterprise Console kopiert. Sie können außerdem erkannte Arbeitsplatzrechner mit Windows 2000 oder höher automatisch schützen. Damit wird die Zeit, in der Computer infiziert werden können, und der erforderliche Arbeitsaufwand zur Organisation und zum Schutz von Computern, reduziert.

Hinweis: Computer mit Windows 95/98, Windows Server Betriebssystemen, Mac OS, Linux oder UNIX werden nicht automatisch geschützt. Sie müssen solche Computer manuell schützen.

Nach der Einrichtung der Synchronisierung können Sie die gewünschten Einstellungen für E-Mail-Benachrichtigungen vornehmen, mit denen ausgewählte Empfänger über bei zukünftigen Synchronisierungen entdeckte neue Computer und Container informiert werden. Wenn Sie Computer in synchronisierten Enterprise Console Gruppen automatisch schützen möchten, können Sie außerdem Benachrichtigungen bei Fehlfunktionen einrichten.

So funktioniert die Synchronisierung mit Active Directory

Enterprise Console bietet „normale“, nicht synchronisierte Gruppen, die selbst verwaltet werden, und Gruppen, die mit Active Directory synchronisiert werden.

Wählen oder erstellen Sie bei der Einrichtung der Synchronisierung einen Synchronisierungspunkt, d.h. eine Enterprise Console-Gruppe, die mit einem Active Directory-Container synchronisiert wird. Alle Untergruppen und Computer, die in dem Active Directory-Container enthalten sein können, werden in Enterprise Console kopiert und mit Active Directory synchronisiert.

Hinweis: Nähere Informationen zu Synchronisierungspunkten finden Sie im Abschnitt [Was ist ein Synchronisierungspunkt?](#) (Seite 37). Nähere Informationen zu Synchronisierungspunkten finden Sie im Abschnitt [Was ist eine synchronisierte Gruppe?](#) (Seite 38).

Nachdem Sie die Synchronisierung mit Active Directory eingerichtet haben, stimmt der synchronisierte Teil der Enterprise Console-Gruppenstruktur mit dem Active Directory-Container überein, mit dem er synchronisiert wurde. Dies bedeutet Folgendes:

- Wenn ein neuer Computer zum Active Directory-Container hinzugefügt wird, erscheint er auch in der Enterprise Console.
- Wenn ein Computer aus Active Directory entfernt oder in einen nicht synchronisierten Container verschoben wird, wird der Computer in die Gruppe **Nicht zugewiesen** in Enterprise Console verschoben.

Hinweis: Wenn ein Computer in die Gruppe **Nicht zugewiesen** verschoben wird, empfängt er keine neuen Richtlinien mehr.

- Wenn ein Computer von einem synchronisierten Container in einen anderen verschoben wird, wird der Computer von einer Enterprise Console-Gruppe in eine andere verschoben.
- Wenn ein Computer bei seiner ersten Synchronisierung bereits in einer Enterprise Console-Gruppe existiert, wird er von dieser Gruppe in die synchronisierte Gruppe verschoben, die mit seinem Speicherort in Active Directory übereinstimmt.
- Wenn ein Computer in eine neue Gruppe mit verschiedenen Richtlinien verschoben wird, werden die neuen Richtlinien an den Computer gesendet.

Standardmäßig erfolgt eine Synchronisierung alle 60 Minuten. Sie können das Synchronisierungsintervall bei Bedarf ändern.

So gehen Sie bei der Synchronisierung vor

Es ist Ihnen überlassen, welche Gruppen mit Active Directory synchronisiert und wie viele Synchronisierungspunkte eingerichtet werden. Sie müssen entscheiden, ob die Größe der Gruppen, die aufgrund der Synchronisierung erstellt werden, überschaubar ist. Sie sollten in der Lage sein, problemlos Software einzusetzen und Computer zu scannen und zu bereinigen. Dies ist besonders wichtig für den ersten Einsatz.

Wir empfehlen folgende Vorgehensweise:

1. Importieren Sie die Gruppenstruktur (ohne Computer) mithilfe der Funktion **Import aus Active Directory**. Anweisungen hierzu finden Sie unter [Importieren von Containern und Computern aus Active Directory](#) (Seite 32).
2. Prüfen Sie die importierte Gruppenstruktur und wählen Sie Ihre Synchronisierungspunkte.
3. Richten Sie Gruppenrichtlinien ein und übertragen Sie diese auf die Gruppen und Untergruppen. Anweisungen hierzu finden Sie unter [Erstellen einer Richtlinie](#) (Seite 29) und [Übertragen einer Richtlinie auf eine Gruppe](#) (Seite 29).
4. Synchronisieren Sie Ihre gewählten Synchronisierungspunkte nacheinander mithilfe von Active Directory. Anweisungen hierzu finden Sie unter [Synchronisierung mit Active Directory](#) (Seite 38).

8.2 Was ist ein Synchronisierungspunkt?

Ein *Synchronisierungspunkt* ist eine Enterprise Console-Gruppe, die auf einen Container (oder eine Unterstruktur) in Active Directory verweist. Ein Synchronisierungspunkt kann Synchronisierungsgruppen enthalten, die von Active Directory importiert wurden.

Im Fensterbereich **Gruppen** erscheint ein Synchronisierungspunkt folgendermaßen:



Sie *können* einen Synchronisierungspunkt verschieben, umbenennen oder löschen. Sie können außerdem Richtlinien und Synchronisierungseinstellungen ändern, u.a. die Einstellungen für den automatischen Schutz für einen Synchronisierungspunkt.

Sie können *keine* Untergruppen in einem Synchronisierungspunkt erstellen oder löschen oder andere Gruppen in den Synchronisierungspunkt verschieben. Sie können keine Computer in einen oder aus einem Synchronisierungspunkt verschieben.

8.3 Was ist eine synchronisierte Gruppe?

Eine *synchronisierte Gruppe* ist eine Untergruppe eines Synchronisierungspunkts, die von Active Directory importiert wurde.

Im Fensterbereich **Gruppen** erscheint eine synchronisierte Gruppe folgendermaßen:



Sie *können* Richtlinien ändern, die einer synchronisierten Gruppe zugewiesen wurden.

Außer Gruppenrichtlinien können Sie *keine* Einstellungen für synchronisierte Gruppen ändern. Sie können eine synchronisierte Gruppe weder umbenennen, verschieben noch löschen. Sie können Computer oder Gruppen nicht in die oder aus der Gruppe verschieben. Sie können in der Gruppe keine Untergruppen erstellen oder löschen. Sie können für die Gruppe keine Synchronisierungseinstellungen ändern.

8.4 Synchronisierung mit Active Directory

Bei rollenbasierter Verwaltung ist hierzu die Berechtigung **Computersuche, -schutz und -gruppen** erforderlich. Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Verfahren Sie zur Synchronisierung mit Active Directory wie folgt:

1. Rechtsklicken Sie auf eine Gruppe, die als Synchronisierungspunkt eingerichtet werden soll, und wählen Sie **Synchronisierung mit Active Directory**.
Der **Assistent zur Synchronisierung mit Active Directory** wird gestartet.
2. Klicken Sie im Fenster **Überblick** des Assistenten auf **Weiter**.
3. Wählen oder erstellen Sie auf der Seite **Wählen Sie eine Enterprise Console-Gruppe** eine Enterprise Console-Gruppe, die stets mit Active Directory (Synchronisierungspunkt) synchronisiert werden soll. Klicken Sie auf **Weiter**.
4. Wählen Sie auf der Seite **Wählen Sie einen Active Directory-Container** einen Active Directory-Container, mit dem die Gruppe synchronisiert werden soll. Geben Sie den Namen des Containers ein (z.B. LDAP://CN=Computers,DC=domain_name,DC=local) oder klicken Sie auf **Durchsuchen**, um den Container in Active Directory aufzurufen. Klicken Sie auf **Weiter**.

Wichtig: Wenn ein Computer in mehreren synchronisierten Active Directory-Containern vorhanden ist, führt dies zu dem Problem, dass Nachrichten endlos zwischen ihm und Enterprise Console gesendet werden. Jeder Computer sollte in Enterprise Console nur einmal aufgeführt werden.

5. Wenn Sie Computer mit Windows 2000 oder höher automatisch schützen möchten, wählen Sie auf der Seite **Automatischer Schutz von Computern** das Kontrollkästchen **Sophos Sicherheitssoftware automatisch installieren** und dann die zu installierende Software aus.

Lassen Sie die Option **Erkennung von Fremdsoftware** ausgewählt, wenn die Software anderer Hersteller automatisch entfernt werden soll.

Wenn das Update-Tool eines anderen Herstellers entfernt werden soll, lesen Sie bitte den Abschnitt [Entfernen von Fremdsoftware](#) (Seite 44).

Hinweis:

Sie können die Firewall nicht auf Computern mit Server-Betriebssystemen oder Windows Vista Starter installieren.

Bevor Sie Sophos NAC auf Computern installieren können, müssen Sie auf den Link zur Eingabe der URL des NAC-Servers klicken.

Alle bei dieser und zukünftigen Synchronisierungen erkannten Computer mit Windows 2000 oder höher werden automatisch und in Übereinstimmung mit der jeweiligen Gruppenrichtlinie geschützt.

Wichtig: Computer mit Windows 95/98, Windows Server-Betriebssystemen, Mac OS oder Linux werden nicht automatisch geschützt. In diesem Fall muss der Schutz manuell eingerichtet werden. Lesen Sie dazu bitte die *Erweiterte Startup-Anleitung* zu *Sophos Endpoint Security and Control*.

Hinweis: Der automatische Schutz kann jederzeit über das Dialogfeld **Synchronisierungseigenschaften** aktiviert oder deaktiviert werden. Anweisungen hierzu finden Sie unter [Anzeigen und Ändern der Synchronisierungseigenschaften](#) (Seite 41).

Klicken Sie auf **Weiter**.

6. Wenn Sie Computer automatisch schützen wollen, geben Sie auf der Seite **Geben Sie Zugangsdaten für Active Directory ein** die Details eines Administratorkontos ein, das zur Installation von Software auf den Computern verwendet wird. Klicken Sie auf **Weiter**.
7. Geben Sie auf der Seite **Wählen Sie das Synchronisierungsintervall** an, wie oft die Enterprise Console-Gruppe mit dem Active Directory-Container synchronisiert werden soll. Die Vorgabe lautet 60 Minuten.

Hinweis: Das Synchronisierungsintervall kann jederzeit über das Dialogfeld **Synchronisierungseigenschaften** geändert werden. Anweisungen hierzu finden Sie unter [Anzeigen und Ändern der Synchronisierungseigenschaften](#) (Seite 41).

8. Prüfen Sie die Angaben auf der Seite **Bestätigen Sie Ihre Auswahl** und klicken Sie dann auf **Weiter**, um fortzufahren.

9. Auf der letzten Seite des Assistenten können Sie die Details der Gruppen und Computer ansehen, die synchronisiert wurden.

Sie können außerdem E-Mail-Benachrichtigungen über neue Computer und Gruppen, die bei zukünftigen Synchronisierungen gefunden werden, an die von Ihnen gewählten Empfänger senden lassen. Wenn Sie Computer in synchronisierten Gruppen automatisch schützen möchten, können Sie außerdem Benachrichtigungen für das Fehlschlagen des automatischen Schutzes einrichten. Klicken Sie auf **Beenden** und aktivieren Sie das Kontrollkästchen auf der letzten Seite des Assistenten. Das Dialogfeld **E-Mail-Benachrichtigungen konfigurieren** wird geöffnet. Anweisungen hierzu finden Sie unter [Einrichten von E-Mail-Benachrichtigungen für Active Directory-Synchronisierung](#) (Seite 171).

Klicken Sie zum Schließen des Assistenten auf **Fertig stellen**.

8.5 Automatisches Schützen von Computern über Synchronisierung

Bei rollenbasierter Verwaltung ist hierzu die Berechtigung **Computersuche, -schutz und -gruppen** erforderlich. Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Arbeitsplatzrechner mit Windows 2000 oder höher können automatisch geschützt werden, wenn sie während der Synchronisierung mit Active Directory erkannt werden.

Wichtig: Computer mit Windows 95/98, Windows Server-Betriebssystemen, Mac OS, Linux oder Unix werden nicht automatisch geschützt. In diesem Fall muss der Schutz manuell eingerichtet werden. Lesen Sie dazu bitte die *Erweiterte Startup-Anleitung zu Sophos Endpoint Security and Control*.

Der automatische Schutz von Computern in synchronisierten Gruppen lässt sich beim Einrichten der Synchronisierung (siehe [Synchronisierung mit Active Directory](#) (Seite 38)) oder durch das nachträgliche Ändern der Synchronisierungseigenschaften aktivieren.

Im Folgenden wird die Aktivierung des Schutzes von Computern in den Synchronisierungseigenschaften beschrieben.

1. Wählen Sie im Bereich **Gruppen** die Gruppe (**Synchronisierungspunkt**), für die Sie den automatischen Schutz aktivieren möchten. Rechtsklicken Sie auf die Gruppe und wählen Sie **Synchronisierungseigenschaften**.

2. Wählen Sie im Dialogfenster **Eigenschaften der Synchronisierung** das Kontrollkästchen **Sophos Sicherheitssoftware automatisch installieren** und dann die zu installierende Software aus.

Lassen Sie die Option **Erkennung von Fremdsoftware** ausgewählt, wenn die Software anderer Hersteller automatisch entfernt werden soll.

Wenn das Update-Tool eines anderen Herstellers entfernt werden soll, lesen Sie bitte den Abschnitt [Entfernen von Fremdsoftware](#) (Seite 44).

Hinweis:

Sie können die Firewall nicht auf Computern mit Server-Betriebssystemen oder Windows Vista Starter installieren.

Bevor Sie Sophos NAC auf Computern installieren können, müssen Sie auf den Link zur Eingabe der URL des NAC-Servers klicken.

3. Geben Sie die Zugangsdaten eines zur Softwareinstallation befugten Administratorkontos ein. Klicken Sie auf **OK**.

Sie können den automatischen Schutz später deaktivieren, indem Sie im Dialogfeld **Synchronisierungseigenschaften** das Kontrollkästchen neben **Sophos Sicherheitssoftware automatisch installieren** deaktivieren.

8.6 Anzeigen und Ändern der Synchronisierungseigenschaften

Bei rollenbasierter Verwaltung ist hierzu die Berechtigung **Computersuche, -schutz und -gruppen** erforderlich. Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

So ändern Sie die Synchronisierungseigenschaften:

1. Wählen Sie im Fensterbereich **Gruppen** die Gruppe (**Synchronisierungspunkt**), deren Synchronisierungseigenschaften Sie ändern möchten. Rechtsklicken Sie auf die Gruppe und wählen Sie **Synchronisierungseigenschaften**.

Das Dialogfeld **Synchronisierungseigenschaften** wird angezeigt.

2. Im Feld **Active Directory-Container** wird der Container angezeigt, mit dem die Gruppen synchronisiert wurde. Wenn Sie die Gruppe mit einem anderen Active Directory-Container synchronisieren möchten, entfernen Sie die Synchronisierung und starten Sie nochmals den **Assistenten zur Synchronisierung mit Active Directory**. Nähere Informationen finden Sie unter [Aktivieren/Deaktivieren der Synchronisierung](#) (Seite 42) und [Synchronisierung mit Active Directory](#) (Seite 38).
3. Legen Sie im Feld **Synchronisierungsintervall** die Häufigkeit der Synchronisierung fest. Die Vorgabe lautet 60 Minuten. Der Mindestwert beträgt 5 Minuten.

4. Aktivieren Sie das Kontrollkästchen **Sophos Sicherheitssoftware automatisch installieren**, wenn Sie alle neu erkannten Windows 2000- oder neueren Arbeitsplatzrechner in Übereinstimmung mit der jeweiligen Gruppenrichtlinie automatisch schützen möchten. Virenschutz ist im Bereich **Funktionen** standardmäßig aktiviert. Wenn noch andere Sophos Sicherheitssoftware installiert werden soll, aktivieren Sie die entsprechenden Kontrollkästchen. Geben Sie die Zugangsdaten eines zur Softwareinstallation befugten Administratorkontos ein.

Hinweis:

Sie können die Firewall nicht auf Computern mit Server-Betriebssystemen oder Windows Vista Starter installieren.

Bevor Sie Sophos NAC auf Computern installieren können, müssen Sie auf den Link zur Eingabe der URL des NAC-Servers klicken.

Hinweis: Nur Arbeitsplatzrechner mit Windows 2000 oder höher können automatisch geschützt werden. Computer mit Windows 95/98, Windows Server-Betriebssystemen, Mac OS, Linux oder Unix können nicht automatisch geschützt werden. In diesem Fall muss der Schutz manuell eingerichtet werden. Lesen Sie dazu bitte die *Erweiterte Startup-Anleitung* zu *Sophos Endpoint Security and Control*.

8.7 Sofortige Synchronisierung mit Active Directory

Bei rollenbasierter Verwaltung ist hierzu die Berechtigung **Computersuche, -schutz und -gruppen** erforderlich. Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Wenn Sie nicht auf das nächste Synchronisierungsintervall warten möchten, lassen sich Enterprise Console-Gruppen (Synchronisierungspunkte) auch sofort mit Active Directory-Containern synchronisieren.

So wird eine sofortige Synchronisierung durchgeführt:

1. Wählen Sie im Fensterbereich **Gruppen** die Gruppe (Synchronisierungspunkt), die mit Active Directory synchronisiert werden soll. Rechtsklicken Sie auf die Gruppe und wählen Sie **Synchronisierungseigenschaften**.
2. Wenn Sie die gewünschten Änderungen vorgenommen haben, klicken Sie auf **OK**.

8.8 Aktivieren/Deaktivieren der Synchronisierung

Bei rollenbasierter Verwaltung ist hierzu die Berechtigung **Computersuche, -schutz und -gruppen** erforderlich. Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

- Zum Aktivieren der Synchronisierung starten Sie den **Assistent zur Synchronisierung mit Active Directory** (siehe Abschnitt [Synchronisierung mit Active Directory](#) (Seite 38)).
- Um die Synchronisierung zu deaktivieren, rechtsklicken Sie auf die Gruppe (**Synchronisierungspunkt**), die Sie nicht mehr mit Active Directory synchronisieren möchten, und wählen Sie **Synchronisierung aufheben**. Klicken Sie auf **Ja** zur Bestätigung.

9 Schützen von Computern

9.1 Vorbereiten der Installation der Virenschutzsoftware

Sie müssen nicht nur dafür sorgen, dass die allgemeinen Systemanforderungen erfüllt werden, es sind außerdem noch weitere Schritte notwendig, bevor auf den Computern Software automatisch installiert werden kann.

Bereiten Sie die Installation der Virenschutzsoftware vor:

1. Unter Windows Vista:

- a) Der Remote-Registrierungsdienst muss gestartet werden und der Starttyp „Automatisch“ lauten. Dieser Dienst ist unter Windows Vista standardmäßig nicht aktiv.
- b) Deaktivieren Sie die Benutzerkontensteuerung. Nach der Installation sollten Sie sie wieder aktivieren.
- c) Deaktivieren Sie den Freigabeassistenten.
- d) Öffnen Sie die Windows-Firewall mit erweiterter Sicherheit. Öffnen Sie in der Systemsteuerung die **Verwaltung**. Stellen Sie sicher, dass **Eingehende Verbindungen** zugelassen werden.
- e) Lassen Sie unter **Eingehende Regeln** die folgenden Prozesse zu. Deaktivieren Sie nach der Installation diese Prozesse wieder.

Remoteverwaltung (NP eingehend) Domäne

Remoteverwaltung (NP eingehend) Privat

Remoteverwaltung (RPC) Domäne

Remoteverwaltung (RPC) Privat

Remoteverwaltung (RPC-EPMAP) Domäne

Remoteverwaltung (RPC-EPMAP) Privat

2. Unter Windows 2003/XP Pro/2000/NT:

- a) Die Dienste „Remoteregistrierung“, „Server“, „Computerbrowser“ und „Taskplaner“ müssen laufen.
- b) Die C\$-Admin-Freigabe muss aktiviert sein.
- c) „Einfache Dateifreigabe“ muss deaktiviert sein (nur XP).

3. Unter Windows XP SP2 oder SP3:
 - a) Die Dienste „Remoteregistrierung“, „Server“, „Computerbrowser“ und „Taskplaner“ müssen laufen.
 - b) Die C\$-Admin-Freigabe muss aktiviert sein.
 - c) „Einfache Dateifreigabe“ muss deaktiviert sein.
 - d) Aktivieren Sie die Datei- und Druckerfreigabe für Microsoft-Netzwerke.
 - e) Die TCP-Ports 8192, 8193 und 8194 müssen geöffnet sein.
 - f) Die Änderungen werden erst nach einem Neustart des Computers wirksam.

9.2 Entfernen von Fremdsoftware

Wenn Sie installierte Sicherheitssoftware entfernen möchten, sollten Sie zunächst wie folgt vorgehen, bevor Sie **Erkennung von Fremdsoftware** im Assistenten zum **Schutz von Computern** auswählen und installieren:

- Wenn auf dem Computer Antivirensoftware von einem anderen Anbieter installiert ist, stellen Sie sicher, dass die Benutzeroberfläche der Software geschlossen ist.
- Wenn auf Computern eine Firewall oder ein HIPS-Produkt anderer Hersteller ausgeführt wird, muss es deaktiviert oder dazu konfiguriert sein, dass das Sophos Installationsprogramm ausgeführt werden kann.
- Wenn nicht nur die Software sondern auch das Update-Tool eines anderen Herstellers entfernt werden soll (zur Verhinderung einer automatischen Neuinstallation), führen Sie bitte die folgenden Schritte aus. Falls auf den Computern kein Update-Tool installiert wurde, ignorieren Sie diese Schritte.

Hinweis: Alle Computer, von denen Virenschutzsoftware anderer Hersteller entfernt wird, müssen lokal neu gestartet werden.

Wenn auf Computern ein Update-Tool eines anderen Herstellers installiert ist und es entfernt werden soll, muss die Konfigurationsdatei geändert werden, bevor im **Assistenten zum Schutz für Computer** die **Erkennung von Fremdsoftware** ausgeführt werden kann:

Hinweis: Wenn auf einem Computer eine Firewall oder HIPS-Produkte eines anderen Herstellers installiert sind, lassen Sie das entsprechende Update-Tool unberührt. Für weitere Informationen lesen Sie die Dokumentation des anderen Herstellers.

So ändern Sie die Konfigurationsdatei:

1. Suchen Sie im zentralen Installationsverzeichnis die Datei „data.zip“.
2. Extrahieren Sie die Konfigurationsdatei „crt.cfg“ aus der Datei „data.zip“.
3. Ändern Sie in der Datei „crt.cfg“ die Zeile „RemoveUpdateTools=0“ in „RemoveUpdateTools=1“.
4. Speichern Sie Ihre Änderungen und speichern Sie „crt.cfg“ im Verzeichnis, das auch „data.zip“ enthält. Verschieben Sie „crt.cfg“ nicht wieder nach „data.zip“, da die Datei ansonsten bei der nächsten Aktualisierung von „data.zip“ überschrieben wird.

Wenn Sie den Assistenten zum **Schutz von Computern** ausführen und die **Erkennung von Fremdsoftware** auswählen, entfernt die geänderte Konfigurationsdatei jegliche Sicherheits-Tools und Sicherheitssoftware von anderen Anbietern.

9.3 Schützen von Computern

Treffen Sie zunächst folgende Vorbereitungen:

- Sie müssen der Gruppe eine Update-Richtlinie zuweisen. Erst dann können die Computer in der Gruppe geschützt werden.
- Wenn Sie Windows XP-Computer automatisch von der Konsole aus schützen möchten, stellen Sie sicher, dass die „Einfache Dateifreigabe“ deaktiviert ist.
- Bei rollenbasierter Verwaltung ist hierzu die Berechtigung **Computersuche, -schutz und -gruppen** erforderlich. Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 13).

Eine automatische Installation ist auf Computern unter Windows 95/98, Mac, Linux und UNIX nicht möglich. Führen Sie die Installation auf diesen Betriebssystemen manuell durch. Nähere Anweisungen können Sie der *Erweiterten Startup-Anleitung für Sophos Endpoint Security and Control* entnehmen. Begleitmaterial zu Sophos Software finden Sie hier: www.sophos.de/support/docs/.

Wenn Sie mit Active Directory synchronisieren und die Computer automatisch schützen, müssen Sie die nachfolgenden Schritte *nicht* befolgen. Details finden Sie u.a. im Abschnitt *Informationen zur Synchronisierung mit Active Directory* (Seite 36).

So können Sie Computer schützen:

1. Verfahren Sie in Abhängigkeit davon, ob sich die Computer bereits in der Gruppe befinden, anhand einer der folgenden Methoden:
 - Wenn sich die Computer, die Sie schützen möchten, in der Gruppe **Nicht zugewiesen** befinden, ziehen Sie sie in eine Gruppe.
 - Wenn die Computer bereits einer Gruppe zugewiesen wurden, wählen Sie sie aus, rechtsklicken Sie darauf und klicken Sie auf **Computer schützen**.

Der **Assistent zum Schutz für Computer** wird gestartet.

2. Befolgen Sie die Anweisungen des Assistenten. Wählen Sie auf der Seite **Funktionsauswahl** die gewünschten Funktionen aus.

Der Antivirenschutz ist immer ausgewählt und muss installiert werden. Sie können auch folgende Funktionen installieren:

- **Compliance Control** (ein Agent für Sophos NAC)

Compliance Control steht nur zur Verfügung, wenn die Komponente in Ihrer Lizenz enthalten ist, und beschränkt sich auf Windows 2000 oder höher.

Vor dem Einsatz von Compliance Control müssen Sie die NAC-Server-URL angeben. Wenn Sophos NAC auf mehreren Servern installiert ist, geben Sie die URL des Computers ein, auf dem der Anwendungsserver ausgeführt wird, und nicht die des Computers mit der Datenbank.

■ **Sophos Client Firewall**

Die Client Firewall steht nur zur Verfügung, wenn die Komponente in Ihrer Lizenz enthalten ist, und beschränkt sich auf Windows 2000 oder höher.

Sie können die Firewall nicht auf Computern mit Server-Betriebssystemen oder Windows Vista Starter installieren.

■ **Erkennung von Fremdsoftware**

Lassen Sie die Option **Erkennung von Fremdsoftware** ausgewählt, wenn die Software anderer Hersteller automatisch entfernt werden soll. Durch die Erkennung von Fremdsoftware werden nur Produkte mit demselben Funktionsumfang wie die von Ihnen installierten Produkte deinstalliert.

3. Auf der Seite **Schutz-Übersicht** werden Installationsprobleme in der Spalte **Sicherheitshinweise** angezeigt. Beheben Sie die Installationsprobleme anhand der Anweisungen im Abschnitt *Sophos Endpoint Security and Control konnte nicht installiert werden* (Seite 191) oder führen Sie auf diesen Computern die Installation manuell durch (mehr Informationen hierzu können Sie der *Erweiterten Startup-Anleitung für Sophos Endpoint Security and Control* entnehmen). Klicken Sie auf **Next**.
4. Geben Sie auf der Seite **Zugangsdaten** die Zugangsdaten eines Kontos ein, mit dem Software installiert werden kann.

Bei diesem Konto handelt es sich in der Regel um ein Domänen-Administratorkonto. Das Konto muss:

- lokale Administratorrechte auf den Computern haben, die Sie schützen möchten.
- sich auf dem Computer anmelden können, auf dem Sie den Management-Server installiert haben.
- Lesezugriff auf den Primary Server-Ort haben, der in der **Update**-Richtlinie angegeben wurde. Mehr dazu erfahren Sie unter *Auswahl der Update-Quelle* (Seite 104).

Hinweis: Wenn Sie ein Domäne-Konto verwenden, *müssen* Sie den Benutzernamen in der Form **Domäne\Benutzer** eingeben.

Wenn Computer auf unterschiedlichen Domänen demselben Active Directory-Schema unterliegen, verwenden Sie das Unternehmensadministratorkonto von Active Directory.

9.4 Anzeigen der Bootstrap-Verzeichnisse

Wenn Enterprise Console auf bestimmten Computern die Virenschutz-, Firewall- oder NAC-Software nicht automatisch installieren kann, können Sie die Installation manuell durchführen.

So können Sie die Installationsprogramme auffinden:

1. Klicken Sie im Menü **Ansicht** auf **Bootstrap-Verzeichnisse**.

2. Im Dialogfeld **Bootstrap-Verzeichnisse** werden für die einzelnen Software-Abonnements die Verzeichnisse mit den Installern sowie die unterstützten Plattformen und Software-Versionen angezeigt. Schreiben Sie sich den Speicherort der benötigten Datei auf.

Wenn die Firewall in Ihrer Lizenz enthalten ist, können Sie diese mit der Antiviren- und NAC- Software unter Windows 2000 und höher installieren. Der Installer mit dem genannten Funktionsumfang befindet sich im Verzeichnis „SAVSCFXP“.

Anweisungen zur manuellen Installation von Sicherheitssoftware auf unterschiedlichen Betriebssystemen finden Sie in der *Erweiterten Startup-Anleitung zu Sophos Endpoint Security and Control*.

10 Ermitteln des Netzwerkschutzes

10.1 So überprüfen Sie, ob Ihr Netzwerk geschützt ist

Das Dashboard bietet Ihnen einen Überblick über den Sicherheitsstatus des Netzwerks. Mehr dazu erfahren Sie unter [Übersicht über das Dashboard](#) (Seite 48) und [Konfigurieren des Dashboards](#) (Seite 51).

Mit Computerlisten und Computerlistenfiltern können Sie problematische Computer ermitteln. So können Sie beispielsweise Computer auffinden, auf denen keine Firewall installiert ist, oder auf denen Meldungen angezeigt werden, bei denen Benutzereingriff erforderlich ist. Mehr dazu erfahren Sie unter [Überprüfen, ob die Computer geschützt sind](#) (Seite 51), [Überprüfen, ob sich die Computer auf dem neuesten Stand befinden](#) (Seite 52) und [Auffinden von Computern mit Problemen](#) (Seite 52).

Zudem können Sie überprüfen, ob alle Computer in einer Gruppe mit den Richtlinien der Gruppe übereinstimmen. Details hierzu finden Sie im Abschnitt [Prüfen, ob Computer die Gruppenrichtlinie verwenden](#) (Seite 31).

10.2 Übersicht über das Dashboard

Mit dem Dashboard können Sie den Sicherheitsstatus Ihres Netzwerks überprüfen. Klicken Sie zum Anzeigen/Ausblenden des Dashboards auf die Schaltfläche **Dashboard** in der Symbolleiste.



Abbildung 4: Das Dashboard

Die Dashboard-Benutzeroberfläche

Das Dashboard setzt sich aus den folgenden sieben Bereichen zusammen:

Computer

In diesem Abschnitt wird die Gesamtanzahl der Computer im Netzwerk sowie die Anzahl verbundener, verwalteter und nicht verwalteter Computer angezeigt.

Klicken Sie zum Anzeigen einer Liste verwalteter, nicht verwalteter, verbundener oder aller Computer auf einen der Links im Bereich **Computer**.

Updates

Aus diesem Bereich geht der Status des Update Managers hervor.

Computer mit Alerts

In diesem Abschnitt werden die Anzahl und der prozentuale Anteil 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 wird die Anzahl der Computer angezeigt, auf denen die Summe der Ereignisse in den vergangenen 7 Tagen den angegebenen Höchstwert überschritten hat.

Klicken Sie auf den jeweiligen Link im Abschnitt **Computer über Ereignis-Grenzwert**, um eine Liste der Computer mit Device Control-, Data Control-, Controlled Application- oder Firewall-Ereignissen aufzurufen.

Richtlinien

In diesem Bereich werden die Anzahl und der prozentuale Anteil verwalteter Computer mit Verstößen gegen Gruppenrichtlinien oder Richtlinienabgleichsfehlern angezeigt. Dazu gehören auch Computer, die noch nicht auf die geänderte Richtlinie reagiert haben, die ihnen von der Konsole gesendet wurde.

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

Schutz

In diesem Abschnitt werden die Anzahl und der prozentuale Anteil verwalteter und verbundener Computer angezeigt, auf denen Sophos Endpoint Security and Control oder Sophos Anti-Virus nicht aktuell sind oder die unbekannte Erkennungsdaten verwenden.

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




Fehler

In diesem Bereich werden die Anzahl und der prozentuale Anteil verwalteter Computer mit ausstehenden Scans, Updates oder Firewall-Fehlern angezeigt.

Klicken Sie zur Anzeige einer Liste verwalteter Computer mit ausstehenden Sophos Produktfehlern auf **Fehler**.

Die Sicherheitsstatusanzeigen des Dashboards

Das Dashboard kann drei Sicherheitsstatusanzeigen anzeigen.

Symbol	Erklärung
	Eine grüne Anzeige entspricht dem Status „Normal“. Die Anzahl betroffener Computer liegt unter der Warnstufe.
	Eine gelbe Anzeige weist auf den Warnstatus hin. Der Warnschwellenwert wurde überschritten.
	Eine rote Anzeige entspricht dem „kritischen“ Status. Der kritische Schwellenwert wurde überschritten.

Die Anzeigen werden für jeden Abschnitt und für das gesamte Dashboard angezeigt.

Hinweis: Eine *Statusanzeige des Dashboard-Bereichs* ist ein Symbol, das in der rechten oberen Ecke eines Dashboard-Bereichs neben der Überschrift erscheint und den Status eines bestimmten Sicherheitsbereichs anzeigt, der von dem Abschnitt dargestellt wird.

Eine Statusanzeige des Dashboard-Bereichs zeigt den Status einer Bereichsanzeige mit dem schwerwiegendsten Status an, d.h.:

- Eine Statusanzeige des Bereichs ändert sich von „Normal“ in „Warnung“, wenn ein Warnschwellenwert für mindestens eine Anzeige in dem Bereich überschritten wird.
- Eine Statusanzeige des Bereichs ändert sich von „Warnung“ in „Kritisch“, wenn ein kritischer Schwellenwert für mindestens eine Anzeige in dem Bereich überschritten wird.

Hinweis: Die *Statusanzeige für das Netzwerk* ist ein Symbol, das in der rechten unteren Ecke der Statuszeile des Enterprise Console-Fensters angezeigt wird und den gesamten Sicherheitsstatus des Netzwerks darstellt.

Eine Statusanzeige für das Netzwerk zeigt den Status des Dashboard-Bereichs mit dem schwerwiegendsten Status an, d.h.:

- Eine Statusanzeige für das Netzwerk ändert sich von „Normal“ auf „Warnung“, wenn ein Warnschwellenwert für mindestens eine Anzeige im Dashboard überschritten wird.
- Eine Statusanzeige für das Netzwerk ändert sich von „Warnung“ in „Kritisch“, wenn ein kritischer Schwellenwert für mindestens eine Anzeige im Dashboard überschritten wird.

Bei der Erstinstallation oder einem Upgrade von Enterprise Console übernimmt das Dashboard die Standardwarnstufen und kritischen Stufen. Sie können Ihre eigene Warnstufen und kritischen Stufen im Dialogfeld **Dashboard-Konfiguration** anlegen. Im Abschnitt [Konfigurieren des Dashboards](#) (Seite 51) finden Sie Anweisungen hierzu.

Sie können außerdem E-Mail-Benachrichtigungen einrichten, die an ausgewählte Empfänger gesendet werden sollen, wenn eine Warnstufe oder eine kritische Stufe für einen Dashboard-Bereich überschritten wird. Genaue Anweisungen finden Sie unter [Einrichten von Netzwerkstatus-E-Mail-Benachrichtigungen](#) (Seite 170).

10.3 Konfigurieren des Dashboards

Bei rollenbasierter Verwaltung müssen Sie zur Konfiguration des Dashboards über die Berechtigung **Systemkonfiguration** verfügen. Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Im Dashboard wird auf der Basis des Prozentsatzes der verwalteten Computer, auf denen Alerts oder Fehler ausstehen, oder der Zeit, die seit dem letzten Update von Sophos vergangen ist, angezeigt, wenn eine Warnstufe oder kritische Stufe erreicht wurde.

Sie können die Warnstufen bzw. kritischen Stufen nach Ihren Wünschen konfigurieren.

1. Klicken Sie im Menü **Extras** auf die Option **Dashboard konfigurieren**.
2. Ändern Sie im Dialogfeld **Dashboard konfigurieren** die zulässigen Höchstwerte in den Textfeldern **Warnstufe** und **Kritische Stufe**. Anweisungen hierzu finden Sie im Folgenden.
 - a) Geben Sie in die Felder **Computer mit ausstehenden Alerts**, **Computer mit fehlerhaften Sophos Produkten** und **Richtlinien und Schutz** den Prozentsatz aller Computer an, die von einem bestimmten Problem maximal betroffen sein dürfen, bis sich die Anzeige in „Warnung“ oder „kritisch“ ändert.
 - b) Geben Sie in das Feld **Computer mit Ereignissen** die Anzahl an Ereignissen ein, die binnen 7 Tagen stattfinden dürfen sollen, bis ein Alert im Dashboard angezeigt wird.
 - c) Geben Sie unter **Letztes Update von Sophos** die Zeit in Stunden, die seit dem letzten erfolgreichen Update von Sophos verstreichen darf, bis die Update-Anzeige von „Warnung“ auf „Kritisch“ geändert wird. Klicken Sie auf **OK**.

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

Sie können außerdem E-Mail-Benachrichtigungen einstellen, die an die gewählten Empfänger gesendet werden sollen, wenn ein Warn- oder ein kritischer Schwellenwert überschritten wurde. Genaue Anweisungen finden Sie unter [Einrichten von Netzwerkstatus-E-Mail-Benachrichtigungen](#) (Seite 170).

10.4 Überprüfen, ob die Computer geschützt sind

Computer sind geschützt, wenn On-Access-Scans und Firewall (sofern installiert) aktiv sind. Für einen vollständigen Schutz muss sich die Software außerdem auf dem neuesten Stand befinden.

Hinweis: Möglicherweise haben Sie sich entschieden, bei bestimmten Computertypen, z.B. auf Fileservern, die On-Access-Scanfunktion zu deaktivieren. Stellen Sie in diesem Fall sicher, dass auf diesen Computern geplante Scans laufen und dass sie aktuell sind.

So überprüfen Sie, ob die Computer geschützt sind:

1. Markieren Sie die Computergruppe, die Sie prüfen möchten.
2. Wenn Sie Computer in einer Untergruppe der Gruppe prüfen möchten, wählen Sie oben rechts in der Dropdown-Liste **Diese Ebene und abwärts**.

- Suchen Sie in der Computerliste auf der Registerkarte **Status** die Spalte **On-Access**.

Wenn in dieser Spalte für den Computer „Aktiv“ angezeigt wird, ist auf dem Computer die On-Access-Scanfunktion aktiviert. Wenn Sie ein graues Schild-Symbol sehen, ist die On-Access-Scanfunktion auf diesem Computer nicht aktiviert.

- Wenn Sie die Firewall installiert haben, sehen Sie in der Spalte **Firewall aktiviert** nach.

Wenn dort „Ja“ steht, ist die Firewall aktiviert. Wenn ein graues Firewall-Symbol und ein „Nein“ angezeigt wird, ist die Firewall deaktiviert.

- Den Status anderer Funktionen (z.B. Application Control oder Data Control) können Sie in der entsprechenden Spalte einsehen.

Weitere Informationen zum Überprüfen des Computerschutzes finden Sie unter [Überprüfen, ob sich die Computer auf dem neuesten Stand befinden](#) (Seite 52).

Weitere Informationen zum Auffinden von Computern mit Problemen über Computerlistenfilter finden Sie unter [Auffinden von Computern mit Problemen](#) (Seite 52).

10.5 Überprüfen, ob sich die Computer auf dem neuesten Stand befinden

Wenn Sie Enterprise Console wie empfohlen eingerichtet haben, sollten die Computer automatisch Updates erhalten.

So können Sie feststellen, ob der Computerschutz auf dem neuesten Stand ist:

- Markieren Sie die Computergruppe, die Sie prüfen möchten.
- Wenn Sie Computer in einer Untergruppe der Gruppe prüfen möchten, wählen Sie oben rechts in der Drop-Down-Liste **Auf dieser Stufe und darunter**.
- Betrachten Sie auf der Registerkarte **Status** die Spalte **Auf dem neuesten Stand** oder rufen Sie die Registerkarte **Update-Details** auf.
 - Wenn in der Spalte **Auf dem neuesten Stand** „Ja“ steht, befindet sich der Computer auf dem neuesten Stand.
 - Wenn ein Uhrensymbol angezeigt wird, befindet sich der Computer nicht auf dem neuesten Stand. Aus dem Text geht hervor, seit wann sich der Computer nicht mehr auf dem neuesten Stand befindet.

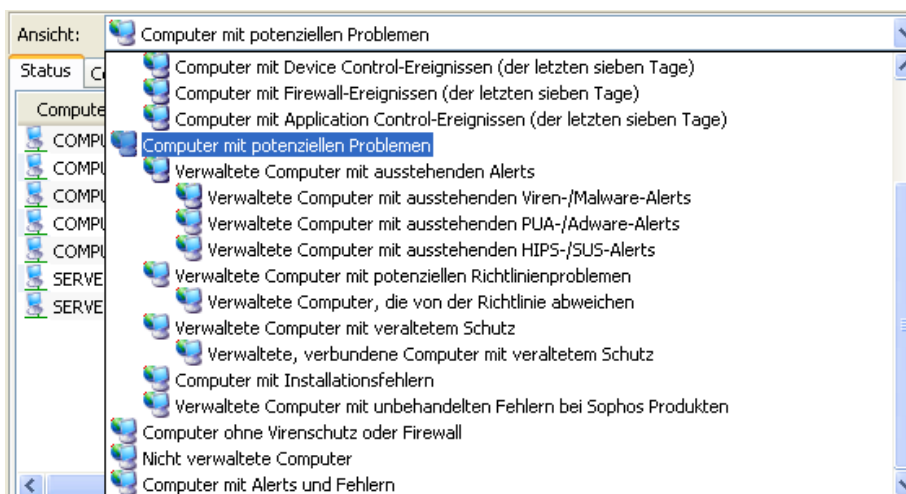
Informationen zum Updaten solcher Computer finden Sie im Abschnitt [Updaten nicht aktueller Computer](#) (Seite 68).

10.6 Auffinden von Computern mit Problemen

So können Sie sich eine Liste der Computer anzeigen lassen, die nicht hinreichend geschützt sind bzw. bei denen Probleme mit dem Computerschutz aufgetreten sind:

- Markieren Sie die Computergruppe, die Sie prüfen möchten.

- Wählen Sie im Dropdown-Menü **Ansicht** die gewünschten Computer aus, z.B. **Computer mit potenziellen Problemen**.



Sie können außerdem einen untergeordneten Eintrag dieses Eintrags auswählen, um von einem bestimmten Problem betroffene Computer anzuzeigen (z.B. Computer, die von einer Gruppenrichtlinie abweichen, Computer mit ausstehenden Alerts oder Computer, bei denen ein Installationsfehler aufgetreten ist).

- Wenn die Gruppe auch Untergruppen enthält, wählen Sie, ob Sie Computer **Nur auf dieser Ebene** oder **Diese Ebene und abwärts** suchen möchten.

Alle Computer mit Schutzproblemen werden aufgelistet.

Nähere Informationen zum Beheben von Schutzproblemen finden Sie im Abschnitt „Fehlersuche“.

11 Benachrichtigungen, Alerts und Fehlermeldungen



11.1 Was bedeuten die Alert-Symbole?

Wenn ein Virus oder Spyware, ein verdächtiges Objekt, Adware oder eine andere potenziell unerwünschte Anwendung erkannt wird, werden Alert-Symbole in der Ansicht **Endpoints** auf der Registerkarte **Status** angezeigt.

Alerts werden in der folgenden Tabelle erklärt. Die anderen Unterabschnitte bieten Anweisungen zum Umgang mit Alerts.

Hinweis: In der Konsole werden außerdem Warnungen angezeigt, wenn Software deaktiviert wurde oder nicht aktuell ist. Weitere Informationen finden Sie unter [So überprüfen Sie, ob Ihr Netzwerk geschützt ist](#) (Seite 48).

Alert-Symbole

Symbol	Erklärung
	Ein rotes Warnsymbol in der Spalte Alarmer und Fehler deutet darauf hin, dass ein Virus, Wurm, Trojaner, Spyware oder verdächtiges Verhalten erkannt wurde.
	Ein gelbes Warnsymbol in der Spalte Alerts und Fehler deutet auf eines der folgenden Probleme hin: <ul style="list-style-type: none"> ■ Eine verdächtige Datei wurde erkannt. ■ Adware oder eine andere potenziell unerwünschte Anwendung wurde erkannt. ■ Ein Fehler ist aufgetreten. Ein gelbes Warnsymbol in der Spalte Richtlinienkonformität weist darauf hin, dass die Richtlinie(n) des Computers von den anderen Computern der Gruppe abweichen.

Wenn für einen Computer mehrere Alerts oder Fehler vorhanden sind, wird in der Spalte **Alerts und Fehler** 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)

Details zu Alerts (z.B. einem erkannten Objekt) finden Sie auf der Registerkarte **Alert- und Fehlerdetails**.

11.2 Umgang mit Alerts zu erkannten Objekten

Bei rollenbasierter Verwaltung gilt als Voraussetzung für das Bereinigen von erkannten Objekten bzw. das Löschen von Alerts die Berechtigung **Korrektur – Bereinigung**. Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

So können Sie die in der Konsole angezeigten Alerts beheben:

1. Markieren Sie in der Ansicht **Endpoints** die Computer, deren Alerts sie anzeigen möchten. Rechtsklicken Sie auf die Auswahl und wählen Sie **Alerts und Fehler löschen** aus.

Das Dialogfeld **Alerts und Fehler löschen** wird angezeigt.

2. Die zu ergreifende Maßnahme hängt von dem Bereinigungsstatus des Alerts ab. Sehen Sie sich die Spalte **Bereinigungsstatus** an, um zu entscheiden, welche Maßnahme ergriffen werden soll.

Tipp: Sie können auf eine Spaltenüberschrift klicken, um Alerts zu sortieren. So können Sie Alerts etwa nach ihrem **Bereinigungsstatus** sortieren, indem Sie auf die gleichnamige Spaltenüberschrift klicken.

Bereinigungsstatus	Beschreibung und zu ergreifende Maßnahme
Bereinigung möglich	Sie können das Objekt löschen. Wählen Sie hierzu den/die Alert(s) aus und klicken Sie auf Bereinigung .
Threat-Typ kann nicht bereinigt werden	Solche erkannten Objekte (z.B. verdächtige Dateien oder verdächtiges Verhalten) lassen sich nicht über die Konsole bereinigen. Sie müssen selbst bestimmen, ob das Objekt zugelassen oder gesperrt werden soll. Sie können Objekte, die Sie nicht als vertrauenswürdig erachten, an Sophos zur Analyse schicken. Weitere Informationen finden Sie unter Auffinden von Informationen zu erkannten Objekten (Seite 56).
Keine Bereinigung möglich	Solche Objekte können nicht über die Konsole bereinigt werden. Nähere Informationen zu Objekten und den entsprechenden Gegenmaßnahmen finden Sie unter Auffinden von Informationen zu erkannten Objekten (Seite 56).
Vollständige Systemüberprüfung erforderlich	Dieses Objekt kann zwar eventuell bereinigt werden, jedoch nur im Zuge einer vollständigen Systemüberprüfung des Endpoints. Anweisungen hierzu finden Sie unter Sofort-Scans (Seite 67).
Neustart erforderlich	Das Objekt wurde teilweise entfernt, die Bereinigung kann jedoch erst nach einem Neustart des Endpoints abgeschlossen werden. Hinweis: Endpoints müssen lokal und nicht von Enterprise Console neu gestartet werden.
Bereinigung fehlgeschlagen	Das Objekt konnte nicht entfernt werden. Unter Umständen ist eine manuelle Bereinigung erforderlich. Weitere Informationen finden Sie unter Bearbeiten erkannter Objekte, falls die Bereinigung fehlschlägt (Seite 58).

Bereinigungsstatus	Beschreibung und zu ergreifende Maßnahme
Bereinigung wird durchgeführt (Start <Zeit>)	Bereinigung wird durchgeführt
Zeit für Bereinigung abgelaufen (Beginn <Zeit>)	Zeit für Bereinigung abgelaufen. Das Objekt wurde möglicherweise nicht bereinigt. Dies kann etwa der Fall sein, wenn der Endpoint nicht mit dem Netzwerk verbunden ist oder das Netzwerk überlastet ist. Sie können versuchen, die Bereinigung zu einem späteren Zeitpunkt zu wiederholen.

Nähere Informationen zum Zulassen von Objekten finden Sie unter [Zulassen von Adware und PUA](#) (Seite 90) und [Zulassen verdächtiger Objekte](#) (Seite 86).

11.3 Auffinden von Informationen zu erkannten Objekten

Anhand der folgenden Schritte erhalten Sie nähere Informationen zu Threats oder sonstigen auf einem Endpoint erkannten und in der Konsole gemeldeten Objekten sowie zu den zu ergreifenden Gegenmaßnahmen:

1. Doppelklicken Sie in der Ansicht **Endpoints** in der Computerliste auf den betroffenen Computer.
2. Scrollen Sie im Dialogfeld **Computer-Details** zur Option **Ausstehende Alerts und Fehler**. Klicken Sie in der Liste mit den erkannten Objekten auf den Namen des gewünschten Objekts.

Sie werden mit der Sophos Website verbunden. Hier finden Sie eine Beschreibung des Objekts und Hinweise zu den zu ergreifenden Gegenmaßnahmen.

Hinweis: Sie können jedoch die **Sicherheitsanalyseseite** auf der Sophos Website (<http://www.sophos.de/security/analyses/>) aufrufen. Klicken Sie auf die Registerkarte des gewünschten Objekttyps , geben Sie den Namen des Objekts in das Suchfeld ein oder suchen Sie es in der Objektliste.

11.4 Löschen von Endpoint-Alerts und -Fehlern über die Konsole

Bei rollenbasierter Administration gilt als Voraussetzung für das Löschen von Alerts und Fehlern die Berechtigung **Korrektur – Bereinigung**. Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Wenn Sie Maßnahmen bei Alerts ergreifen oder wissen, dass der Computer sicher ist, können Sie das in der Konsole angezeigte Alert-Symbol löschen.

Hinweis: Alerts zu Installationsfehlern lassen sich nicht löschen. Alerts lassen sich nur löschen, wenn Sophos Endpoint Security and Control auf dem Computer installiert ist.

1. Markieren Sie in der Ansicht **Endpoints** die Computer, für die Sie Alerts löschen möchten. Rechtsklicken Sie auf die Auswahl und wählen Sie **Alerts und Fehler löschen** aus.

Das Dialogfeld **Alerts und Fehler löschen** wird angezeigt.

2. Rufen Sie zum Löschen von Alerts oder Fehlermeldungen bei Sophos Produkten die Registerkarte „Alerts“ bzw. „Fehler“ auf, wählen Sie die gewünschten Alerts/Fehler aus und klicken Sie auf **Löschen**.

Gelöschte Alerts werden nicht mehr in der Konsole angezeigt.

Weitere Informationen zum Löschen von Update Manager-Alerts aus der Konsole finden Sie unter [Löschen von Update Manager-Alerts aus der Konsole](#) (Seite 57).

11.5 Löschen von Update Manager-Alerts aus der Konsole

Bei rollenbasierter Administration gilt als Voraussetzung für das Löschen von Alerts die Berechtigung **Korrektur – Bereinigung**. Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

So löschen Sie Update Manager-Alerts aus der Konsole:

1. Markieren Sie in der Ansicht **Update Manager** die zu löschenden Alerts. Rechtsklicken Sie und wählen Sie **Alerts löschen**.

Das Fenster **Update Manager-Alerts** wird angezeigt.

2. Um die Alerts zu löschen, wählen Sie die gewünschten Alerts aus und klicken Sie auf **Löschen**.

Gelöschte Alerts werden nicht mehr in der Konsole angezeigt.

12 Bereinigen von Computern

12.1 Sofortiges Bereinigen von Computern

Computer unter Windows 2000 und höher, auf denen sich ein Virus oder unerwünschte Anwendungen befinden, können sofort bereinigt werden.

Bei rollenbasierter Verwaltung müssen Sie zur Bereinigung über die Berechtigung **Korrektur – Bereinigung** verfügen. Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Hinweis: Zur Bereinigung von Windows 95/98/Me- und NT4-, Macintosh-, Linux- oder UNIX-Systemen können Sie entweder anhand der Anweisungen im Abschnitt [Einrichten der automatischen Bereinigung](#) (Seite 59) eine automatische Bereinigung von der Konsole aus einrichten oder die Computer einzeln bereinigen, wie unter [Bearbeiten erkannter Objekte, falls die Bereinigung fehlschlägt](#) (Seite 58) beschrieben.

Wenn ein Objekt (z.B. ein Trojaner oder eine potenziell unerwünschte Anwendung) vor der Bereinigung des betroffenen Computers „teilweise erkannt“ wurde, führen Sie eine vollständige Systemüberprüfung durch, um alle Komponenten des erkannten Objektfragments aufzufinden. Wechseln Sie in der Computerliste in die Ansicht **Endpoints**, rechtsklicken Sie auf den betroffenen Computer und klicken Sie auf **Vollständige Systemüberprüfung**. Weitere Informationen finden Sie unter [Zum Teil erkanntes Objekt](#) (Seite 193).

So können Sie Ihre Computer sofort bereinigen:

1. Wechseln Sie in der Computerliste in die Ansicht **Endpoints**, rechtsklicken Sie auf den/die zu bereinigenden Computer und wählen Sie **Alerts und Fehler löschen**.
2. Wählen Sie im Dialogfeld **Alerts und Fehler löschen** die Registerkarte **Alerts**. Aktivieren Sie das Kontrollkästchen neben allen Objekten, die Sie bereinigen möchten oder klicken Sie auf **Alles markieren**. Klicken Sie auf **Bereinigung**.

Wenn die Bereinigung erfolgreich war, werden die Alerts der Computerliste nicht mehr angezeigt.

Wenn weiterhin Alerts vorhanden sind, sollten Sie die Computer manuell bereinigen. Mehr dazu erfahren Sie unter [Bearbeiten erkannter Objekte, falls die Bereinigung fehlschlägt](#) (Seite 58).

12.2 Bearbeiten erkannter Objekte, falls die Bereinigung fehlschlägt

Wenn Sie Computer nicht von der Konsole aus bereinigen können, führen Sie die Bereinigung manuell durch:

1. Doppelklicken Sie in der Computerliste auf den infizierten Computer.
2. Scrollen Sie im Dialogfeld **Computer-Details** zur Option **Ausstehende Alerts und Fehler**. Klicken Sie in der Liste mit den erkannten Objekten auf das Objekt, das Sie entfernen möchten.

Eine Verbindung zur Sophos Website wird hergestellt; hier finden Sie Tipps zur Bereinigung des Computers.

3. Gehen Sie zu dem Computer und führen Sie die Bereinigung manuell durch.

Hinweis: Auf der Sophos Website stehen außerdem spezielle Desinfektions-Tools für bestimmte Viren und Würmer zum Download bereit.

12.3 Einrichten der automatischen Bereinigung

Bei rollenbasierter Verwaltung:

- Zur Ausführung dieses Tasks ist die Berechtigung **Richtlinieneinstellung – Virenschutz und HIPS** erforderlich.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Computer können automatisch bereinigt werden, wenn ein Virus oder ein anderes Objekt gefunden wird. Zu diesem Zweck ändern Sie die Einstellungen für die On-Access-Scans und geplanten Scans wie folgt:

Hinweis: Adware und andere potenziell unerwünschte Anwendungen (PUA) werden bei On-Access-Scans nicht bereinigt. Befolgen Sie in Zusammenhang mit Adware und PUA die Anweisungen im Abschnitt [Sofortiges Bereinigen von Computern](#) (Seite 58) beschrieben, oder aktivieren Sie die automatische Bereinigung von Adware/PUA bei geplanten Scans.

1. Prüfen Sie, welche Antivirus- und HIPS-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.
Mehr dazu erfahren Sie unter [Welche Richtlinien sind einer Gruppe zugewiesen?](#) (Seite 25).
2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Antivirus und HIPS**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.
Das Dialogfeld **Antivirus- und HIPS-Richtlinie** wird angezeigt.

3. Richten Sie die automatische Bereinigung für On-Access-Scans ein.

Klicken Sie im Fensterbereich **Antivirus- und HIPS-Konfiguration** auf die Schaltfläche **On-Access-Scans**. Klicken Sie im Dialogfeld **Einstellungen für On-Access-Scans** auf die Registerkarte **Bereinigung**. Wählen Sie die Optionen aus, wie nachfolgend erläutert.

Viren/Spyware

Wählen Sie **Objekte mit Virus/Spyware automatisch bereinigen**. Sie können außerdem festlegen, was mit den Objekten geschehen soll, falls die Bereinigung fehlschlägt:

- Nur Zugriff verweigern (Standard)
- Löschen
- Zugriff verweigern und in das Standardverzeichnis verschieben
- Zugriff verweigern und verschieben nach <angegebener UNC-Pfad>

Hinweis: Unter Windows 95 oder 98 werden die Einstellungen für die Vorgehensweise bei fehlgeschlagener Bereinigung nicht übernommen.

Wenn Sie **Zugriff verweigern und verschieben nach** wählen und einen Speicherort angeben, verschieben Mac OS X-Computer infizierte Objekte trotzdem in den Standard-Speicherort. Die gewählten Optionen im Bereich **Zugriff verweigern und in den Standardspeicherort verschieben** und **Zugriff verweigern und in Standardverzeichnis verschieben** werden auf Linux- oder UNIX-Computern ignoriert.

Verdächtige Dateien

Hinweis: Die Einstellungen zu verdächtigen Dateien werden nur ab Windows 2000 übernommen.

Sie können festlegen, was mit verdächtigen Dateien geschehen soll, wenn sie erkannt werden:

- Nur Zugriff verweigern (Standard)
- Löschen
- Zugriff verweigern und in das Standardverzeichnis verschieben
- Zugriff verweigern und verschieben nach <angegebener UNC-Pfad>

4. Richten Sie die automatische Bereinigung für geplante Scans ein.

Markieren Sie im Dialogfeld **Antivirus- und HIPS-Richtlinie** im Fensterbereich **Geplante Scans** den Scan 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**. Stellen Sie nun folgende Optionen ein:

Viren/Spyware

Wählen Sie **Objekte mit Virus/Spyware automatisch bereinigen**. Sie können außerdem festlegen, was mit den Objekten geschehen soll, falls die Bereinigung fehlschlägt:

- Nur Zugriff verweigern (Standard)
- Löschen
- Zugriff verweigern und in das Standardverzeichnis verschieben
- Zugriff verweigern und verschieben nach <angegebener UNC-Pfad>

Hinweis: Wenn Sie **Zugriff verweigern und verschieben nach** wählen und einen Speicherort angeben, verschieben Computer unter Windows 95 und 98 infizierte Objekte trotzdem in den Standard-Speicherort.

Adware und PUA

Sie können **Adware und PUA automatisch bereinigen** wählen.

Hinweis: Diese „Adware und PUA“-Einstellung ist nur für Windows 2000 und aufwärts relevant.

Verdächtige Dateien

Hinweis: Die Einstellungen zu verdächtigen Dateien werden nur ab Windows 2000 übernommen.

Sie können festlegen, was mit verdächtigen Dateien geschehen soll, wenn sie erkannt werden:

- Nur Zugriff verweigern (Standard)
- Löschen
- Zugriff verweigern und in das Standardverzeichnis verschieben
- Zugriff verweigern und verschieben nach <angegebener UNC-Pfad>

13 Ereignisanzeige

13.1 Allgemeine Informationen

Application Control-, Firewall-, Data Control-, Device Control-Ereignisse auf einem Endpoint (z.B. die Firewall hat eine Anwendung blockiert) werden an Enterprise Console 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 Data Control-Ereignisse, die in den vergangenen 7 Tagen von einem bestimmten Benutzer ausgelöst wurden.

Im Dashboard wird die Anzahl der Computer angezeigt, deren Ereignisanzahl in den vergangenen 7 Tagen einen festgelegten Höchstwert überschritten hat. Nähere Informationen zum Festlegen des Höchstwerts finden Sie im Abschnitt [Konfigurieren des Dashboards](#) (Seite 51).

Sie können einstellen, dass die von Ihnen ausgewählten Empfänger bei Ereignissen benachrichtigt werden. Weitere Informationen finden Sie im Abschnitt „Alerts“.

13.2 Anzeigen von Application Control-Ereignissen

So können Sie sich Application Control-Ereignisse anzeigen lassen:

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

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. 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.

Die Eingabe folgender Platzhalter ist erlaubt: ? für ein einzelnes Zeichen und * für eine Zeichenfolge.

4. Wenn Sie Ereignisse für einen bestimmten Anwendungstyp aufrufen möchten, wählen Sie im Dropdown-Menü **Anwendungstyp** den Anwendungstyp aus.

Standardmäßig werden in der Ereignisanzeige Ereignisse für alle Anwendungstypen angezeigt.

5. 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 66).

13.3 Anzeige von Data Control-Ereignissen

So können Sie sich Data Control-Ereignisse anzeigen lassen:

1. Klicken Sie im Menü **Ansicht** auf **Data Control-Ereignisse**.
Das Dialogfeld **Data 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. Wenn Sie Ereignisse für einen bestimmten Benutzer, Computer oder eine bestimmte Datei aufrufen möchten, geben Sie den entsprechenden Namen in das zugehörige Feld ein.
Wenn Sie keine spezifischen Angaben machen, werden Ereignisse für alle Benutzer, Computer und Dateien angezeigt.
Die Eingabe folgender Platzhalter ist erlaubt: ? für ein einzelnes Zeichen und * für eine Zeichenfolge.
4. Wenn Sie Ereignisse für eine bestimmte Regel aufrufen möchten, wählen Sie im Dropdown-Menü **Regelname** den Regelnamen aus.
Standardmäßig werden in der Ereignisanzeige Ereignisse für alle Regeln angezeigt.
5. Wenn Sie Ereignisse für einen bestimmten Dateityp aufrufen möchten, wählen Sie im Dropdown-Menü **Dateityp** den Dateityp aus.
Standardmäßig werden in der Ereignisanzeige Ereignisse für alle Dateitypen angezeigt.
6. Klicken Sie zur Anzeige einer Ereignisliste auf **Suche**.

Sie können die Liste mit Data Control-Ereignissen in eine Datei exportieren. Mehr dazu erfahren Sie unter [Exportieren der Ereignisliste in eine Datei](#) (Seite 66).

13.4 Anzeige von Device Control-Ereignissen

So können Sie sich Device Control-Ereignisse anzeigen lassen:

1. Klicken Sie im Menü **Ansicht** auf **Device Control-Ereignisse**.
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.
Die Eingabe folgender Platzhalter ist erlaubt: ? für ein einzelnes Zeichen und * für eine Zeichenfolge.
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 [Ausschließen eines Geräts von allen Richtlinien](#) (Seite 153).

Sie können die Liste von Device Control-Ereignissen in eine Datei exportieren. Mehr dazu erfahren Sie unter [Exportieren der Ereignisliste in eine Datei](#) (Seite 66).

13.5 Anzeige von Firewall-Ereignissen

Firewall-Ereignisse werden nur einmal von einem Computer an die Konsole gesendet. Identische Ereignisse von verschiedenen Computern werden in der **Firewall – Ereignisanzeige** gruppiert. In der Spalte **Anzahl** wird angezeigt, wie häufig ein Ereignis von diversen Endpoints gesendet wurde.

So werden Firewall-Ereignisse angezeigt:

1. Klicken Sie im Menü **Ansicht** auf **Firewall-Ereignisse**.
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. Wenn Sie Ereignisse eines bestimmten Typs aufrufen möchten, wählen Sie den gewünschten Typ im Dropdown-Menü **Ereignistyp** aus.
Standardmäßig werden in der Ereignisanzeige Ereignisse für alle Typen angezeigt.
4. Wenn Sie Ereignisse für eine bestimmte Datei aufrufen möchten, geben Sie in das Feld **Dateiname** den entsprechenden Namen ein.
Wenn Sie keine spezifischen Angaben machen, werden Ereignisse für alle Dateien angezeigt.
Die Eingabe folgender Platzhalter ist erlaubt: ? für ein einzelnes Zeichen und * für eine Zeichenfolge.
5. Klicken Sie zur Anzeige einer Ereignisliste auf **Suche**.

Im Dialogfeld **Firewall – Ereignisanzeige** können Sie anhand der Anweisungen im Abschnitt [Erstellen einer Firewall-Regel](#) (Seite 125) eine Firewall-Regel erstellen.

Sie können die Liste mit Firewall-Ereignissen in eine Datei exportieren. Mehr dazu erfahren Sie unter [Exportieren der Ereignisliste in eine Datei](#) (Seite 66).

13.6 Anzeige von Manipulationsschutz-Ereignissen

Es wird zwischen den folgenden Manipulationsschutz-Ereignissen unterschieden:

- Erfolgreiche Manipulationsschutz-Ereignisse (Anzeige des Namens des authentifizierten Benutzers sowie des Authentifizierungszeitpunkts).
- Nicht erfolgreiche Manipulationsschutz-Ereignisse (Anzeige des Zielprodukts/der Zielkomponente, des Manipulationszeitpunkts und der Daten des Benutzers, der den Manipulationsversuch unternommen hat).

So können Sie sich Manipulationsschutz-Ereignissen anzeigen lassen:

1. Klicken Sie im Menü **Ansicht** auf **Manipulationsschutz-Ereignisse**.

Das Dialogfeld **Manipulationsschutz – 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. Wenn Sie Ereignisse eines bestimmten Typs aufrufen möchten, wählen Sie den gewünschten Typ im Dropdown-Menü **Ereignistyp** aus.

Standardmäßig werden in der Ereignisanzeige Ereignisse für alle Typen 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.

Die Eingabe folgender Platzhalter ist erlaubt: ? für ein einzelnes Zeichen und * für eine Zeichenfolge.

5. Klicken Sie zur Anzeige einer Ereignisliste auf **Suche**.

Sie können die Ereignisliste in eine Datei exportieren. Mehr dazu erfahren Sie unter [Exportieren der Ereignisliste in eine Datei](#) (Seite 66).

13.7 Aufrufen gesperrter Websites

Sie können sich anzeigen lassen, welche Websites in letzter Zeit auf einem Endpoint gesperrt wurden.

So rufen Sie in letzter Zeit gesperrte Websites auf:

1. Doppelklicken Sie in der Ansicht **Endpoints** in der Computerliste auf den Computer, dessen gesperrte Websites angezeigt werden sollen.
2. Navigieren Sie im Dialogfeld **Computer-Details** zu **Letzte gesperrte Websites**.

Sie können auch einen Report erstellen, aus dem die Anzahl gesperrter Websites für einen bestimmten Benutzer hervorgeht. Weitere Informationen finden Sie unter [Konfigurieren des Reports „Ereignisse nach Benutzer“](#) (Seite 180).

13.8 Exportieren der Ereignisliste in eine Datei

Sie können Application Control-, Firewall-, Data Control- oder 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 62), [Anzeige von Data Control-Ereignissen](#) (Seite 63), [Anzeige von Device Control-Ereignissen](#) (Seite 63) und [Anzeige von Firewall-Ereignissen](#) (Seite 64).

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.

14 Scannen von Computern

14.1 Scan-Informationen

Standardmäßig erkennt Sophos Endpoint Security and Control bekannte und unbekannt Viren, Trojaner, Würmer und Spyware automatisch, wenn ein Benutzer versucht, auf Dateien zuzugreifen, in denen sie enthalten sind. Außerdem wird das Verhalten der Programme analysiert, die auf dem System laufen.

Ferner können Sie die folgenden Einstellungen in Sophos Endpoint Security and Control vornehmen:

- Scannen von Computern auf verdächtige Dateien. Mehr dazu erfahren Sie unter [Scannen auf verdächtige Dateien](#) (Seite 85).
- Scannen auf Adware und potenziell unerwünschte Anwendungen. Mehr dazu erfahren Sie unter [Scannen auf Adware und PUA](#) (Seite 89).
- Scannen von Computern zu festen Zeiten. Mehr dazu erfahren Sie unter [Scannen von Computern zu bestimmten Zeiten](#) (Seite 98).

Nähere Informationen zur Konfiguration der Scan-Funktionen finden Sie im Abschnitt „Konfigurieren der Anti-Virus- und HIPS-Richtlinie“.

In diesem Abschnitt wird beschrieben, wie eine **vollständige Systemüberprüfung** ausgewählter Computer sofort durchgeführt werden kann.

14.2 Sofort-Scans

Sie können einen oder mehrere Computer sofort scannen, ohne auf den nächsten geplanten Scan warten zu müssen.

Bei rollenbasierter Verwaltung müssen Sie zum Updaten von Computern über die Berechtigung **Korrektur – Updates und Scans** verfügen. Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Hinweis: Sofortige vollständige Systemüberprüfungen über die Konsole sind nur unter Windows 2000 oder höher und UNIX möglich.

So werden Computer sofort gescannt:

1. Wählen Sie den Computer in der Computer-Liste oder eine Gruppe im Fensterbereich **Gruppen**. Rechtsklicken Sie darauf und wählen Sie **Vollständige Systemüberprüfung**. Sie können aber auch im Menü **Maßnahmen** die Option **Vollständige Systemüberprüfung** wählen.
2. Wenn all Angaben im Dialogfeld **Vollständige Systemüberprüfung** richtig sind, klicken Sie auf **OK**, um die Überprüfung zu starten.

15 Updates

15.1 Updaten nicht aktueller Computer

Bei rollenbasierter Verwaltung müssen Sie zum Updaten von Computern über die Berechtigung **Korrektur – Updates und Scans** verfügen. Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Nach dem Einrichten der Update-Richtlinien und der Übernahme der Richtlinien auf Netzwerkcomputern, werden die Computer automatisch auf dem neuesten Stand gehalten. Sofern kein Problem mit der Update-Funktion vorliegt, müssen Sie Computer nicht manuell updaten.

Wenn in der Computerliste in der Ansicht **Endpoints** ein Uhersymbol neben einem Computer in der Spalte **Auf dem neuesten Stand** auf der Registerkarte **Status** angezeigt wird, befindet sich die Sicherheitssoftware des Computers nicht mehr auf dem aktuellen Stand. Aus dem Text geht hervor, seit wann sich der Computer nicht mehr auf dem neuesten Stand befindet.

Ein Computer kann aus einem von zwei Gründen nicht aktuell sein:

- Der Computer hat kein Update vom Server erhalten.
- Auf dem Server ist nicht die neueste Sophos Software verfügbar.

So können Sie das Problem bestimmen und die Computer updaten:

1. Wählen Sie in der Ansicht **Endpoints** die Gruppe mit den Computern aus, die sich nicht auf dem neuesten Stand befinden.
2. Klicken Sie in der Registerkarte **Status** auf die Spalte **Auf dem neuesten Stand**, um die Computer nach Aktualität zu sortieren.
3. Klicken Sie auf die Registerkarte **Update-Details** und sehen Sie in der Spalte **Primärserver** nach.

Dort wird das Verzeichnis angezeigt, von dem aus die Computer jeweils ihre Updates beziehen.

4. Sehen Sie sich jetzt die Computer an, die sich von einem bestimmten Verzeichnis aus aktualisieren.
 - *Wenn einige nicht aktuell sind, andere aber doch*, besteht das Problem auf einzelnen Computern. Rechtsklicken Sie darauf und klicken Sie auf die Option **Computer jetzt updaten**.
 - *Wenn alle Computer nicht aktuell sind*, könnte das Problem am Verzeichnis liegen. Klicken Sie im Menü **Ansicht** auf **Update Manager**. Rechtsklicken Sie auf den Update Manager, der das Verzeichnis auf dem neuesten Stand hält, von dem Sie vermuten, dass es nicht aktuell ist, und wählen Sie **Jetzt updaten**. Klicken Sie im Menü **Ansicht** auf **Endpoints**. Wählen Sie die Computer aus, die nicht mehr aktuell sind, rechtsklicken Sie darauf und klicken Sie auf **Computer jetzt updaten**.

Wenn Sie mehrere Update Manager besitzen, können Sie im Update-Hierarchie-Report nachsehen, welche Freigaben von den einzelnen Update Managern auf dem neuesten Stand gehalten werden. Zum Aufrufen des Update-Hierarchie-Reports klicken Sie im Menü

Extras auf Report-Verwaltung. Wählen Sie im Dialogfeld **Update-Richtlinie** die Option **Report Manager** und klicken Sie auf **Ausführen**. Sehen Sie sich den Report-Abschnitt „Von Update-Managern verwaltete Freigaben“ an.

16 Konfigurieren von Software-Abonnements

16.1 Software-Abonnements

Durch Software-Abonnements wird festgelegt, welche Endpoint-Softwareversionen für die jeweiligen Plattformen von Sophos heruntergeladen werden.

Der **Download-Assistent für Sicherheitssoftware** richtet ein Standardabonnement ein („Empfohlen“). Das Abonnement umfasst die empfohlenen Versionen der gewählten Software.

Wenn Sie nicht die empfohlene Version abonnieren möchten, befolgen Sie die Konfigurationsanweisungen unter [Abonnieren von Sicherheitssoftware](#) (Seite 71).

Wenn Sie den Assistenten nach der Installation von Enterprise Console nicht ausgeführt haben, finden Sie im Abschnitt [Ausführen des Download-Assistenten für Sicherheitssoftware](#) (Seite 72) nähere Informationen.

16.2 Update-Arten

Jede Hauptversion einer Softwarelösung (z.B. Sophos Endpoint Security and Control 9) für die jeweiligen Betriebssysteme (z.B. Windows 2000 und höher) umfasst mehrere Versionen. Durch Festlegen einer Update-Art können Sie die Softwareversion auswählen, die von Sophos heruntergeladen werden und auf den Endpoints installiert werden soll. Es stehen drei Software-Versionen kategorisierter Updates und drei Software-Versionen fester Updates zur Auswahl.

Kategorisierte Updates

Folgende Kategorien werden angeboten:

Kategorie	Beschreibung
Empfohlen	Die von Sophos für angemessen erachtete Version zum Bezug der aktuellen Produktversion. Sophos empfiehlt in der Regel die Installation der neuesten Version der Endpoint-Software auf Computern.
Vorherig	Die vor der aktuellen Version empfohlene Version.
Alt	Die älteste Softwareversion, für die Sophos Updates anbietet.

Hinweis: Möglicherweise werden künftig weitere Kategorien folgen.

Wenn Sie mit dem **Download-Assistent für Sicherheitssoftware** ein Abonnement einrichten, werden jeweils die empfohlenen Softwareversionen für Updates ausgewählt.

Wenn Sie eine bestimmte Version abonniert haben, etwa „empfohlen“ oder „vorherig“, lädt Enterprise Console stets die Version mit der entsprechenden Bezeichnung von Sophos herunter. Die Download-Versionen werden in der Regel jeden Monat geändert.

Feste Updates

Feste Versionen werden mit neuen Threat-Erkennungsdaten, jedoch nicht mit den monatlichen Software-Updates upgedatet.

Wenn Sie neue Versionen vor der Installation im Hauptnetzwerk testen möchten, empfiehlt sich, bis zum Abschluss der Tests feste Updates im Hauptnetzwerk einzusetzen.

In der Regel sind drei Versionen fester Updates für jedes Betriebssystem erhältlich (die Updates der vergangenen drei Monate). Ein festes Update kann etwa wie folgt aussehen: Sophos Endpoint Security and Control für Windows 2000 und höher, Version 9.4.3.

Feste Updates werden von Sophos heruntergeladen, bis sie eingestellt werden. Bei Einstellung eines festen Updates wird neben allen **Update Managern**, die diese Version herunterladen, ein Alert angezeigt. Wenn Sie E-Mail-Benachrichtigungen eingerichtet haben, wird der Administrator zudem per E-Mail darüber informiert.

Standardmäßig nimmt Enterprise Console bei Einstellung eines festen Updates das älteste verfügbare feste Update in das Abonnement auf.

Hinweis: Diese Option können Sie durch Deaktivieren des Kontrollkästchens **Nicht mehr unterstützte Abonnements einer bestimmten Version automatisch updaten** im Abonnement ändern. Wenn Sie nicht unterstützte Software ausführen, ist Ihr Computer vor neuen Threats nicht geschützt. Sophos rät daher zu umgehenden Updates auf eine unterstützte Version.

16.3 Abonnieren von Sicherheitssoftware

Bei rollenbasierter Verwaltung:

- Sie müssen über die Berechtigung **Richtlinieneinstellung – Updates** verfügen, um Änderungen an einem Software-Abonnement vornehmen zu können.
- Wenn ein Abonnement einer Update-Richtlinie angehört, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befindet, können Sie es nicht ändern.

Nähere Informationen zur rollenbasierten Verwaltung können Sie dem Abschnitt [Rollen und Teilverwaltungseinheiten](#) (Seite 13) entnehmen.

So können Sie Sicherheitssoftware abonnieren:

1. Klicken Sie im Menü **Ansicht** auf **Update Manager**.
2. Doppelklicken Sie im Fenster **Software-Abonnements** auf das zu ändernde Abonnement oder klicken Sie zum Erstellen eines neuen Abonnements auf **Hinzufügen**.
Das Dialogfenster **Software-Abonnements** wird angezeigt.
Wenn Sie eine Kopie eines vorhandenen Abonnements anlegen möchten, rechtsklicken Sie auf das Abonnement und wählen Sie **Abonnement duplizieren**. Geben Sie dem Abonnement einen neuen Namen und doppelklicken Sie darauf. Das Dialogfeld **Software-Abonnement** wird geöffnet.
3. Im Dialogfeld **Software-Abonnements** können Sie auf Wunsch den Namen des Abonnements ändern.

4. Wählen Sie die Betriebssysteme aus, für die Sie Software herunterladen möchten.

Wichtig: Wenn Sie Sophos Anti-Virus für NetWare herunterladen möchten, lesen Sie bitte auf der Sophos Website den Support-Artikel 59192 (<http://www.sophos.de/support/knowledgebase/article/59192.html>).

5. Für jede ausgewählte Plattform gilt: Klicken Sie neben der Plattform in das Feld **Version** und klicken Sie nochmal. Wählen Sie in der Dropdown-Liste die gewünschte Version aus, die Sie herunterladen möchten.

In der Regel bietet sich die Option „Empfohlen“ an, da so sichergestellt wird, dass Software automatisch auf dem neuesten Stand gehalten wird. Im Abschnitt [Update-Arten](#) (Seite 70) können Sie sich über weitere Update-Arten informieren.

Wichtig: Wenn Sie eine „feste Version“ (z.B. 9.1.2) ausgewählt haben, empfiehlt es sich, die Option **Nicht mehr unterstützte Abonnements einer bestimmten Version automatisch updaten** nicht zu deaktivieren. Wenn Sie nicht unterstützte Software nutzen, sind Ihre Computer vor neuen Threats nicht sicher.

Wenn Sie Sophos Sicherheitssoftware abonniert haben, können Sie Abonnement-Alerts einrichten. Nähere Informationen zu Abonnement-E-Mail-Alerts können Sie dem Abschnitt [Einrichten von Abonnement-Alerts](#) (Seite 163) entnehmen.

Konfigurieren Sie den Update Manager nach dem Erstellen des neuen Software-Abonnements, damit er wie unter [Anzeigen oder Ändern der Update Manager-Konfiguration](#) (Seite 73) erläutert verwaltet wird.

16.4 Ausführen des Download-Assistenten für Sicherheitssoftware

Bei rollenbasierter Verwaltung müssen Sie zum Ausführen des **Download-Assistenten für Sicherheitssoftware** über die Berechtigung **Richtlinieneinstellung – Updates** verfügen. Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Wenn Sie den **Download-Assistenten für Sicherheitssoftware** nach der Installation von Enterprise Console nicht ausgeführt haben, verfahren Sie wie folgt:

- Klicken Sie im Menü **Maßnahmen** auf **Ausführen des Download-Assistenten für Sicherheitssoftware**.

Der **Download-Assistent für Sicherheitssoftware** leitet Sie durch die Softwareauswahl und den Download.

16.5 Update-Richtlinien, die Software-Abonnements nutzen

So können Sie feststellen, welche Update-Richtlinien ein Software-Abonnement nutzen:

- Wählen Sie das Software-Abonnement aus, rechtsklicken Sie darauf und klicken Sie auf **Nutzungsstatistik**.

Im Dialogfeld **Software-Abonnement-Nutzung** werden die Update-Richtlinien aufgelistet, die das Abonnement nutzen.

17 Konfigurieren des Update Managers

17.1 Wozu dient ein Update Manager?

Mit einem Update Manager können Sie automatische Updates von Sophos Sicherheitssoftware über die Sophos Website konfigurieren. Der Update Manager wird mit Enterprise Console installiert und verwaltet.

Sie können mehrere Update Manager installieren. Wenn Ihr Unternehmensnetzwerk beispielsweise mehrere Standorte umfasst, empfiehlt sich, einen zusätzlichen Update Manager an einem Remote-Standort zu installieren. Nähere Informationen hierzu finden Sie unter [Hinzufügen eines weiteren Update Managers](#) (Seite 80).

17.2 Funktionsweise eines Update Managers

Nach der Konfiguration führt der Update Manager die folgenden Aufgaben aus:

- Er stellt in regelmäßigen Abständen eine Verbindung zu einem Datenverteilungs-Warehouse bei Sophos bzw. in Ihrem Netzwerk her.
- Er lädt Updates für Threat-Erkennungsdaten und für Sicherheitssoftware herunter, die der Administrator abonniert hat.
- Er legt die Software-Updates in installierbarer Form in einer oder mehreren Netzwerkgigabiten ab.

Die Computer laden Updates automatisch aus den Gigabiten herunter, sofern die installierte Software entsprechend konfiguriert wurde (z.B. durch Übertragen einer Update-Richtlinie).

17.3 Anzeigen oder Ändern der Update Manager-Konfiguration

Bei rollenbasierter Verwaltung müssen Sie zum Konfigurieren eines Update Managers über die Berechtigung **Richtlinieneinstellung – Updates** verfügen. Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

1. Wenn Sie sich in der Ansicht **Endpoints** befinden, klicken Sie in der Symbolleiste auf das **Update Manager**-Symbol. Die Ansicht **Update Manager** wird angezeigt.
2. Wählen Sie den Update Manager, dessen Konfiguration angezeigt oder geändert werden soll, in der Liste aus. Rechtsklicken Sie darauf und klicken Sie auf **Konfiguration**.

Hinweis: Sie können jedoch auch wie folgt verfahren: Rufen Sie das Menü **Maßnahmen** auf, richten Sie den Mauszeiger auf **Update Manager** und klicken Sie anschließend auf **Konfiguration**.

Das Dialogfenster **Update Manager konfigurieren** wird angezeigt.

3. Anweisungen zum Ändern der Konfigurationseinstellungen entnehmen Sie bitte den folgenden Abschnitten.

- [Auswahl einer Update-Quelle für einen Update Manager](#) (Seite 74).
- [Auswahl der Software zum Download](#) (Seite 75).
- [Festlegen des Download-Verzeichnisses](#) (Seite 76).
- [Erstellen/Ändern eines Update-Zeitplans](#) (Seite 77).
- [Konfigurieren des Update Manager-Protokolls](#) (Seite 78).
- [Konfigurieren der Selbst-Update-Funktion von Update Managern](#) (Seite 78).

Weitere Informationen zum Löschen von Update Manager-Alerts aus der Konsole finden Sie unter [Löschen von Update Manager-Alerts aus der Konsole](#) (Seite 57).

Wenn Sie den Update Manager konfiguriert haben, können Sie Ihre Update-Richtlinie konfigurieren und sie auf die Endpoints übertragen.

17.4 Auswahl einer Update-Quelle für einen Update Manager

Bei rollenbasierter Verwaltung müssen Sie zum Konfigurieren eines Update Managers über die Berechtigung **Richtlinieneinstellung – Updates** verfügen. Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Sie müssen eine Quelle auswählen, von der ein Update Manager Sicherheitssoftware und Updates herunterlädt, die im Netzwerk verteilt werden.

Sie können mehrere Quellen angeben. Bei der ersten Quelle handelt es sich um die Primärquelle. Wenn der Update Manager kein Update von der Hauptquelle beziehen kann, greift er auf die anderen Quellen in der Liste zu.

1. Wenn Sie sich in der Ansicht **Endpoints** befinden, klicken Sie in der Symbolleiste auf das **Update Manager**-Symbol. Die Ansicht **Update Manager** wird angezeigt.
2. Wählen Sie aus der Update Manager-Liste den Update-Manager aus, dem eine Quelle zugewiesen werden soll. Rechtsklicken Sie darauf und klicken Sie auf **Konfiguration**.
3. Klicken Sie im Fenster **Update Manager konfigurieren** auf der Registerkarte **Quellen** auf die Option **Hinzufügen**.
4. Geben Sie in das Dialogfeld **Quellenangaben** die Adresse der Quelle in das **Adress**-Feld ein. Es kann sich bei der Adresse um einen UNC- oder einen HTTP-Pfad handeln.

Wenn Sie Software und Updates direkt von Sophos herunterladen möchten, wählen Sie **Sophos**.

5. Geben Sie bei Bedarf den **Benutzernamen** und das **Kennwort** für den Zugriff auf die Update-Quelle in die entsprechenden Felder ein.
 - Wenn die Update-Quelle „Sophos“ lautet, geben Sie die Download-Zugangsdaten ein, die Sie von Sophos erhalten haben.

- Wenn es sich bei der Update-Quelle um die von einem Update Manager einer höheren Hierarchieebene erstellte Standard-Update-Quelle handelt, sind die Felder **Benutzername** und **Kennwort** bereits ausgefüllt.

Die Standard-Update-Freigabe ist eine UNC-Freigabe \\<ComputerName>\SophosUpdate. ComputerName steht dabei für den Namen des Computers, auf dem der Update Manager installiert wurde.

- Wenn Sie nicht auf einen Standard-Update-Quelle im Netzwerk zugreifen, geben Sie die Zugangsdaten des Kontos ein, das Lesezugriff auf die Freigabe besitzt. Falls der **Benutzername** auch eine Domäne erfordert, geben Sie ihn im Format Domäne\Benutzername ein.
6. Wenn Sie auf die Update-Quelle über einen Proxyserver zugreifen, wählen Sie die Option **Über Proxyserver verbinden**. Geben Sie anschließend die **Adresse** und den **Port** des Proxyservers an. Geben Sie die **Zugangsdaten** des Proxyservers ein. Falls der Benutzername auch eine Domäne erfordert, geben Sie ihn im Format Domäne\Benutzername ein. Klicken Sie auf **OK**.

Die neue Quelle wird in der Liste im Dialogfeld **Update Manager konfigurieren** angezeigt.

Wenn Sie bereits einen Update Manager auf einem anderen Computer installiert haben, erscheint die die Freigabe, von der der Update Manager Software und Updates bezieht, in der Adressenliste. Sie können die Freigabe als Quelle für den konfigurierten Update Manager auswählen. Anschließend können Sie die gewünschte Primäradresse mit Hilfe der Pfeilschaltflächen rechts neben der Liste ganz nach oben verschieben.

17.5 Auswahl der Software zum Download

Bei rollenbasierter Verwaltung müssen Sie zum Konfigurieren eines Update Managers über die Berechtigung **Richtlinieneinstellung – Updates** verfügen. Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Sie müssen die Abonnements auswählen, die der Update Manager auf dem neuesten Stand halten soll.

1. Wenn Sie sich in der Ansicht **Endpoints** befinden, klicken Sie in der Symbolleiste auf das **Update Manager**-Symbol. Die Ansicht **Update Manager** wird angezeigt.
2. Wählen Sie den gewünschten Update Manager aus der Liste aus. Rechtsklicken Sie darauf und klicken Sie auf **Konfiguration**.
3. Rufen Sie im Dialogfeld **Update Manager konfigurieren** die Registerkarte **Abonnements** auf und wählen Sie ein Abonnement aus der Liste mit den vorhandenen Abonnements aus.

Details zum Abonnement (z.B. vom Abonnement erfasste Software) können Sie per Klick auf **Details** aufrufen.

4. Klicken Sie zum Verschieben des gewählten Abonnements in die Liste „Abonniert für“ auf die Schaltfläche „Hinzufügen“.



Klicken Sie zum Verschieben aller Abonnements in die Liste „Abonniert für“ auf die Schaltfläche „Alle hinzufügen“.



17.6 Festlegen des Download-Verzeichnisses

Bei rollenbasierter Verwaltung müssen Sie zum Konfigurieren eines Update Managers über die Berechtigung **Richtlinieneinstellung – Updates** verfügen. Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Wenn Sie angegeben haben, welche Software heruntergeladen werden soll, können Sie nun das Download-Verzeichnis im Netzwerk angeben. Standardmäßig wird die Software in einer UNC-Freigabe \\<Computername>\SophosUpdate abgelegt. Dabei ist „Computername“ der Name des Computers, auf dem der Update Manager installiert ist.

Heruntergeladene Software kann auf weitere Freigaben im Netzwerk verteilt werden. Nehmen Sie hierzu eine vorhandene Netzwerkfreigabe in die Liste der verfügbaren Freigaben auf und verschieben Sie sie von dort anhand der folgenden Anweisungen in die Liste der Update-Freigaben. Stellen Sie sicher, dass das **SophosUpdateMgr**-Konto über Lesezugriff auf die Freigaben verfügt.

Im Abschnitt [Unterstützte Netzwerkfreigaben](#) (Seite 77) können Sie nachlesen, welche Systeme unterstützt werden.

So legen Sie das Download-Verzeichnis fest:

1. Wenn Sie sich in der Ansicht **Endpoints** befinden, klicken Sie in der Symbolleiste auf das **Update Manager**-Symbol. Die Ansicht **Update Manager** wird angezeigt.
2. Wählen Sie den gewünschten Update Manager aus der Liste aus. Rechtsklicken Sie darauf und klicken Sie auf **Konfiguration**.
3. Rufen Sie im Dialogfeld **Update Manager konfigurieren** die Registerkarte **Verteilung** auf und wählen Sie ein Software-Abonnement aus der Liste aus.
4. Wählen Sie eine Freigabe aus der Liste der verfügbaren Freigaben aus und verschieben Sie sie durch Klicken auf die Schaltfläche „Hinzufügen“ in die Liste „Update auf“.

Die Standardfreigabe \\<Computername>\SophosUpdate befindet sich immer in der Liste „Update auf“. Die Freigabe kann nicht gelöscht werden.

Die Liste der verfügbaren Freigaben umfasst alle Freigaben, die Enterprise Console bekannt sind und nicht bereits von einem anderen Update Manager genutzt werden.

Über die Schaltfläche „Hinzufügen“ (>) bzw. „Entfernen“ (<) können Sie Freigaben in die Liste aufnehmen oder aus der Liste entfernen.

5. Wenn Sie eine Beschreibung zu einer Freigabe oder Zugangsdaten zum Schreiben in die Freigabe angeben möchten, wählen Sie die Freigabe aus und klicken Sie auf **Konfigurieren**. Geben Sie im Dialogfeld **Freigaben-Manager** die Beschreibung und die Zugangsdaten ein. Wenn Sie die gleichen Zugangsdaten für mehrere Freigaben eingeben möchten, wählen Sie die Freigaben in der Liste **Update auf** aus und klicken Sie auf **Konfigurieren**. Geben Sie in das Dialogfeld **Mehrere Freigaben konfigurieren** die Zugangsdaten zum Schreiben auf die Freigaben ein.

17.7 Unterstützte Netzwerkfreigaben

Netzwerkfreigaben der folgenden Betriebssysteme werden unterstützt:

- Freigaben in Windows NT und höher.
- Auf Linux-Servern gehostete Samba-Freigaben, z.B. SUSE Linux Enterprise 10 (SLES 10).
- Auf Netware 5.1 SP3- und Netware 6.5 SP3- bis SP7-Kerneln gehostete Samba-Freigaben.
- Auf Mac OSX 10.2 und höher gehostete Samba-Freigaben.
- Auf Unix gehostete Samba-Freigaben.
- Novell Storage Services (NSS)-Freigaben mit NDS-Authentifizierung, gehostet auf Novell Open Enterprise Server 1 und 2, Linux-Kernel.
- Netware File System (NFS)-Freigaben mit NDS-Authentifizierung, gehostet auf Netware 5.1 SP3 und Netware 6.5 SP3 bis SP7, Netware-Kernel.
- NetApp Filer.
- Auf Novell Open Enterprise Server 1 und 2 gehostete Samba-Freigaben.
- Novell Storage Services (NSS)-Freigaben, mit NDS-Authentifizierung, gehostet auf Netware 5.1 SP3 und Netware 6.5 SP3 bis SP7, Netware-Kernel.

17.8 Erstellen/Ändern eines Update-Zeitplans

Bei rollenbasierter Verwaltung müssen Sie zum Konfigurieren eines Update Managers über die Berechtigung **Richtlinieneinstellung – Updates** verfügen. Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Standardmäßig sucht ein Update Manager alle 10 Minuten nach Updates für Threat-Erkennungsdaten. Sie können das Update-Intervall ändern. Der Mindestwert beträgt 5 Minuten. Der Höchstwert beträgt 1440 Minuten (24 Stunden). Sophos empfiehlt ein Update-Intervall von 10 Minuten für Threat-Erkennungsdaten, um sicherzustellen, dass Sie umgehend vor neu erkannten Threats geschützt sind.

Standardmäßig sucht ein Update Manager alle 60 Minuten nach Software-Updates für Threat-Erkennungsdaten. Sie können das Update-Intervall ändern. Der Mindestwert beträgt 10 Minuten. Der Höchstwert beträgt 1440 Minuten (24 Stunden).

Als Update-Intervall ist etwa „stündlich an allen Tagen“ denkbar. Sie können jedoch auch komplexere Zeitpläne erstellen und etwa unterschiedliche Update-Zeiträume für unterschiedliche Tage festlegen.

Hinweis: Sie können unterschiedliche Zeitpläne für alle Tagen festlegen. Jedem Wochentag kann jeweils nur ein Zeitplan zugeordnet werden.

1. Wenn Sie sich in der Ansicht **Endpoints** befinden, klicken Sie in der Symbolleiste auf das **Update Manager**-Symbol. Die Ansicht **Update Manager** wird angezeigt.
2. Wählen Sie aus der Update Manager-Liste den Update-Manager aus, für den ein Zeitplan erstellt werden soll. Rechtsklicken Sie darauf und klicken Sie auf **Konfiguration**.
3. Rufen Sie im Dialogfeld **Update Manager konfigurieren** die Registerkarte **Zeitplan** auf und legen Sie ein Intervall für Threat-Detection-Daten fest.
4. Geben Sie ein Intervall für Software-Updates ein.
 - Wenn Sie ein Update-Intervall für alle Stunden festlegen möchten, wählen Sie die Option **Auf Updates prüfen alle n Minuten** und geben Sie ein Intervall in Minuten an.
 - Wenn Sie einen komplexeren Zeitplan wünschen oder den einzelnen Wochentagen unterschiedliche Zeitpläne zuweisen möchten, wählen Sie die Option **Geplante Updates einrichten und verwalten** aus und klicken Sie anschließend auf **Hinzufügen**.

Geben Sie in das Dialogfeld **Update-Zeitplan** einen Namen für den Zeitplan ein und wählen Sie die Wochentage und Update-Intervalle aus.

17.9 Konfigurieren des Update Manager-Protokolls

Bei rollenbasierter Verwaltung müssen Sie zum Konfigurieren eines Update Managers über die Berechtigung **Richtlinieneinstellung – Updates** verfügen. Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

1. Wenn Sie sich in der Ansicht **Endpoints** befinden, klicken Sie in der Symbolleiste auf das **Update Manager**-Symbol. Die Ansicht **Update Manager** wird angezeigt.
2. Wählen Sie aus der Update Manager-Liste den Update-Manager aus, für den ein Protokoll erstellt werden soll. Rechtsklicken Sie darauf und klicken Sie auf **Konfiguration**.
3. Geben Sie im Dialogfeld **Update Manager konfigurieren** auf der Registerkarte **Protokolle** an, wie lange das Protokoll gespeichert werden soll, und wählen Sie die Maximalgröße des Protokolls aus.

17.10 Konfigurieren der Selbst-Update-Funktion von Update Managern

Bei rollenbasierter Verwaltung müssen Sie zum Konfigurieren eines Update Managers über die Berechtigung **Richtlinieneinstellung – Updates** verfügen. Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

1. Wenn Sie sich in der Ansicht **Endpoints** befinden, klicken Sie in der Symbolleiste auf das **Update Manager**-Symbol. Die Ansicht **Update Manager** wird angezeigt.
2. Wählen Sie aus der Update Manager-Liste den Update-Manager aus, dessen Updates konfiguriert werden sollen. Rechtsklicken Sie darauf und klicken Sie auf **Konfiguration**.

3. Wählen Sie im Dialogfeld **Update Manager konfigurieren** auf der Registerkarte **Erweitert** die gewünschte Update Manager-Version aus.
Wenn Sie beispielsweise die Option „empfohlen“ auswählen, wird der Update Manager stets an die Version mit der entsprechenden Bezeichnung angepasst. Die Version des Update Managers ändert sich dabei.

17.11 Sofort-Update-Suche

Bei rollenbasierter Verwaltung müssen Sie hierzu über die Berechtigung **Korrektur – Updates und Scans** verfügen. Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Nach der Konfiguration sucht der Update Manager nach vorhandenen Updates und lädt sie in Einklang mit dem festgelegten Zeitplan von der Update-Quelle in die automatisch verwalteten Update-Freigaben herunter. Wenn der Update Manager sofort nach Threat-Detection-Daten-Updates, Software-Updates für Endpoints sowie Software-Updates für den Update Manager selbst suchen soll, verfahren Sie wie folgt:

1. Wenn Sie sich in der Ansicht **Endpoints** befinden, klicken Sie in der Symbolleiste auf das **Update Manager**-Symbol. Die Ansicht **Update Manager** wird angezeigt.
2. Wählen Sie aus der Update Manager-Liste den Update-Manager aus, der upgedatet werden soll. Rechtsklicken Sie darauf und wählen Sie **Jetzt updaten**.

17.12 Übersicht über Update Manager

1. Wenn Sie sich in der Ansicht **Endpoints** befinden, klicken Sie in der Symbolleiste auf das **Update Manager**-Symbol. Die Ansicht **Update Manager** wird angezeigt.
2. Suchen Sie in der Update Manager-Liste in den Spalten **Alerts** und **Fehler** nach möglichen Problemen.
3. Wenn neben einem Update Manager ein Alert oder Fehler angezeigt wird, rechtsklicken Sie auf den Update Manager und klicken Sie auf die Option **Update Manager-Details**.

Im Dialogfeld **Computer-Details** werden der Zeitpunkt der letzten Software- und Threat-Detection-Daten-Updates, der Status der vom Update Manager verwalteten Abonnements und der Status des Update Managers angezeigt.

4. Nähere Informationen zum Status eines Update Managers und zur Fehlersuche finden Sie in der Spalte **Beschreibung**.

Hinweis: Wenn Update Manager vorübergehend keine Updates beziehen können, werden im Dashboard der Update Manager keine Fehler oder Alerts angezeigt. Fehler oder Alerts werden nur dann angezeigt, wenn die Zeit seit dem letzten Update die in [Erstellen/Ändern eines Update-Zeitplans](#) (Seite 77) festgelegten Warn- oder kritischen Stufen überschritten hat.

17.13 Übernahme der Konfigurationseinstellungen

Bei rollenbasierter Verwaltung müssen Sie hierzu über die Berechtigung **Korrektur – Updates und Scans** verfügen. Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

1. Wenn Sie sich in der Ansicht **Endpoints** befinden, klicken Sie in der Symbolleiste auf das **Update Manager**-Symbol. Die Ansicht **Update Manager** wird angezeigt.
2. Wählen Sie den Update Manager aus der Liste aus, für den die Einstellungen übernommen werden sollen. Rechtsklicken Sie auf die Auswahl und wählen Sie **Konformität mit Konfiguration**.

17.14 Hinzufügen eines weiteren Update Managers

Sophos Update Manager (SUM) wird immer auf dem Computer installiert, auf dem sich auch Enterprise Console befindet. Wenn Sie sich bei der Installation für das **Benutzerdefinierte Setup** entschieden haben, befindet sich auf diesem Computer auch der Management-Server.

Sie können einen oder mehrere Update Manager in Ihr Netzwerk aufnehmen. So wird der installierte Update Manager entlastet und Updates werden effektiver installiert. Sie können zusätzliche Update Manager auf einem Computer installieren, auf dem sich noch kein Update Manager befindet.

Wichtig: Entfernen Sie nicht den Update Manager, der sich auf dem selben Computer wie der Management-Server von Enterprise Console befindet. Enterprise Console kann das Netzwerk nicht vollständig schützen, bis für den Update Manager eine Update-Quelle eingerichtet wurde. Enterprise Console empfängt dann die erforderlichen Updates (Informationen zu den empfohlenen Sicherheitssoftware-Versionen, neue und aktualisierte Content Control Lists für Data Control oder die aktualisierte Liste überwachter Geräte und Anwendungen).

Öffnen Sie auf dem Computer, auf dem ein weiterer Update Manager installiert werden soll, Port 80, damit der zusätzliche Update Manager Sicherheitssoftware von Sophos oder einem anderen Update Manager über HTTP herunterladen kann. Öffnen Sie die Ports 137, 138, 139 und 445 auf dem Computer, damit der Update Manager Sicherheitssoftware von einem anderen Update Manager über einen UNC-Pfad herunterladen kann.

Wenn die Windows-Version des Computers über integrierte Netzwerkerkennung verfügt, diese Funktion jedoch deaktiviert ist, aktivieren Sie sie und starten Sie den Computer neu.

Wenn der Computer unter Windows Server 2008 betrieben wird, deaktivieren Sie die Benutzerkontensteuerung und starten Sie den Computer neu. Nach der Installation des Update Managers und der Anmeldung für die Sophos Updates können Sie die Benutzerkontensteuerung wieder aktivieren.

Wenn der Computer unter Windows 2000 betrieben wird, muss er nach der Installation neu gestartet werden.

Wenn sich der Computer in einer Domäne befindet, melden Sie sich als Domänenadministrator an.

Wenn sich der Computer in einer Arbeitsgruppe befindet, melden Sie sich als lokaler Administrator an.

Der Update Manager-Installer befindet sich in der Freigabe (\\Servername\SUMInstallSet) auf dem Computer, auf dem der Management-Server von Enterprise Console installiert ist. Sie können sich das Verzeichnis, in dem sich der Installer befindet, anzeigen lassen: Rufen Sie das Menü **Ansicht** auf und klicken Sie auf **Sophos Update Manager-Verzeichnis**.

Sie können den Sophos Update Manager über die Remotedesktop-Funktion von Windows installieren.

So können Sie weitere Update Manager installieren:

1. Führen Sie den Sophos Update Manager-Installer **Setup.exe** aus.
Ein Installations-Assistent öffnet sich.
 2. Klicken Sie im Startbildschirm des Assistenten auf **Weiter**.
 3. Lesen Sie die **Lizenzvereinbarung**. Wenn Sie mit den Bedingungen einverstanden sind, klicken Sie auf **Ich stimme den Bedingungen des Lizenzvertrags zu**. Klicken Sie auf **Weiter**.
 4. Übernehmen Sie den Standardzielordner auf der Seite **Zielordner** oder klicken Sie auf **Ändern** und geben Sie einen neuen Zielordner an. Klicken Sie auf **Weiter**.
 5. Wählen Sie auf der Seite **Sophos Update Manager-Konto** ein Konto aus, über das Endpoints auf die vom Update Manager erstellte Standard-Update zugreifen können. Die Standard-Update-Freigabe lautet \\<ComputerName>\SophosUpdate. ComputerName steht dabei für den Namen des Computers, auf dem der Update Manager installiert wurde. Das Konto muss Lesezugriff auf die Freigabe haben. Administratorrechte sind jedoch nicht erforderlich.
Sie können den Standardbenutzer oder einen vorhandenen Benutzer auswählen oder einen neuen Benutzer erstellen.
Standardmäßig weist der Installer dem **SophosUpdateMgr**-Konto Lesezugriff auf die Update-Freigabe, jedoch keine interaktiven Anmelderechte zu.
Wenn Sie später weitere Update-Freigaben hinzufügen möchten, wählen Sie ein vorhandenes Konto oder erstellen Sie ein neues Konto, das mit Lesezugriffsrechten an den Freigaben ausgestattet ist. Stellen Sie ansonsten sicher, dass das **SophosUpdateMgr**-Konto über Lesezugriff auf die Freigaben verfügt.
 6. Geben Sie auf der Seite **Kontodetails zu Sophos Update Manager** in Abhängigkeit von der auf der vorherigen Seite gewählten Option das Kennwort des Standardbenutzers oder die Kontodaten des neuen Benutzers ein oder wählen Sie ein vorhandenes Konto aus.
Das Kennwort des Kontos muss Ihrer Kennwortrichtlinie entsprechen.
 7. Klicken Sie im Dialogfeld **Das Programm kann jetzt installiert werden** auf die Option **Installieren**.
 8. Klicken Sie nach Abschluss der Installation auf **Fertig stellen**.
- Der Computer, auf dem Sophos Update Manager installiert wurde, wird nun in Enterprise Console in der Ansicht **Update Manager** angezeigt. (Klicken Sie im Menü **Ansicht** auf **Update Manager**).
- Wählen Sie den Update Manager zur Konfiguration aus, rechtsklicken Sie darauf und klicken Sie anschließend auf **Konfiguration**.

17.15 Freigeben von Sicherheitssoftware in einem Webserver

Bisweilen empfiehlt sich, Sophos Sicherheitssoftware in einem Webserver freizugeben, damit Computer über HTTP darauf zugreifen können. Bei der Installation von Sophos Anti-Virus für UNIX, Version 4, *muss* dieser Schritt durchgeführt werden, kann jedoch auf Wunsch auch erst nach dem Download von Sophos Anti-Virus für UNIX, Version 4, erfolgen.

So geben Sie Sicherheitssoftware in einem Webserver frei:

1. Den Pfad zur Freigabe, in die die Sicherheitssoftware heruntergeladen wurde („Bootstrap-Verzeichnis“), können Sie wie folgt ermitteln:
 - a) Klicken Sie in Enterprise Console im Menü **Ansicht** auf **Bootstrap-Verzeichnisse**.
Im Dialogfeld **Bootstrap-Verzeichnisse** werden in der Spalte **Verzeichnis** die Bootstrap-Verzeichnisse für alle Plattformen angezeigt.
 - b) Notieren Sie sich den Pfad bis ausschließlich des Ordners des zentralen Installationsverzeichnisses. Beispiel:
`\\server name\SophosUpdate`
2. Stellen Sie das Bootstrap-Verzeichnis, einschließlich der Unterordner, auf dem Webserver bereit.
3. Legen Sie Benutzernamen und Kennwörter zum Schutz vor unerlaubtem Zugriff auf den Ordner im Webserver fest.

Hinweis: Anweisungen zur Freigabe von Ordnern im Internet und zum Einrichten von Zugangsdaten entnehmen Sie bitte dem Begleitmaterial des Webservers. Wenden Sie sich bei weiteren Fragen bitte an Ihren Webserver-Betreiber.

18 Konfigurieren der Antivirus- und HIPS-Richtlinie

18.1 Die Antivirus- und HIPS-Richtlinie

Anti-Virus- und HIPS-Richtlinien dienen der Erkennung und Beseitigung von Viren, Trojanern, Würmern, Spyware sowie Adware und anderen potenziell unerwünschten Anwendungen. Zudem können Sie mit der Richtlinie nach verdächtigem Verhalten, verdächtigen Dateien und Rootkits suchen. Sie können den Computergruppen jeweils unterschiedliche Einstellungen zuweisen.

Standardmäßig erkennt Sophos Endpoint Security and Control bekannte und unbekannte Viren, Trojaner, Würmer und Spyware automatisch, wenn ein Benutzer versucht, auf Dateien zuzugreifen, in denen sie enthalten sind. Außerdem wird das Verhalten der Programme analysiert, die auf dem System laufen.

Ferner können Sie die folgenden Einstellungen in Sophos Endpoint Security and Control vornehmen:

- [Scannen auf verdächtige Dateien](#) (Seite 85)
- [Scannen auf Adware und PUA](#) (Seite 89)
- [Scannen von Computern zu bestimmten Zeiten](#) (Seite 98)

Computer können außerdem automatisch bereinigt werden, wenn ein Virus oder eine andere Bereinigung gefunden wird. Ändern Sie hierzu die Einstellungen von On-Access-Scans anhand der Anweisungen im Abschnitt [Einrichten der automatischen Bereinigung](#) (Seite 59).

Hinweis: Bei rollenbasierter Verwaltung:

- Zum Bearbeiten der Antivirus- und HIPS-Richtlinie müssen Sie über die Berechtigung **Richtlinieneinstellung – Antivirus und HIPS** verfügen.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Nähere Informationen zur rollenbasierten Verwaltung können Sie dem Abschnitt [Rollen und Teilverwaltungseinheiten](#) (Seite 13) entnehmen.

Hinweis: On-Access-Scans auf UNIX-Computern oder geplante Scans auf Macintosh Computern sind in Enterprise Console 4.5 nicht möglich. Wählen Sie eine andere Scan-Variante aus. Weitere Informationen zu Scan-Optionen können Sie dem *Benutzerhandbuch* zu *Sophos Anti-Virus für UNIX* bzw. der *Konfigurationsanleitung* zu *Sophos Anti-Virus für Mac OS X* entnehmen.

18.2 Scannen auf Viren, Trojaner, Würmer und Spyware

Standardmäßig erkennt Sophos Endpoint Security and Control bekannte und unbekannte Viren, Trojaner, Würmer und Spyware automatisch, wenn ein Benutzer versucht, auf Dateien zuzugreifen, in denen sie enthalten sind.

18.3 Erkennung verdächtigen Verhaltens und verdächtiger Dateien (HIPS)

18.3.1 Was ist HIPS?

Host Intrusion Prevention System (HIPS) schützt Computer vor verdächtigen Dateien, unbekanntem Viren und verdächtigem Verhalten. HIPS umfasst die beiden folgenden Methoden: Erkennung verdächtigen Verhaltens und Erkennung verdächtiger Dateien.

Hinweis: HIPS ist nur in Sophos Endpoint Security and Control für Windows 2000 integriert.

Erkennung verdächtigen Verhaltens

Die Erkennung verdächtigen Verhaltens ist die dynamische Analyse aller Programme, die auf einem Computer laufen, um potenziell schädliche Aktivitäten zu erkennen und zu sperren. Zu verdächtigem Verhalten zählen beispielsweise Änderungen an der Registrierung, die das automatische Ausführen eines Virus zulassen, wenn der Computer neu gestartet wird.

Die Erkennung verdächtigen Verhaltens umfasst auch die „Pufferüberlauf-Erkennung“, eine dynamische Verhaltensanalyse aller ausgeführten Programme zur Erkennung von Pufferüberlauf-Angriffen.

Hinweis: Die „Pufferüberlauf-Erkennung“ steht unter Windows Vista, Windows 2008, Windows 7 und 64-Bit-Versionen von Windows nicht zur Verfügung. Diese Betriebssysteme werden durch die DEP (Data Execution Prevention)-Funktion von Microsoft vor Pufferüberläufen geschützt.

Nähere Informationen zur Konfiguration der Erkennung verdächtigen Verhaltens finden Sie unter [Erkennen und Sperren verdächtigen Verhaltens](#) (Seite 84).

Erkennung verdächtiger Dateien

Sophos Endpoint Security and Control kann nach verdächtigen Dateien suchen. Diese enthalten bestimmte Merkmale, die für Malware typisch sind, aber nicht ausreichen, um die Datei als neue Malware zu identifizieren.

Nähere Informationen zur Konfiguration der Erkennung verdächtiger Dateien finden Sie unter [Scannen auf verdächtige Dateien](#) (Seite 85).

18.3.2 Erkennen und Sperren verdächtigen Verhaltens

Bei rollenbasierter Verwaltung:

- Zur Ausführung dieses Tasks ist die Berechtigung **Richtlinieneinstellung – Virenschutz und HIPS** erforderlich.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Standardmäßig führt Sophos Endpoint Security and Control zwar eine Verhaltensanalyse der Programme durch, die auf dem System ausgeführt werden, sperrt Programme mit verdächtigem Verhalten jedoch nicht.

Es empfiehlt sich, Sophos Endpoint Security and Control vor dem Aktivieren des automatischen Blockierens verdächtiger Dateien eine Weile im Alert-Modus zu betreiben und die gewünschten Programme zuzulassen. Wenn verdächtiges Verhalten oder Pufferüberlauf erkannt wird, können Sie verdächtige Objekte entweder entfernen oder zulassen. Nähere Informationen finden Sie unter [Sofortiges Bereinigen von Computern](#) (Seite 58) und [Zulassen verdächtiger Objekte](#) (Seite 86). Blockieren Sie verdächtiges Verhalten, nachdem Sie die gewünschten Programme zugelassen haben.

1. Prüfen Sie, welche Antivirus- und HIPS-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.

Mehr zu diesem Thema erfahren Sie unter [Welche Richtlinien sind einer Gruppe zugewiesen?](#) (Seite 25).

2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Antivirus und HIPS**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.
3. Klicken Sie im Dialogfeld **Antivirus- und HIPS-Richtlinie** auf die Schaltfläche **Verdächtiges Verhalten (HIPS)**.

Das Fenster **Verdächtiges Verhalten** wird angezeigt. Standardmäßig sind alle Optionen aktiviert (**Erkennung verdächtigen Verhaltens**, **Erkennung von Pufferüberläufen** und **Nur Alerts ausgeben**) aktiviert.

4. Aktivieren Sie die Option **Nur Alerts ausgeben**.

18.3.3 Scannen auf verdächtige Dateien

Bei rollenbasierter Verwaltung:

- Zur Ausführung dieses Tasks ist die Berechtigung **Richtlinieneinstellung – Virenschutz und HIPS** erforderlich.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Bei einer *verdächtigen Datei* handelt es sich um eine Datei, die bestimmte, für Malware typische Merkmale aufweist, die jedoch nicht ausreichen, um die Datei als neue Malware zu identifizieren (z.B. eine Datei, die dynamischen Dekomprimierungscode enthält, der häufig von Malware verwendet wird).

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

1. Prüfen Sie, welche Antivirus- und HIPS-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.

Mehr zu diesem Thema erfahren Sie unter [Welche Richtlinien sind einer Gruppe zugewiesen?](#) (Seite 25).

2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Antivirus und HIPS**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.
3. Stellen Sie die Optionen im Dialogfeld **Antivirus- und HIPS-Richtlinie** folgendermaßen ein:

■ **On-Access-Scans**

Stellen Sie zur Konfiguration von On-Access-Scans sicher, dass im Bereich **Antivirus- und HIPS-Konfiguration** das Kontrollkästchen **On-Access-Scans aktivieren** aktiviert wurde. Klicken Sie neben dem Kontrollkästchen auf die Schaltfläche **Konfigurieren**.

Wählen Sie auf der Registerkarte **Scans** im Bereich **Scanoptionen** das Kontrollkästchen **Verdächtige Dateien (HIPS) einbeziehen**. Klicken Sie auf **OK**.

■ **Geplante Scans**

Klicken Sie zum Konfigurieren von geplanten Scans im Bereich **Geplante Scans** auf **Hinzufügen** (oder wählen Sie einen bestehenden Scan und klicken Sie auf **Ändern**).

Geben Sie im Dialogfeld **Einstellungen für geplante Scans** Ihre Einstellungen ein und klicken Sie auf **Konfigurieren**.

Aktivieren Sie im Dialogfeld **Scan- und Bereinigungs-Einstellungen** auf der Registerkarte **Scans** im Bereich **Scanoptionen** das Kontrollkästchen **Verdächtige Dateien (HIPS) einbeziehen**. Klicken Sie auf **OK**.

Wenn eine verdächtige Datei erkannt wird, können Sie die Datei entweder entfernen oder zulassen. Nähere Informationen finden Sie unter [Sofortiges Bereinigen von Computern](#) (Seite 58) und [Zulassen verdächtiger Objekte](#) (Seite 86).

18.3.4 Zulassen verdächtiger Objekte

Bei rollenbasierter Verwaltung:

- Zur Ausführung dieses Tasks ist die Berechtigung **Richtlinieneinstellung – Virenschutz und HIPS** erforderlich.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Wenn Sie eine oder mehrere HIPS-Optionen aktiviert haben (z.B. Erkennung verdächtigen Verhaltens, Erkennung von Pufferüberläufen oder Erkennung verdächtiger Dateien), jedoch einige der Objekte verwenden möchten, können Sie sie folgendermaßen zulassen:

1. Prüfen Sie, welche Antivirus- und HIPS-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.
Mehr dazu erfahren Sie unter [Welche Richtlinien sind einer Gruppe zugewiesen?](#) (Seite 25).
2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Antivirus und HIPS**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.
3. Klicken Sie im Dialogfeld **Antivirus- und HIPS-Richtlinie** auf die Schaltfläche **Autorisierungen**.

4. Klicken Sie im Dialogfeld **Authorization Manager** auf die Registerkarte des Verhaltenstyps, der erkannt wurde, z.B. Pufferüberlauf.
 - Wenn Sie ein erkanntes Programm zulassen möchten, suchen Sie es in der Liste **Bekannt** und verschieben Sie es von dort in die Liste **Zugelassen**.
 - Wenn Sie Objekte zulassen möchten, die Sophos Endpoint Security and Control *nicht* als verdächtig eingestuft, klicken Sie auf die Option **Neuer Eintrag**. Suchen Sie nach dem Objekt und nehmen Sie es in die Liste **Zugelassen** auf.

Wenn Sie ein Objekt aus der Liste entfernen möchten, wählen Sie das Objekt und klicken Sie auf **Eintrag löschen**. Wenn Sie das Objekt zugelassen haben, wird es wieder blockiert, wenn Sie es aus der Liste entfernen. Verwenden Sie diese Option also nur, wenn Sie sicher sind, dass das Objekt nicht zugelassen werden muss. Diese Option löscht das Objekt nicht von der Festplatte.

18.4 Sophos Live-Schutz

18.4.1 Allgemeine Informationen

Dank Sophos Live-Schutz lässt sich über ein "In-the-Cloud"-Verfahren sofort feststellen, ob eine Datei eine Bedrohung darstellt. Bei Bedarf werden umgehend die in der Schutzkonfiguration der Antivirus- und HIPS-Richtlinie festgelegten Maßnahmen ergriffen.

Die Malware-Erkennung wird durch den Live-Schutz erheblich verbessert, und es kommt nicht zu unerwünschten Erkennungen. Das Verfahren basiert auf einem Sofortabgleich mit den aktuellen Malwaredateien. Wenn neue Malware erkannt wird, kann Sophos binnen Sekunden Updates bereitstellen.

Folgende Optionen müssen zur Nutzung des Live-Schutzes aktiviert sein:

■ Live-Schutz aktivieren

Wenn eine Datei von einem Antiviren-Scan auf einem Endpoint als verdächtig eingestuft wurde, anhand der Threatkennungsdateien (IDEs) auf dem Computer jedoch nicht festgestellt kann, ob die Datei virenfrei ist, werden bestimmte Daten (z.B. die Prüfsumme der Datei) zur weiteren Analyse an Sophos übermittelt. Bei der "In-the-Cloud"-Prüfung wird durch Abgleich mit der Datenbank der SophosLabs festgestellt, ob es sich um eine verdächtige Datei handelt. Die Datei wird als virenfrei oder von Malware betroffen eingestuft. Das Ergebnis der Prüfung wird an den Computer übertragen, und der Status der Datei wird automatisch aktualisiert.

■ Dateisamples automatisch an Sophos senden

Wenn die Datei als potenzielle Malware eingestuft wird, anhand der Eigenschaften der Datei jedoch keine eindeutige Klassifizierung möglich ist, kann Sophos über den Live-Schutz ein Dateisample anfordern. Wenn diese Option aktiviert ist und Sophos noch kein Dateisample vorliegt, wird die Datei automatisch an Sophos übermittelt.

Dateisamples helfen Sophos bei der Optimierung der Malware-Erkennung und minimieren falsche Erkennungen (sog. „False Positives“).

Hinweis: Samples dürfen maximal 10 MB groß sein. Das Zeitlimit für den Sample-Upload beträgt 30 Sekunden. Es wird davon abgeraten, Samples über eine langsamen Internetverbindung zu übertragen (weniger als 56 kbit/s).

Wichtig: Sie müssen sicherstellen, dass die Sophos-Domäne, an die die Dateidaten gesendet werden, in Ihrer Web-Filter-Lösung zu den vertrauenswürdigen Seiten hinzugefügt wurde. Nähere Informationen finden Sie im Support-Artikel **62637** (<http://www.sophos.de/support/knowledgebase/article/62637.html>).

Wenn Sie eine Web-Filter-Lösung von Sophos einsetzen (z.B. WS1000 Web Appliance), müssen Sie nicht tätig werden, da Sophos-Domänen zu den vertrauenswürdigen Seiten zählen.

18.4.2 Aktivieren/Deaktivieren von Sophos Live-Schutz

Bei rollenbasierter Verwaltung:

- Zur Ausführung dieses Tasks ist die Berechtigung **Richtlinieneinstellung – Virenschutz und HIPS** erforderlich.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 13).

Standardmäßig übermittelt Endpoint Security and Control Dateidaten an Sophos (z.B. Prüfsummen), jedoch keine Dateisamples. Aktivieren Sie beide Optionen, um Sophos Live-Schutz in vollem Umfang ausnutzen zu können.

So aktivieren/deaktivieren Sie die Optionen von Sophos Live-Schutz:

1. Prüfen Sie, welche Antivirus- und HIPS-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.
Mehr dazu erfahren Sie unter *Welche Richtlinien sind einer Gruppe zugewiesen?* (Seite 25).
2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Antivirus und HIPS**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.
3. Klicken Sie im Dialogfeld **Antivirus- und HIPS-Richtlinie** auf die Schaltfläche **Sophos Live-Schutz**.
4. Verfahren Sie im Dialogfeld **Sophos Live-Schutz** wie folgt:
 - Wenn Sie das Senden von Dateidaten an Sophos ein- bzw. ausschalten möchten, aktivieren bzw. deaktivieren Sie das Kontrollkästchen **Live-Schutz aktivieren**.
 - Wenn Sie das Senden von Dateisamples an Sophos ein- bzw. ausschalten möchten, aktivieren bzw. deaktivieren Sie das Kontrollkästchen **Dateisamples automatisch an Sophos senden**.

Hinweis: Wenn ein Datei-Sample an Sophos zum Online-Scan gesendet wird, werden die Dateidaten immer mitgesendet.

18.5 Scannen auf Adware und PUA

Bei rollenbasierter Verwaltung:

- Zur Ausführung dieses Tasks ist die Berechtigung **Richtlinieneinstellung – Virenschutz und HIPS** erforderlich.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

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

Es empfiehlt sich, die Suche nach potenziell unerwünschten Anwendungen über einen geplanten Scan zu starten. Auf diese Weise können Sie gefahrlos Anwendungen bearbeiten, die *bereits* auf Ihrem Computer aktiv sind. Sie können dann die On-Access-Erkennung aktivieren, um Ihre Computer in Zukunft zu schützen.

1. Prüfen Sie, welche Antivirus- und HIPS-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.

Mehr zu diesem Thema erfahren Sie unter [Welche Richtlinien sind einer Gruppe zugewiesen?](#) (Seite 25).

2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Antivirus und HIPS**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.

Das Dialogfeld **Antivirus- und HIPS-Richtlinie** wird geöffnet.

3. Klicken Sie im Fensterbereich **Geplante Scans** auf **Hinzufügen**, um einen neuen Scan zu erstellen, oder doppelklicken Sie auf einen Scan in der Liste, um ihn zu bearbeiten.
4. Im Dialogfeld **Einstellungen zu geplanten Scans** klicken Sie auf **Konfigurieren** (unten im Fenster).
5. Wählen Sie im Dialogfeld **Scan- und Bereinigungs-Einstellungen** auf der Registerkarte **Scans** unter **Scan-Einstellungen** die Option **Adware und PUA einbeziehen**. Klicken Sie auf **OK**.

Wenn der Scan ausgeführt wird, kann Sophos Endpoint Security and Control Adware oder potenziell unerwünschte Anwendungen melden.

6. Wenn Ihr Computer die Anwendungen starten soll, müssen Sie diese zulassen (mehr dazu erfahren Sie im Abschnitt [Zulassen von Adware und PUA](#) (Seite 90)). Andernfalls entfernen Sie die Anwendungen (mehr dazu erfahren Sie im Abschnitt [Sofortiges Bereinigen von Computern](#) (Seite 58)).

7. Wenn Sie die On-Access-Erkennung aktivieren möchten, öffnen Sie nochmals das Dialogfeld **Antivirus- und HIPS-Richtlinie**. Aktivieren Sie im Bereich **Antivirus- und HIPS-Konfiguration** das Kontrollkästchen **On-Access-Scans aktivieren**, falls noch nicht geschehen. Klicken Sie neben dem Kontrollkästchen auf die Schaltfläche **Konfigurieren**. Wählen Sie im Dialogfeld **On-Access-Scan-Einstellungen** die Option **Adware und PUA einbeziehen**.

Hinweis: 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 194).

18.6 Zulassen von Adware und PUA

Bei rollenbasierter Verwaltung:

- Zur Ausführung dieses Tasks ist die Berechtigung **Richtlinieneinstellung – Virenschutz und HIPS** erforderlich.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Wenn Sie Sophos Endpoint Security and Control für die Erkennung von Adware und potenziell unerwünschten Anwendungen (PUA) konfiguriert haben, kann damit eventuell die Verwendung einer erwünschten Anwendung verhindert werden.

Verfahren Sie zum Zulassen erwünschter Anwendungen wie folgt:

1. Prüfen Sie, welche Antivirus- und HIPS-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.
Mehr dazu erfahren Sie unter [Welche Richtlinien sind einer Gruppe zugewiesen?](#) (Seite 25).
2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Antivirus und HIPS**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.
3. Klicken Sie im Dialogfeld **Antivirus- und HIPS-Richtlinie** auf die Schaltfläche **Autorisierung**.
4. Wählen Sie im Dialogfeld **Authorization Manager** auf der Registerkarte **Adware und PUA** in der Liste **Bekannte Adware/PUA** die gewünschte Anwendung. Klicken Sie auf **Hinzufügen**, um sie in die Liste **Zugel. Adware/PUA** aufzunehmen.
5. Wenn die zuzulassende Anwendung nicht angezeigt wird, klicken Sie auf **Neuer Eintrag**.
Das Dialogfeld **Neue Adware/PUA** wird angezeigt.
6. Rufen Sie die Sicherheitsanalysen auf der Sophos Website <http://www.sophos.de/security/analyses> auf. Suchen Sie auf der Registerkarte **Adware/PUA** die gewünschte Anwendung.
7. Geben Sie in Enterprise Console in das Dialogfeld **Neue Adware/PUA** den Namen der gewünschten Anwendung ein und klicken Sie auf **OK**.

Die Anwendung wird in die Liste **Bekannte Adware/PUA** aufgenommen.

- Wählen Sie die Anwendung aus und klicken Sie auf **Hinzufügen**, um sie in die Liste **Zugel. Adware/PUA** aufzunehmen.

Wenn Sie eine Anwendung aus der Liste entfernen möchten, wählen Sie die Anwendung und klicken Sie auf **Eintrag löschen**.

18.7 Ändern der Scan-Objekte

Bei rollenbasierter Verwaltung:

- Zur Ausführung dieses Tasks ist die Berechtigung **Richtlinieneinstellung – Virenschutz und HIPS** erforderlich.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Standardmäßig scannt Sophos Endpoint Security and Control Dateitypen, die für Viren anfällig sind. Sie können weitere Dateitypen (Scan-Objekte) scannen lassen oder auch bestimmte Dateitypen von Scans ausschließen.

Die standardmäßig gescannten Dateitypen sind vom Betriebssystem abhängig und ändern sich bei Produkt-Updates. Sie können eine Liste der Dateitypen ansehen, wenn Sie zu einem Computer mit dem entsprechenden Betriebssystem gehen, Sophos Endpoint Security and Control oder Sophos Anti-Virus öffnen und dort die Konfigurationsseite mit den Erweiterungen aufrufen.

Hinweis:

Diese Optionen sind nur für Windows-Computer relevant.

Ab Windows 2000 können Sie die Einstellungen für On-Access-Scans und geplante Scans separat ändern. Unter Windows NT/95/98 werden Änderungen an den Einstellungen für geplante Scans auch für On-Access-Scans übernommen.

Sie können Änderungen auf Mac OS X-Computern mithilfe des Sophos Update Managers, einem mit Sophos Anti-Virus für Mac OS X gelieferten Dienstprogramm, durchführen. So öffnen Sie den Sophos Update Manager: Öffnen Sie auf einem Mac ein **Finder**-Fenster und rufen Sie den Ordner **Sophos Anti-Virus:ESOSX** auf. Doppelklicken Sie auf **Sophos Update Manager**. Weitere Details werden in der Sophos Update Manager-Hilfe aufgeführt.

Die Virenschutzeinstellungen auf Linux-Computern können Sie über die Befehle „savconfig“ und „savscan“ ändern. Anweisungen hierzu finden Sie im *Benutzerhandbuch für Sophos Anti-Virus für Linux*.

Die Virenschutzeinstellungen für UNIX-Computer können Sie über den Befehl „savscan“ ändern. Anweisungen hierzu finden Sie im *Benutzerhandbuch für Sophos Anti-Virus für UNIX*.

So lassen sich die Scan-Objekte ändern:

1. Prüfen Sie, welche Antivirus- und HIPS-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.
Mehr zu diesem Thema erfahren Sie unter [Welche Richtlinien sind einer Gruppe zugewiesen?](#) (Seite 25).
2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Antivirus und HIPS**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.
3. Stellen Sie die Optionen im Dialogfeld **Antivirus- und HIPS-Richtlinie** folgendermaßen ein:
 - Stellen Sie zur Konfiguration von On-Access-Scans sicher, dass im Bereich **Antivirus- und HIPS-Konfiguration** das Kontrollkästchen **On-Access-Scans aktivieren** aktiviert wurde. Klicken Sie neben dem Kontrollkästchen auf die Schaltfläche **Konfigurieren**.
 - Klicken Sie zur Konfiguration von geplanten Scans Sie im Bereich **Geplante Scans** auf **Erweiterungen und Ausschlüsse**.
4. Wählen Sie auf der Registerkarte **Erweiterungen** die Option **Ausführbare und infizierbare Dateien scannen**.
 - Um weitere Dateitypen zu scannen, klicken Sie auf **Hinzufügen** und geben im Feld **Erweiterung** die entsprechende Dateinamenserweiterung ein, z.B. PDF.
 - Um standardmäßig gescannte Dateitypen auszuschließen, klicken Sie auf **Ausschließen**. Das Dialogfeld **Erweiterungen ausschließen** wird angezeigt. Geben Sie die Dateierweiterung ein.

Standardmäßig werden Dateien ohne Erweiterung gescannt.

Hinweis: Sie können auch alle Dateien scannen lassen; dies beeinträchtigt jedoch die Leistung des Computers.

18.8 Ausschließen von Objekten von On-Access-Scans

Bei rollenbasierter Verwaltung:

- Zur Ausführung dieses Tasks ist die Berechtigung **Richtlinieneinstellung – Virenschutz und HIPS** erforderlich.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Sie können Objekte von On-Access-Scans ausschließen.

Hinweis:

Diese Optionen beschränken sich auf Windows 2000 (und aufwärts), Mac OS X und Linux.

Enterprise Console 4.5 kann auf UNIX-Computern keine On-Access-Scans durchführen.

Wenn Sie Objekte unter Windows NT/95/98 ausschließen möchten, nehmen Sie die entsprechenden Einstellungen auf den Konfigurationsseiten für **Geplante Scans** vor, die sich

auch auf On-Access-Scans beziehen. Mehr zu diesem Thema erfahren Sie unter [Ausschließen von Objekten von geplanten Scans](#) (Seite 100).

1. Prüfen Sie, welche Antivirus- und HIPS-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.
Mehr zu diesem Thema erfahren Sie unter [Welche Richtlinien sind einer Gruppe zugewiesen?](#) (Seite 25).
2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Antivirus und HIPS**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.
Das Dialogfeld **Antivirus- und HIPS-Richtlinie** wird geöffnet.
3. Klicken Sie im Feld **On-Access-Scans** auf die Schaltfläche **Konfigurieren**.
4. Klicken Sie auf die Registerkarte **Windows-Ausschlüsse, Mac-Ausschlüsse** oder **Linux/UNIX-Ausschlüsse**. Um Objekte zu der Liste hinzuzufügen, klicken Sie auf **Hinzufügen** und geben den vollständigen Pfad im Dialogfeld **Objekt ausschließen** ein.
Die von Scans ausschließbaren Objekte variieren je nach Computertyp. Mehr zu diesem Thema erfahren Sie unter [Objekte, die von Scans ausgeschlossen werden können](#) (Seite 101).

18.9 Scannen auf Rootkits

Bei rollenbasierter Verwaltung:

- Zur Ausführung dieses Tasks ist die Berechtigung **Richtlinieneinstellung – Virenschutz und HIPS** erforderlich.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Beim Durchführen einer **vollständigen Systemüberprüfung** wird auch auf Rootkits gescannt. (Mehr dazu erfahren Sie unter [Sofort-Scans](#) (Seite 67)). Wenn Sie die Einstellungen für einen geplanten Scan ändern möchten, verfahren Sie wie folgt.

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

1. Prüfen Sie, welche Antivirus- und HIPS-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten. Mehr dazu erfahren Sie unter [Welche Richtlinien sind einer Gruppe zugewiesen?](#) (Seite 25).
2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Antivirus und HIPS**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.
3. Klicken Sie im Dialogfeld **Antivirus- und HIPS-Richtlinie** im Bereich **Geplante Scans** auf **Hinzufügen** (oder markieren Sie einen bestehenden Scan und klicken Sie auf **Ändern**).
4. Geben Sie im Dialogfeld **Einstellungen für geplante Scans** Ihre Einstellungen ein und klicken Sie auf **Konfigurieren**.
5. Wählen Sie im Dialogfeld **Einstellungen zu Scans und Bereinigung ändern** auf der Registerkarte **Überprüfung** das Kontrollkästchen **Macintosh-Viren einbeziehen**. Klicken Sie auf **OK**.

18.10 Scannen von Archivdateien

Bei rollenbasierter Verwaltung:

- Zur Ausführung dieses Tasks ist die Berechtigung **Richtlinieneinstellung – Virenschutz und HIPS** erforderlich.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Hinweis: Durch das Scannen von Archivdateien verlangsamt sich der Scan-Vorgang. Archive müssen jedoch in der Regel nicht gescannt werden. Auch wenn Sie diese Option nicht auswählen und Sie versuchen, auf eine Datei zuzugreifen, die aus dem Archiv entpackt wurde, wird die entpackte Datei gescannt. Es empfiehlt sich daher nicht, diese Option zu wählen.

1. Prüfen Sie, welche Antivirus- und HIPS-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.
Mehr dazu erfahren Sie unter [Welche Richtlinien sind einer Gruppe zugewiesen?](#) (Seite 25).
2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Antivirus und HIPS**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.
3. Klicken Sie im Dialogfeld **Antivirus- und HIPS-Richtlinie** im Bereich **Geplante Scans** auf **Hinzufügen** (oder markieren Sie einen bestehenden Scan und klicken Sie auf **Ändern**).
4. Geben Sie im Dialogfeld **Einstellungen zu geplanten Scans** Ihre Einstellungen ein und klicken Sie dann auf **Konfigurieren** (unten in diesem Fenster).
5. Wählen Sie im Dialogfeld **Einstellungen zu Scans und Bereinigung ändern** auf der Registerkarte **Scannen** die Option **Archivdateien scannen**. Klicken Sie auf **OK**.

18.11 Scannen von Macintosh-Dateien

Bei rollenbasierter Verwaltung:

- Zur Ausführung dieses Tasks ist die Berechtigung **Richtlinieneinstellung – Virenschutz und HIPS** erforderlich.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Sie können in Sophos Endpoint Security and Control das Scannen von Macintosh-Dateien, die auf Windows-Computern gespeichert sind, aktivieren.

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

1. Prüfen Sie, welche Antivirus- und HIPS-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.
Mehr zu diesem Thema erfahren Sie unter [Welche Richtlinien sind einer Gruppe zugewiesen?](#) (Seite 25).

2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Antivirus und HIPS**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.
3. Stellen Sie die Optionen im Dialogfeld **Antivirus- und HIPS-Richtlinie** folgendermaßen ein:
 - **On-Access-Scans**

Stellen Sie bei der Konfiguration von On-Access-Scans sicher, dass im Feld **On-Access-Scans** die Option **On-Access-Scans aktivieren** ausgewählt ist. Klicken Sie neben dem Kontrollkästchen auf die Schaltfläche **Konfigurieren**.

Wählen Sie auf der Registerkarte **Scans** im Bereich **Scanoptionen** das Kontrollkästchen **Macintosh-Viren einbeziehen**.
 - **Geplante Scans**

Klicken Sie zum Konfigurieren von geplanten Scans im Bereich **Geplante Scans** auf **Hinzufügen** (oder wählen Sie einen bestehenden Scan und klicken Sie auf **Ändern**).

Geben Sie im Dialogfeld **Einstellungen für geplante Scans** Ihre Einstellungen ein und klicken Sie auf **Konfigurieren**.

Wählen Sie im Dialogfeld **Einstellungen zu Scans und Bereinigung ändern** auf der Registerkarte **Scans** das Kontrollkästchen **Macintosh-Viren einbeziehen**.

18.12 Der Web-Schutz

Der Web-Schutz bietet mehr Sicherheit vor Threats im Internet: Die Funktion unterbinden den Zugriff auf Seiten, die bekanntermaßen Malware hosten. Nach einem Abgleich mit der Online-Malware-Datenbank von Sophos in Echtzeit wird der Zugriff auf betroffene Seiten verweigert.

Der Web-Schutz leistet Folgendes:

- Sperren des Netzwerkzugriffs auf schädliche Websites.
- Scannen von mit Internet Explorer heruntergeladenen Dateien und Daten.

Nähere Informationen zum Aktivieren des Web-Schutzes können Sie dem Abschnitt [Aktivieren des Web-Schutzes](#) (Seite 95) entnehmen.

18.13 Aktivieren des Web-Schutzes

Bei rollenbasierter Verwaltung:

- Zur Ausführung dieses Tasks ist die Berechtigung **Richtlinieneinstellung – Virenschutz und HIPS** erforderlich.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

So aktivieren Sie den Web-Schutz:

1. Prüfen Sie, welche Antivirus- und HIPS-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.

Mehr zu diesem Thema erfahren Sie unter [Welche Richtlinien sind einer Gruppe zugewiesen?](#) (Seite 25).

2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Antivirus und HIPS**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.
3. Wählen Sie im Dialogfeld **Antiviren- und HIPS-Richtlinie** neben der Option **Zugriff auf schädliche Websites sperren Ein** aus. Diese Option ist standardmäßig aktiviert.

Anweisungen zum Zulassen bestimmter Websites entnehmen Sie bitte dem Abschnitt [Zulassen von Websites](#) (Seite 96).

4. Wählen Sie zum Scannen von mit Internet Explorer heruntergeladenen Daten und Dateien neben **Download-Scans**: die Option **Ein**.

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

18.14 Zulassen von Websites

Bei rollenbasierter Verwaltung:

- Zur Ausführung dieses Tasks ist die Berechtigung **Richtlinieneinstellung – Virenschutz und HIPS** erforderlich.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).



Vorsicht: Wenn Sie Websites, die als schädlich eingestuft wurden, zulassen, sind Sie nicht vor Threats geschützt. Stellen Sie sicher, dass der Zugriff auf eine Website sicher ist, bevor Sie sie zulassen.

Wenn Sie die Sperrung einer von Sophos als schädlich eingestuften Website aufheben möchten, fügen Sie die Seite zur Liste der zugelassenen Seiten hinzu. URLs zugelassener Websites werden nicht von der Web-Filterfunktion von Sophos erfasst.

Hinweis: Wenn Download-Scans aktiviert sind und Sie eine Seite mit einem Threat in Internet Explorer aufrufen, wird der Zugriff auf die Seite gesperrt, auch wenn die Website zugelassen wurde.

So lassen Sie eine Website zu:

1. Prüfen Sie, welche Antivirus- und HIPS-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.

Mehr dazu erfahren Sie unter [Welche Richtlinien sind einer Gruppe zugewiesen?](#) (Seite 25).

2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Antivirus und HIPS**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.

3. Klicken Sie im Dialogfeld **Antivirus- und HIPS-Richtlinie** auf die Schaltfläche **Autorisierungen**.
4. Klicken Sie im Dialogfeld **Authorization Manager** auf der Registerkarte **Websites** auf **Hinzufügen**, um eine Website anhand einer der verfügbaren Optionen hinzuzufügen.
Sie können den Domännennamen, die IP-Adresse oder die IP-Adresse mit Subnetzmaske einer Website hinzufügen.

Wenn Sie eine Website bearbeiten oder aus der Liste entfernen möchten, wählen Sie die Website aus und klicken Sie auf **Ändern** oder **Entfernen**.

Im Abschnitt [Aufrufen gesperrter Websites](#) (Seite 65) wird erläutert, wie Sie eine Liste der in letzter Zeit gesperrten Websites auf einem Endpoint aufrufen können.

18.15 Aktivieren/Deaktivieren der On-Access-Scans

Bei rollenbasierter Verwaltung:

- Zur Ausführung dieses Tasks ist die Berechtigung **Richtlinieneinstellung – Virenschutz und HIPS** erforderlich.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Standardmäßig scannt Sophos Endpoint Security and Control Dateien, wenn der Anwender versucht, auf sie zuzugreifen und verweigert den Zugriff, wenn sie nicht virenfrei sind.

Möglicherweise möchten Sie On-Access-Scans auf Exchange-Servern oder auf Servern, deren Leistung beeinträchtigt ist, ausschalten. Fassen Sie in diesem Fall die Server zu einer eigenen Gruppe zusammen und ändern Sie die Antiviren- und HIPS-Richtlinie für diese Gruppe wie folgt:

Wichtig: Wenn Sie On-Access-Scans auf einem Server ausschalten, empfehlen wir Ihnen, auf den entsprechenden Computern geplante Scans einzurichten.

1. Prüfen Sie, welche Antivirus- und HIPS-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.
Mehr dazu erfahren Sie unter [Welche Richtlinien sind einer Gruppe zugewiesen?](#) (Seite 25).
2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Antivirus und HIPS**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.
Das Dialogfeld **Antivirus- und HIPS-Richtlinie** wird geöffnet.
3. Deaktivieren Sie zum Ausschalten von On-Access-Scans das Kontrollkästchen neben **On-Access-Scans aktivieren**. Klicken Sie dann im Bereich **Geplante Scans** auf **Hinzufügen** und richten Sie einen geplanten Scan ein.

Wenn Sie später On-Access-Scans wieder aktivieren möchten, aktivieren Sie das Kontrollkästchen **On-Access-Scans** erneut.

18.16 Ändern der Bedingungen für On-Access-Scans

Bei rollenbasierter Verwaltung:

- Zur Ausführung dieses Tasks ist die Berechtigung **Richtlinieneinstellung – Virenschutz und HIPS** erforderlich.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Sie können angeben, ob Dateien gescannt werden sollen, wenn sie geöffnet („beim Lesen“), gespeichert („beim Schreiben“) oder umbenannt werden.

Hinweis:

Das Scannen von Dateien „beim Schreiben“ oder „beim Umbenennen“ kann sich auf die Leistung des Computers auswirken. Diese Optionen werden gewöhnlich nicht empfohlen.

Diese Optionen sind nur für Windows-Computer relevant.

1. Prüfen Sie, welche Antivirus- und HIPS-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.
Mehr zu diesem Thema erfahren Sie unter [Welche Richtlinien sind einer Gruppe zugewiesen?](#) (Seite 25).
2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Antivirus und HIPS**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.
3. Klicken Sie im Dialogfeld **Antivirus- und HIPS-Richtlinie** im Bereich **On-Access-Scans** auf die Schaltfläche **Konfigurieren**.
4. Wählen Sie im Dialogfeld **Einstellungen zu On-Access-Scans** auf der Registerkarte **Scan** im Bereich **Auslöser für On-Access-Scans** die gewünschten Optionen.

18.17 Scannen von Computern zu bestimmten Zeiten

Bei rollenbasierter Verwaltung:

- Zur Ausführung dieses Tasks ist die Berechtigung **Richtlinieneinstellung – Virenschutz und HIPS** erforderlich.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Computer können zu festgesetzten Zeiten gescannt werden.

Hinweis: Geplante Scans können nur auf Windows-, UNIX-, und Linux-Computern ausgeführt werden. Unter Windows 95/98 können geplante Scans nur ausgeführt werden, wenn das Sophos Anti-Virus-Fenster geöffnet ist.

1. Prüfen Sie, welche Antivirus- und HIPS-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.
Mehr dazu erfahren Sie unter [Welche Richtlinien sind einer Gruppe zugewiesen?](#) (Seite 25).
2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Antivirus und HIPS**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.
3. Klicken Sie im Dialogfeld **Antivirus- und HIPS-Richtlinie** im Bereich **Geplante Scans** auf **Hinzufügen**.
4. Geben Sie im Dialogfeld **Einstellungen zu geplanten Scans** einen Namen für den geplanten Scan ein. Wählen Sie die Objekte aus, die gescannt werden sollen (standardmäßig werden alle lokalen Festplatten oder bereitgestellten Dateisysteme gescannt). Wählen Sie den gewünschten Scanzzeitpunkt (Datum und Uhrzeit) aus.
5. Wenn Sie andere Scan-Optionen ändern oder diesen Scan zum Bereinigen von Computern konfigurieren möchten, klicken Sie unten im Dialogfeld auf **Konfigurieren**.
Mehr zu den Optionen für geplante Scans erfahren Sie unter [Ändern der Einstellungen für geplante Scans](#) (Seite 99).

18.18 Ändern der Einstellungen für geplante Scans

Bei rollenbasierter Verwaltung:

- Zur Ausführung dieses Tasks ist die Berechtigung **Richtlinieneinstellung – Virenschutz und HIPS** erforderlich.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

So können Sie die Einstellungen für geplante Scans ändern:

1. Prüfen Sie, welche Antivirus- und HIPS-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.
Mehr dazu erfahren Sie unter [Welche Richtlinien sind einer Gruppe zugewiesen?](#) (Seite 25).
2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Antivirus und HIPS**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.

3. Wählen Sie im Dialogfeld **Antivirus- und HIPS-Richtlinie** im Bereich **Geplante Scans** die gewünschten Einstellungen vor.

Sie können die folgenden Änderungen vornehmen:

- Wenn Sie die Dateitypen ändern möchten, die von *allen* geplanten Scans erfasst werden, klicken Sie auf **Erweiterungen und Ausschlüsse**.
- Wenn Sie spezifische Einstellungen einer Scanfunktion ändern möchten (z.B. Scan-Objekte, Scan-Zeit, Scan-Optionen, Bereinigung), markieren Sie den Scan und klicken auf **Ändern**. Klicken Sie dann im Dialogfeld **Einstellungen zu geplanten Scans** auf **Konfigurieren**.

Hinweis: Nähere Informationen zu Scan-Optionen finden Sie unter [Scannen auf verdächtige Dateien](#) (Seite 85), [Scannen auf Adware und PUA](#) (Seite 89) und [Scannen von Archivdateien](#) (Seite 94). Bereinigungs-Optionen werden unter [Einrichten der automatischen Bereinigung](#) (Seite 59) näher erläutert.

18.19 Ausschließen von Objekten von geplanten Scans

Bei rollenbasierter Verwaltung:

- Zur Ausführung dieses Tasks ist die Berechtigung **Richtlinieneinstellung – Virenschutz und HIPS** erforderlich.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Sie können Objekte von geplanten Scans ausschließen.

Hinweis:

Die Einstellungen für die ausgeschlossenen Objekte für geplante Scans treffen auch für vollständige Systemüberprüfungen zu, die von der Konsole gestartet werden, und für Scans über die Option „Meinen Computer scannen“ auf Netzwerkcomputern. Mehr dazu erfahren Sie unter [Sofort-Scans](#) (Seite 67).

Unter Windows NT/95/98 werden Änderungen an den Einstellungen für geplante Scans auch für On-Access-Scans übernommen.

Auf Macintosh-Computern sind keine geplanten Scans möglich.

1. Prüfen Sie, welche Antivirus- und HIPS-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.
Mehr dazu erfahren Sie unter [Welche Richtlinien sind einer Gruppe zugewiesen?](#) (Seite 25).
2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Antivirus und HIPS**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.
3. Das Dialogfeld **Antivirus- und HIPS-Richtlinie** wird angezeigt. Klicken Sie im Fensterbereich **Geplante Scans** auf **Erweiterungen und Ausschlüsse**.

4. Klicken Sie auf die Registerkarte **Windows-Ausschlüsse** oder **Linux-/UNIX-Ausschlüsse**. Um Objekte zu der Liste hinzuzufügen, klicken Sie auf **Hinzufügen** und geben den vollständigen Pfad im Dialogfeld **Objekt ausschließen** ein.

Die von Scans ausschließbaren Objekte variieren je nach Computertyp. Mehr dazu erfahren Sie unter [Objekte, die von Scans ausgeschlossen werden können](#) (Seite 101).

18.20 Objekte, die von Scans ausgeschlossen werden können

Objekte, die von Scans ausgeschlossen werden können, variieren je nach Betriebssystem.

Windows 2000 und höher

Unter Windows 2000 und höher können Sie Laufwerke, Ordner und Dateien ausschließen.

Sie können die Platzhalter * und ? benutzen.

Der Platzhalter ? kann nur für Dateinamen oder Erweiterungen benutzt werden. Er ersetzt in der Regel ein einziges Zeichen. Am Ende eines Dateinamens kann das Fragezeichen jedoch auch ein fehlendes Zeichen ersetzen. Beispiel: Die Eingabe von „datei?.txt“ dient als Ersatz für „datei.txt“, „datei1.txt“ sowie „datei12.txt“, jedoch nicht „datei123.txt“.

Der Platzhalter * kann nur für Dateinamen oder -erweiterungen in der Form *[Dateiname].** oder **.[Erweiterung]* verwendet werden. Beispiel: Die Eingabe von „datei*.txt“, „datei.txt*“ und „datei.*txt“ ist nicht zulässig.

Weitere Details werden im Abschnitt „Sophos Anti-Virus“ in der Hilfe zu Sophos Endpoint Security and Control 9 beschrieben.

Windows NT

Unter Windows NT können Sie Dateien und Verzeichnisse ausschließen.

Windows 95/98

Unter Windows 95/98 können Sie Dateien, Verzeichnisse (für geplante Scans) und Laufwerke ausschließen.

Mac OS X

Unter Mac OS X können Sie Volumes, Ordner und Dateien ausschließen.

Obwohl Platzhalter nicht unterstützt werden, können Sie Objekte ausschließen, indem Sie die Ausnahmen mit einem einfachen oder doppelten Schrägstrich voran- oder nachstellen.

Weitere Einzelheiten werden in den Hilfedateien oder dem Benutzerhandbuch für Sophos Anti-Virus für Mac OS X aufgeführt.

Linux oder UNIX

Unter Linux und UNIX können Sie Verzeichnisse und Dateien ausschließen, indem Sie einen Pfad angeben (mit oder ohne Platzhalter).

Hinweis: Enterprise Console unterstützt nur Pfad-basierte Linux- und UNIX-Ausnahmen. Sie können außerdem andere Arten von Ausnahmen direkt auf den verwalteten Computern einrichten. Sie können dann reguläre Ausdrücke verwenden und Dateitypen und Dateisysteme

ausschließen. Anweisungen dazu finden Sie im *Benutzerhandbuch für SophosAnti-Virus für Linux* oder für *Sophos Anti-Virus für UNIX*.

Wenn Sie eine weitere Pfad-basierte Ausnahme auf einem verwalteten Linux- oder UNIX-Computer einrichten, wird dieser Computer der Konsole als von der Gruppenrichtlinie abweichend gemeldet.

19 Konfigurieren der Update-Richtlinie

19.1 Update-Richtlinie

Eine Update-Richtlinie hält die Sicherheitssoftware auf Ihren Computer auf dem neuesten Stand. Enterprise Console sucht nach Updates und lädt diese in festgelegten Zeitabständen bei Bedarf herunter.

Mit der Standardrichtlinie können Sie die im Abonnement „Neueste“ festgelegte Software installieren und updaten.

Anweisungen zum Ändern der Standard-Update-Richtlinie oder Erstellen einer neuen Richtlinie finden Sie in den folgenden Abschnitten.

- [Auswahl eines Abonnements](#) (Seite 103)
- [Auswahl der Update-Quelle](#) (Seite 104)
- [Update-Zeitpläne](#) (Seite 105)
- [Ändern der Erstinstallationsquelle](#) (Seite 106)
- [Update-Protokoll](#) (Seite 107)

Bei Upgrades von Enterprise Console 3.x werden die vor dem Upgrade vorhandenen Richtlinien zu „alten Update-Richtlinien“. Weitere Informationen hierzu finden Sie im Abschnitt „Alte Update-Richtlinien“.

Hinweis: Bei rollenbasierter Verwaltung:

- Zum Konfigurieren einer Update-Richtlinie müssen Sie über die Berechtigung **Richtlinieneinstellung – Updates** verfügen.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Nähere Informationen zur rollenbasierten Verwaltung können Sie dem Abschnitt [Rollen und Teilverwaltungseinheiten](#) (Seite 13) entnehmen.

19.2 Auswahl eines Abonnements

Bei rollenbasierter Verwaltung:

- Zum Konfigurieren einer Update-Richtlinie müssen Sie über die Berechtigung **Richtlinieneinstellung – Updates** verfügen.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Durch Software-Abonnements wird festgelegt, welche Endpoint-Softwareversionen für die jeweiligen Systeme von Sophos heruntergeladen werden. Das Standard-Abonnement umfasst die aktuelle Software für Windows 2000 und höher.

So können Sie ein Abonnement auswählen:

1. Prüfen Sie, welche Update-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.
Mehr dazu erfahren Sie unter [Welche Richtlinien sind einer Gruppe zugewiesen?](#) (Seite 25).
2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Update**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.
3. Klicken Sie im Dialogfeld **Update-Richtlinie** auf die Registerkarte **Abonnements** und wählen Sie ein Abonnement für Software, die Sie auf dem neuesten Stand halten möchten.

19.3 Auswahl der Update-Quelle

Bei rollenbasierter Verwaltung:

- Zum Konfigurieren einer Update-Richtlinie müssen Sie über die Berechtigung **Richtlinieneinstellung – Updates** verfügen.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Standardmäßig beziehen die Computer von folgender Freigabe Updates:

\\<ComputerName>\SophosUpdate. ComputerName steht dabei für den Namen des Computers, auf dem der Update Manager installiert wurde. Sie können eine andere Freigabe angeben.

Sie können außerdem eine alternative Update-Quelle angeben. Wenn Computer keine Verbindung zur Haupt-Update-Quelle herstellen können, versuchen sie, Updates von der alternativen Quelle zu beziehen. Sophos empfiehlt, dass Sie eine alternative Quelle für Updates einrichten, wenn Sie Computer haben, die nicht immer mit dem Unternehmensnetzwerk verbunden sind, z.B. Laptops.

So können Sie eine Update-Quelle eingeben:

1. Prüfen Sie, welche Update-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.
Mehr dazu erfahren Sie unter [Welche Richtlinien sind einer Gruppe zugewiesen?](#) (Seite 25).
2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Updating**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.
3. Verfahren Sie im Dialogfeld **Update-Richtlinie** wie folgt:
 - Wenn Sie die primäre Update-Quelle ändern möchten, rufen Sie die Registerkarte **Primärserver** auf.
 - Wenn Sie eine alternative Update-Quelle angeben möchten, öffnen Sie die Registerkarte **Sekundärserver** und wählen Sie die Option **Sekundärserver festlegen**.

4. Rufen Sie im Dialogfeld **Update-Richtlinie** die Registerkarte **Primärserver** auf. Geben Sie in das **Adressfeld** die Adresse (UNC-Pfad (Netzwerk-Pfad) oder Internet-Adresse) der Freigabe ein, von der Endpoints in der Regel Updates beziehen.

Wichtig: Wenn Sie eine HTTP-Adresse (z.B. eine Update-Freigabe im Internet) oder eine Freigabe, die nicht von einem verwalteten Update Manager gewartet wird, angegeben haben, kann Enterprise Console nicht prüfen, ob die in der Abonnement-Richtlinie angegebene Software unter dieser Adresse vorhanden ist. Sie müssen manuell überprüfen, ob die Freigabe die in der Abonnement-Richtlinie festgelegte Software enthält. Andernfalls werden die Computer nicht upgedatet.

5. Wenn Sie Macintosh-Computer mit Enterprise Console verwalten möchten und im Feld **Adresse** eine UNC-Freigabe angegeben haben, wählen Sie im Bereich **Mac OS-spezifische Optionen** ein Protokoll aus, über das die Macs auf die Update-Freigabe zugreifen sollen.
6. Geben Sie bei Bedarf den **Benutzernamen** für den Zugriff auf den Server ein. Geben Sie dann das Kennwort ein und bestätigen Sie das Kennwort. Das Konto benötigt Lesezugriff auf die Freigabe, die Sie in das Adressfeld eingegeben haben.

Hinweis: Falls der Benutzername auch eine Domäne erfordert, geben Sie ihn im Format Domäne\Benutzername ein.

7. Wenn Sie die zu verwendende Bandbreite beschränken möchten, klicken Sie auf **Erweitert**. Wählen Sie im Dialogfeld **Erweiterte Einstellungen** die Option **Bandbreite verringern** und geben Sie mit Hilfe des Schiebereglers die Bandbreite in KBit/s an. Wenn Sie mehr Bandbreite angeben, als dem Computer zur Verfügung steht, wird für die Updates die verfügbare Bandbreite benutzt.
8. Wenn Sie über einen Proxyserver auf die Update-Quelle zugreifen, klicken Sie auf **Proxyserver-Details**. Wählen Sie im Dialogfeld **Proxy-Details** die Option **Internetverbindung über Proxy**. Geben Sie anschließend die **Adresse** und den **Port** des Proxyservers an. Geben Sie die **Zugangsdaten** des Proxyservers ein. Falls der Benutzername auch eine Domäne erfordert, geben Sie ihn im Format Domäne\Benutzername ein.
Bei einigen Internet Service Providern werden Internetanfragen an einen Proxyserver gesendet.

19.4 Update-Zeitpläne

Bei rollenbasierter Verwaltung:

- Zum Konfigurieren einer Update-Richtlinie müssen Sie über die Berechtigung **Richtlinieneinstellung – Updates** verfügen.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Standardmäßig sucht der Computer alle 5 Minuten nach Updates.

Hinweis: Wenn Updates direkt von Sophos heruntergeladen werden, werden die Update-Intervalleinstellungen nicht übernommen. Computer mit Sophos PureMessage können alle 15 Minuten nach Updates suchen. Computer ohne Sophos PureMessage werden alle 60 Minuten aktualisiert.

So können Sie das Update-Intervall festlegen:

1. Prüfen Sie, welche Update-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.
Mehr dazu erfahren Sie unter [Welche Richtlinien sind einer Gruppe zugewiesen?](#) (Seite 25).
2. Doppelklicken Sie im Bereich **Richtlinien** auf **Update**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.
3. Rufen Sie im Dialogfeld **Update-Richtlinie** die Registerkarte **Zeitplan** auf und stellen Sie sicher, dass das Kontrollkästchen **Sophos Updates automatisch herunterladen** aktiviert ist. Geben Sie ein Intervall für Software-Updates (in Minuten) ein.
4. Wenn Sie Updates über eine Einwahlverbindung durchführen, wählen Sie **Bei Internetverbindung auf Updates prüfen**.

Die Computer versuchen dann bei jeder Internetverbindung ein Update durchzuführen.

19.5 Ändern der Erstinstallationsquelle

Bei rollenbasierter Verwaltung:

- Zum Konfigurieren einer Update-Richtlinie müssen Sie über die Berechtigung **Richtlinieneinstellung – Updates** verfügen.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Standardmäßig wird Sicherheitssoftware auf Computern installiert und dann über die auf der Registerkarte **Primärserver** angegebenen Quelle aktualisiert. Sie können eine andere Quelle für die Erstinstallation angeben.

Hinweis:

Diese Einstellung ist nur für Windows 2000 und höher relevant.

Wenn Ihr Primärserver eine HTTP- (Internet)-Adresse ist und Sie die Installation auf den Computern von der Konsole aus durchführen möchten, müssen Sie eine Quelle für die Erstinstallation angeben.

So können Sie die Quelle für die Erstinstallation ändern:

1. Prüfen Sie, welche Update-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.
Mehr dazu erfahren Sie unter [Welche Richtlinien sind einer Gruppe zugewiesen?](#) (Seite 25).
2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Update**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.
3. Deaktivieren Sie im Dialogfeld **Update-Richtlinie** auf der Registerkarte **Erstinstallationsquelle** das Kontrollkästchen **Adresse des Primärservers übernehmen**. Geben Sie dann die Adresse der gewünschten Quelle ein.

19.6 Update-Protokoll

Bei rollenbasierter Verwaltung:

- Zum Konfigurieren einer Update-Richtlinie müssen Sie über die Berechtigung **Richtlinieneinstellung – Updates** verfügen.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Standardmäßig wird die Update-Aktivität von Computern protokolliert. Das Protokoll darf standardmäßig maximal 1 MB umfassen. Die Voreinstellung für den Protokollgrad lautet „normal“.

So können Sie die Protokolleinstellungen ändern:

1. Prüfen Sie, welche Update-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.
Mehr dazu erfahren Sie unter [Welche Richtlinien sind einer Gruppe zugewiesen?](#) (Seite 25).
2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Updating**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.
3. Stellen Sie sicher, dass im Dialogfeld **Update-Richtlinie** auf der Registerkarte **Protokollierung** die Option **Sophos AutoUpdates protokollieren** aktiviert ist. Geben Sie in das Feld **Max. Protokollgröße** die gewünschte Größe in MB ein.
4. Wählen Sie im Feld **Protokollgrad** die Option **Normal** oder **Ausführlich** aus.
In ausführlichen Protokollen werden mehr Aktivitäten protokolliert als gewöhnlich, was sich auch auf die Protokollgröße auswirkt. Verwenden Sie diese Einstellung nur, wenn Sie das ausführliche Protokoll zur Problembehebung benötigen.

19.7 Ändern der Zugangsdaten zum Primärserver

Bei rollenbasierter Verwaltung:

- Zum Konfigurieren einer Update-Richtlinie müssen Sie über die Berechtigung **Richtlinieneinstellung – Updates** verfügen.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

So ändern Sie die Zugangsdaten des Primärserver:

1. Doppelklicken Sie im Bereich **Richtlinien** auf **Update**. Doppelklicken Sie dann auf die Update-Richtlinie, die Sie ändern möchten.
2. Geben Sie im Dialogfeld **Update-Richtlinie** auf der Registerkarte **Primärserver** die neuen Zugangsdaten zum Zugang für den Server ein. Sie können bei Bedarf auch andere Angaben ändern.

3. Wählen Sie im Feld **Gruppen** eine Gruppe aus, die die soeben geänderte Update-Richtlinie verwendet. Rechtsklicken Sie auf die Auswahl und wählen Sie **Konformität mit > Gruppen-Update-Richtlinie**.

Wiederholen Sie diesen Schritt für alle Gruppen in der Richtlinie.

19.8 Updaten von Computern ohne permanente Netzwerkverbindung

Bei rollenbasierter Verwaltung:

- Zum Konfigurieren einer Update-Richtlinie müssen Sie über die Berechtigung **Richtlinieneinstellung – Updates** verfügen.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Wenn manche Computer nicht ständig mit dem Netzwerk verbunden sind (z.B. Laptops, die auch außerhalb des Unternehmens eingesetzt werden), können Sie eine alternative Update-Quelle für die Zeit angeben, in der die Computer nicht mit dem Netzwerk verbunden sind.

Mögliche Update-Quellen sind ein Update-Ordner auf einer von Ihrem Unternehmen verwalteten Website oder die Sophos Website. Anweisungen zum Erstellen eines Update-Ordners auf einem Webserver finden Sie unter [Freigeben von Sicherheitssoftware in einem Webserver](#) (Seite 82).

So legen Sie eine zweite Update-Quelle fest:

1. Prüfen Sie, welche Update-Richtlinie von der/den Computergruppe/n verwendet wird, die Sie konfigurieren möchten. Mehr dazu erfahren Sie unter [Welche Richtlinien sind einer Gruppe zugewiesen?](#) (Seite 25).
2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Update**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.
3. Rufen Sie im Dialogfeld **Update-Richtlinie** die Registerkarte **Sekundärserver** und wählen Sie **Sekundärserver festlegen** aus.
4. Geben Sie in das **Adressfeld** die **Adresse** (UNC (Netzwerk)-Pfad oder Internetadresse) der Freigabe ein, von der Endpoints Updates heruntergeladen sollen, wenn sie die andere Quelle nicht kontaktieren können.

Wichtig: Bei Verwendung einer HTTP-Adresse (z.B. einer internetbasierten Update-Freigabe) oder einer Freigabe, die nicht von einem verwalteten Update Manager verwaltet wird, kann Enterprise Console nicht feststellen, ob die im Abonnement angegebene Software unter dieser Adresse verfügbar ist. Sie müssen manuell überprüfen, ob die Freigabe die in der Abonnement-Richtlinie festgelegte Software enthält. Andernfalls werden die Computer nicht upgedatet.

5. Geben Sie bei Bedarf den **Benutzernamen** für den Zugriff auf den Server ein. Geben Sie dann das Kennwort ein und bestätigen Sie das Kennwort.

Das Konto muss:

- Lesezugriff auf die in das Adressfeld eingegebene Freigabe besitzen (und zur Freigabe browsen können).
- sich am Computer in der Gruppe oder der Gruppe anmelden können.

Nähere Informationen zum Überprüfen eines Windows-Benutzerkontos finden Sie im Sophos Support-Artikel 11637

(<http://www.sophos.de/support/knowledgebase/article/11637.html>) näher beschrieben.

Hinweis: Falls der Benutzername auch eine Domäne erfordert, geben Sie ihn im Format Domäne\Benutzername ein.

6. Wenn Sie die zu verwendende Bandbreite beschränken möchten, klicken Sie auf **Erweitert**. Wählen Sie im Dialogfeld **Erweiterte Einstellungen** die Option **Bandbreite verringern** und geben Sie mit Hilfe des Schiebereglers die Bandbreite in KBit/s an. Wenn Sie mehr Bandbreite angeben, als dem Computer zur Verfügung steht, wird für die Updates die verfügbare Bandbreite benutzt.
7. Wenn Sie über einen Proxyserver auf die Update-Quelle zugreifen, klicken Sie auf **Proxyserver-Details**. Wählen Sie im Dialogfeld **Proxy-Details** die Option **Internetverbindung über Proxy**. Geben Sie anschließend die **Adresse** und den **Port** des Proxyservers an. Geben Sie die **Zugangsdaten** des Proxyservers ein. Falls der Benutzername auch eine Domäne erfordert, geben Sie ihn im Format Domäne\Benutzername ein.
Bei einigen Internet Service Providern werden Internetanfragen an einen Proxyserver gesendet.

20 Alte Update-Richtlinien

20.1 Informationen zu alten Update-Richtlinien

Bei Upgrades von Enterprise Console 3.x werden die vor dem Upgrade vorhandenen Richtlinien zu „alten Update-Richtlinien“. Der neue, effizientere Sophos Update Manager wird in Anlehnung an Ihre vorhandenen Update-Einstellungen (aus Sophos EM Library) installiert. Mit dem Migrations-Assistenten von EM Library zu Update Manager können Sie Enterprise Console-Computergruppen migrieren, damit Sie von Update Manager aktualisiert werden. Gruppen, die nicht vom Assistenten erfasst werden, verwenden weiterhin die alten Update-Richtlinien.

Anweisungen zum Migrieren von Gruppen, die nicht vom Migrations-Assistenten erfasst wurden, finden Sie in der *Erweiterten Upgrade-Anleitung zu Sophos Endpoint Security and Control*.

Wenn Sie die alten Update-Richtlinien vor der Migration weiter einsetzen möchten, entnehmen Sie bitte dem Abschnitt [Konfigurieren alter Update-Richtlinien](#) (Seite 110) entsprechende Anweisungen.

Informationen zum Setup von EM Library und Erstellen von zentralen Installationsverzeichnissen (CIDs) finden sie in der Hilfe zu EM Library. So öffnen Sie EM Library: Klicken Sie im Dashboard, im Abschnitt **Updates** auf den Link **EM Library zuletzt upgedatet um <Zeit>**.

Hinweis: Bei rollenbasierter Verwaltung:

- Sie müssen über die Berechtigung **Richtlinieneinstellung – Updates** verfügen, um eine alte Richtlinie konfigurieren zu können.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Nähere Informationen zur rollenbasierten Verwaltung können Sie dem Abschnitt [Rollen und Teilverwaltungseinheiten](#) (Seite 13) entnehmen.

20.2 Konfigurieren alter Update-Richtlinien

Bei rollenbasierter Verwaltung:

- Sie müssen über die Berechtigung **Richtlinieneinstellung – Updates** verfügen, um eine alte Richtlinie konfigurieren zu können.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Sie müssen die Schritte für alle Computertypen (z.B. Windows 2000 und höher) in den Gruppen durchführen, auf die Sie diese Update-Richtlinie übertragen.

So können Sie alte Updates konfigurieren:

1. Öffnen Sie die gewünschte alte Update-Richtlinie.
 - Rechtsklicken Sie zum *Erstellen einer alten Update-Richtlinie* im Bereich **Richtlinien** auf **Alte Richtlinie einbeziehen** und wählen Sie **Richtlinie erstellen**. Geben Sie einen Namen für die Richtlinie ein und drücken Sie dann die **Eingabetaste**, um den Namen zu speichern. Doppelklicken Sie auf die neue Richtlinie, um sie zu bearbeiten.
 - Doppelklicken Sie zum *Ändern der Standardrichtlinien* auf **Alte Richtlinien einbeziehen** und dann auf **Standard**.
 - Wenn Sie eine *erstellte Richtlinie ändern* möchten, prüfen Sie, welche Update-Richtlinie von den Computer-Gruppen verwendet wird, die Sie konfigurieren möchten. (Mehr dazu erfahren Sie unter [Welche Richtlinien sind einer Gruppe zugewiesen?](#) (Seite 25).) Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Alte Richtlinie einbeziehen**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.
2. Wählen Sie im Dialogfeld **Alte Update-Richtlinie** ein Betriebssystem. Klicken Sie auf **Konfigurieren**.
3. Klicken Sie im Dialogfeld **Update-Richtlinie festlegen** auf die Registerkarte **Primärserver** und stellen Sie die Optionen wie nachfolgend beschrieben ein.

Adresse

Geben Sie die Adresse (UNC (Netzwerk)-Pfad oder Internetadresse) ein, von der Sophos Anti-Virus Updates herunterlädt. Eine Liste der Standard-Update-Verzeichnisse (zentralen Installationsverzeichnisse) finden Sie unter [Standardverzeichnisse für alte Updates](#) (Seite 119).

Benutzername

Wenn erforderlich, geben Sie den **Benutzernamen** für das Konto ein, mit dem auf den Server zugegriffen wird, und geben Sie dann das **Kennwort** ein. Dieses Konto benötigt Leserechte für das Verzeichnis, das Sie in das Adressfeld eingegeben haben.

Hinweis: Wenn der **Benutzername** die Domäne enthalten muss, verwenden Sie die Form `domäne\benutzername`.

Erweiterte Einstellungen und Proxy-Details

Wenn Sie die zu verwendende Bandbreite beschränken möchten, klicken Sie auf **Erweitert**. Mehr dazu erfahren Sie unter [Verringern der Bandbreite](#) (Seite 117).

Wenn Sie über einen Proxyserver auf die Update-Quelle zugreifen, klicken Sie auf **Proxyserver-Details**. Mehr dazu erfahren Sie unter [Angabe eines Proxyservers für alte Updates](#) (Seite 116). Bei einigen Internet Service Providern werden Internetanfragen an einen Proxyserver gesendet.

4. Klicken Sie auf die Registerkarte **Zeitplan** und geben Sie die Details ein, wie nachfolgend beschrieben.

Netzwerkcomputer können Sophos Updates automatisch herunterladen

Wählen Sie diese Option, wenn die Computer in regelmäßigen Intervallen aktualisiert werden sollen. Geben Sie dann das Intervall (in Minuten) ein, in dem die Computer nach aktualisierter Software suchen sollen. Die Vorgabe lautet 5 Minuten.

Hinweis: Wenn die Computer Updates direkt von Sophos herunterladen, haben diese Intervalleinstellungen keine Auswirkung. Computer mit Sophos PureMessage können alle 15 Minuten nach Updates suchen. Computer ohne Sophos PureMessage werden alle 60 Minuten aktualisiert.

Bei Einwahl auf Updates prüfen

Wählen Sie diese Option, wenn die Computer Updates über eine Einwahlverbindung zum Internet durchführen. Computers will then attempt to update whenever they connect to the internet.

5. Klicken Sie im Fensterbereich **Richtlinien** auf die neue Update-Richtlinie und ziehen Sie diese auf die Computergruppe, die Sie konfigurieren möchten.

Hinweis: Wenn Sie nur eine Richtlinie bearbeitet haben, die bereits auf die Gruppe übertragen wurde (z.B. die Standardrichtlinie), müssen Sie Schritt 5 nicht durchführen.

20.3 Auswahl der Quelle für alte Updates

Bei rollenbasierter Verwaltung:

- Sie müssen über die Berechtigung **Richtlinieneinstellung – Updates** verfügen, um eine alte Richtlinie konfigurieren zu können.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Wenn sich Computer automatisch aktualisieren sollen, müssen Sie angeben, von wo aus sie die Updates herunterladen.

Hinweis: Sie müssen angeben, wo die einzelnen Computertypen (z.B. Windows 2000 und höher) Updates beziehen.

1. Prüfen Sie, welche alte Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.
Mehr dazu erfahren Sie unter [Welche Richtlinien sind einer Gruppe zugewiesen?](#) (Seite 25).
2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Alte Richtlinie einbeziehen**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.
3. Wählen Sie im Dialogfeld **Alte Update-Richtlinie** ein Betriebssystem. Klicken Sie auf **Konfigurieren**.

4. Klicken Sie im Dialogfeld **Update-Richtlinie festlegen** auf die Registerkarte **Primärserver**. Nehmen Sie die folgenden Einstellungen vor:

Adresse

Geben Sie die Adresse (UNC (Netzwerk)-Pfad oder Internetadresse) ein, von der Sophos Anti-Virus Updates herunterlädt. Eine Liste der Standard-Update-Verzeichnisse (zentralen Installationsverzeichnisse) finden Sie unter [Standardverzeichnisse für alte Updates](#) (Seite 119).

Benutzername

Falls erforderlich, geben Sie den **Benutzernamen** für das Konto ein, mit dem auf den Server zugegriffen wird, und geben Sie dann das **Kennwort** ein. Dieses Konto benötigt Leserechte für das Verzeichnis, das Sie in das Adressfeld eingegeben haben.

Hinweis: Falls der **Benutzername** auch eine Domäne erfordert, geben Sie ihn im Format Domäne\Benutzername ein.

Erweiterte Einstellungen und Proxy-Details

Wenn Sie die zu verwendende Bandbreite beschränken möchten, klicken Sie auf **Erweitert**. Mehr dazu erfahren Sie unter [Verringern der Bandbreite](#) (Seite 117).

Wenn Sie über einen Proxyserver auf die Update-Quelle zugreifen, klicken Sie auf **Proxyserver-Details**. Mehr dazu erfahren Sie unter [Angaben eines Proxyservers für alte Updates](#) (Seite 116). Bei einigen Internet Service Providern werden Internetanfragen an einen Proxyserver gesendet.

20.4 Angabe einer alternativen Quelle für alte Updates

Bei rollenbasierter Verwaltung:

- Sie müssen über die Berechtigung **Richtlinieneinstellung – Updates** verfügen, um eine alte Richtlinie konfigurieren zu können.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Sie können eine alternative Update-Quelle angeben. Wenn Computer keine Verbindung zur Haupt-Update-Quelle herstellen können, versuchen sie, Updates von der alternativen Quelle zu beziehen.

Sophos empfiehlt, dass Sie eine alternative Quelle für Updates einrichten, wenn Sie Computer haben, die nicht immer mit dem Unternehmensnetzwerk verbunden sind, z.B. Laptops.

Hinweis: Sie müssen angeben, wo die einzelnen Computertypen (z.B. Windows 2000 und höher) Updates beziehen.

1. Prüfen Sie, welche alte Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.
Mehr dazu erfahren Sie unter [Welche Richtlinien sind einer Gruppe zugewiesen?](#) (Seite 25).

2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Alte Richtlinie einbeziehen**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.
3. Wählen Sie im Dialogfeld **Alte Update-Richtlinie** ein Betriebssystem. Klicken Sie auf **Konfigurieren**.
4. Klicken Sie im Dialogfeld **Update-Richtlinie festlegen** auf die Registerkarte **Sekundärserver**. Wählen Sie **Sekundärserver festlegen**. Geben Sie dann die Details ein, wie nachfolgend erläutert.

Adresse

Geben Sie die **Adresse** (UNC (Netzwerk)-Pfad oder Internetadresse) ein, von der Computer Updates heruntergeladen werden sollen, wenn sie die andere Quelle nicht kontaktieren können. Wenn Sie Sophos wählen, lädt Sophos Anti-Virus Updates direkt von Sophos aus dem Internet herunter.

Benutzername

Falls erforderlich, geben Sie den **Benutzernamen** für das Konto ein, mit dem auf den Server zugegriffen wird, und geben Sie dann das **Kennwort** ein. Dieses Konto benötigt Leserechte für das Verzeichnis, das Sie in das Adressfeld eingegeben haben.

Hinweis: Falls der **Benutzername** auch eine Domäne erfordert, geben Sie ihn im Format Domäne\Benutzername ein.

Erweiterte Einstellungen und Proxy-Details

Wenn Sie die zu verwendende Bandbreite beschränken möchten, klicken Sie auf **Erweitert**. Mehr dazu erfahren Sie unter [Verringern der Bandbreite](#) (Seite 117).

Wenn Sie über einen Proxyserver auf die Update-Quelle zugreifen, klicken Sie auf **Proxyserver-Details**. Mehr dazu erfahren Sie unter [Angabe eines Proxyservers für alte Updates](#) (Seite 116). Bei einigen Internet Service Providern werden Internetanfragen an einen Proxyserver gesendet.

20.5 Zeitpläne für alte Updates

Bei rollenbasierter Verwaltung:

- Sie müssen über die Berechtigung **Richtlinieneinstellung – Updates** verfügen, um eine alte Richtlinie konfigurieren zu können.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Sie können festlegen, wann und wie oft Computer, die alte Updates beziehen, upgedatet werden.

Hinweis: Die Einstellungen müssen für alle Computertypen gesondert eingegeben werden (z.B. Windows 2000 und höher).

1. Prüfen Sie, welche alte Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.
Mehr dazu erfahren Sie unter [Welche Richtlinien sind einer Gruppe zugewiesen?](#) (Seite 25).

2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Alte Richtlinie einbeziehen**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.
3. Wählen Sie im Dialogfeld **Alte Update-Richtlinie** ein Betriebssystem. Klicken Sie auf **Konfigurieren**.
4. Klicken Sie im Dialogfeld **Update-Richtlinie festlegen** auf die Registerkarte **Zeitplan**. Geben Sie dann die Details, wie nachfolgend erläutert, ein.

Netzwerkcomputer können Sophos Updates automatisch herunterladen

Wählen Sie diese Option, wenn die Computer in regelmäßigen Intervallen aktualisiert werden sollen. Geben Sie dann das Intervall (in Minuten) ein, in dem die Computer nach aktualisierter Software suchen sollen. Die Vorgabe lautet 5 Minuten.

Hinweis: Wenn die Computer Updates direkt von Sophos herunterladen, haben diese Intervalleinstellungen keine Auswirkung. Computer mit Sophos PureMessage können alle 15 Minuten nach Updates suchen. Computer ohne Sophos PureMessage werden alle 60 Minuten aktualisiert.

Bei Einwahl auf Updates prüfen

Wählen Sie diese Option, wenn die Computer Updates über eine Einwahlverbindung zum Internet durchführen. Computers will then attempt to update whenever they connect to the internet.

20.6 Computer jetzt updaten

Bei rollenbasierter Verwaltung müssen Sie hierzu über die Berechtigung **Korrektur – Updates und Scans** verfügen. Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Sie können einen Computer oder mehrere Computer sofort updaten, ohne auf das automatische Update warten zu müssen.

1. Markieren Sie die Computer, die Sie aktualisieren möchten.
2. Rechtsklicken Sie auf die Auswahl und wählen Sie **Computer jetzt updaten**.

20.7 Updates bei Einwahl

Bei rollenbasierter Verwaltung:

- Sie müssen über die Berechtigung **Richtlinieneinstellung – Updates** verfügen, um eine alte Richtlinie konfigurieren zu können.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Wenn sich Computer, die alte Updates beziehen, immer dann updaten sollen, wenn eine Verbindung zum Internet hergestellt wird, verfahren Sie wie folgt:

Hinweis: Die Einstellungen müssen für alle Computertypen gesondert eingegeben werden (z.B. Windows 2000 und höher).

1. Prüfen Sie, welche alte Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.
Mehr dazu erfahren Sie unter [Welche Richtlinien sind einer Gruppe zugewiesen?](#) (Seite 25).
2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Alte Richtlinie einbeziehen**.
Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.
3. Wählen Sie im Dialogfeld **Alte Update-Richtlinie** ein Betriebssystem. Klicken Sie auf **Konfigurieren**.
4. Klicken Sie im Dialogfeld **Update-Richtlinie festlegen** auf die Registerkarte **Zeitplan**.
Wählen Sie **Bei Einwahl nach Updates suchen**.

20.8 Angeben eines Proxyservers für alte Updates

Bei rollenbasierter Verwaltung:

- Sie müssen über die Berechtigung **Richtlinieneinstellung – Updates** verfügen, um eine alte Richtlinie konfigurieren zu können.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Wenn die Computer Updates aus dem Internet beziehen, müssen Sie einen Proxyserver angeben, über den die Verbindung zum Internet hergestellt wird.

Hinweis: Die Einstellungen müssen für alle Computertypen gesondert eingegeben werden (z.B. Windows 2000 und höher).

1. Wenn Sie dies nicht bereits durchgeführt haben, prüfen Sie, welche alte Update-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten. (Mehr dazu erfahren Sie unter [Welche Richtlinien sind einer Gruppe zugewiesen?](#) (Seite 25).)
Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Alte Richtlinie einbeziehen**.
Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten. Wählen Sie im Dialogfeld **Alte Update-Richtlinie** ein Betriebssystem. Klicken Sie auf **Konfigurieren**.
2. Klicken Sie in der Registerkarte **Update-Richtlinie festlegen** je nach Bedarf auf die Registerkarte **Primärserver** oder **Sekundärserver**. Vergewissern Sie sich, dass alle eingegebenen Daten korrekt sind. Klicken Sie dann auf **Proxy-Details**.
3. Wählen Sie im Dialogfeld **Proxyserver-Details** die Option **Internetverbindung über Proxyserver herstellen** aus. Geben Sie anschließend die **Adresse** und den **Port** des Proxyservers an. Geben Sie die **Zugangsdaten** des Proxyservers ein. Wenn der Benutzername die Domäne enthalten muss, verwenden Sie die Form `domäne\benutzername`.

20.9 Verringern der Bandbreite

Bei rollenbasierter Verwaltung:

- Sie müssen über die Berechtigung **Richtlinieneinstellung – Updates** verfügen, um eine alte Richtlinie konfigurieren zu können.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Sie können die Bandbreite einschränken, die für die Updates verwendet wird. So steht auch noch Bandbreite für andere Zwecke zur Verfügung (z.B. zum Download von E-Mails).

Hinweis: Die Einstellungen müssen für alle Computertypen gesondert eingegeben werden (z.B. Windows 2000 und höher).

1. Wenn Sie dies nicht bereits durchgeführt haben, prüfen Sie, welche alte Update-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten. (Mehr dazu erfahren Sie unter [Welche Richtlinien sind einer Gruppe zugewiesen?](#) (Seite 25).) Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Alte Richtlinie einbeziehen**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten. Wählen Sie im Dialogfeld **Alte Update-Richtlinie** ein Betriebssystem. Klicken Sie auf **Konfigurieren**.
2. Klicken Sie im Dialogfeld **Update-Richtlinie festlegen** auf die Registerkarte **Primärserver** bzw. **Sekundärserver**. Vergewissern Sie sich, dass alle eingegebenen Daten korrekt sind. Klicken Sie dann auf **Erweitert**.
3. Wählen Sie im Dialogfeld **Erweiterte Einstellungen** die Option **Bandbreite verringern** und geben Sie mit Hilfe des Schiebereglers die Bandbreite in KBit/s an. Wenn Sie mehr Bandbreite angeben, als dem Computer zur Verfügung steht, wird für die Updates die verfügbare Bandbreite benutzt.

20.10 Ändern der Erstinstallationsquelle

Bei rollenbasierter Verwaltung:

- Sie müssen über die Berechtigung **Richtlinieneinstellung – Updates** verfügen, um eine alte Richtlinie konfigurieren zu können.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Standardmäßig wird auf den Computern Antiviren-Software installiert und von der Quelle aus (dem Primärserver) upgedatet, die Sie angegeben haben, als Sie die Computergruppe eingerichtet haben. Wenn Sie die Erstinstallation von einer anderen Quelle aus durchführen möchten, gehen Sie folgendermaßen vor:

Hinweis:

Diese Einstellung ist nur für Windows 2000 und höher relevant.

Wenn Ihr Primärserver eine HTTP (Internet)-Adresse ist und Sie die Installation auf den Computern von der Konsole aus durchführen möchten, müssen Sie eine Quelle für die Erstinstallation angeben.

1. Prüfen Sie, welche alte Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.
Mehr dazu erfahren Sie unter [Welche Richtlinien sind einer Gruppe zugewiesen?](#) (Seite 25).
2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Alte Richtlinie einbeziehen**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.
3. Wählen Sie im Dialogfeld **Alte Update-Richtlinie** ein Betriebssystem, z.B. Windows 2000 und höher. Klicken Sie auf **Konfigurieren**.
4. Klicken Sie im Dialogfeld **Update-Richtlinie festlegen** auf die Registerkarte **Erstinstallationsquelle**. Deaktivieren Sie die Option **Adresse des Primärservers übernehmen**. Geben Sie dann die Adresse der gewünschten Quelle ein.

20.11 Protokoll für alte Updates

Bei rollenbasierter Verwaltung:

- Sie müssen über die Berechtigung **Richtlinieneinstellung – Updates** verfügen, um eine alte Richtlinie konfigurieren zu können.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Sie können Computer so konfigurieren, dass ihre Update-Aktivität protokolliert wird.

Hinweis: Die Einstellungen müssen für alle Computertypen gesondert eingegeben werden (z.B. Windows 2000 und höher).

1. Prüfen Sie, welche alte Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.
Mehr dazu erfahren Sie unter [Welche Richtlinien sind einer Gruppe zugewiesen?](#) (Seite 25).
2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Alte Richtlinie einbeziehen**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.
3. Wählen Sie im Dialogfeld **Alte Update-Richtlinie** ein Betriebssystem. Klicken Sie auf **Konfigurieren**.

4. Klicken Sie im Dialogfeld **Einrichten der Update-Richtlinie** auf die Registerkarte **Protokoll**. Vergewissern Sie sich, dass **Sophos AutoUpdates protokollieren** ausgewählt ist. Setzen Sie dann die anderen Optionen, wie nachfolgend erläutert.

Maximale Protokollgröße

Geben Sie eine maximale Größe für das Protokoll in MB an.

Protokollgrad

Sie können zwischen der Einstellung **Normal** und **Ausführlich** wählen. In ausführlichen Protokollen werden mehr Aktivitäten protokolliert als gewöhnlich, was sich auch auf die Protokollgröße auswirkt. Verwenden Sie diese Einstellung nur, wenn Sie das ausführliche Protokoll zur Problembeseitigung benötigen.

20.12 Standardverzeichnisse für alte Updates

Wenn Sie die Standardeinstellungen beim Einrichten der Sophos EM Library übernommen haben, lauten die Verzeichnisse, von denen alle Produkte installiert und upgedatet werden, folgendermaßen:

Hinweis: Das Verzeichnis für „Sophos Endpoint Security and Control“ enthält den Installer für Sophos Anti-Virus, Sophos Client Firewall und Sophos NAC.

Sophos Endpoint Security and Control für Windows 2000/XP/2003/Vista	\\Servername\InterChk\SAVSCFXP
Sophos Anti-Virus für Windows 2000/XP/2003/Vista	\\Servername\InterChk\ESXP
Sophos Anti-Virus für Windows NT	\\Servername\InterChk\ESNT
Sophos Anti-Virus für Windows 95/98/Me	\\Servername\InterChk\ES9X
Sophos Anti-Virus für Mac OS X	\\Servername\InterChk\ESOSX
Sophos Anti-Virus für Linux	\\Servername\InterChk\savlinux
Sophos Anti-Virus für UNIX	\\Servername\InterChk\EESAVUNIX

21 Konfigurieren der Firewall-Richtlinie

21.1 Einrichten der Firewall

Die Firewall ist standardmäßig aktiviert und sperrt unnötigen Datenverkehr. Daher sollten regelmäßig genutzte Anwendungen in der Firewall zugelassen werden. Testen Sie die Einstellungen vor der Installation. Weitere Hinweise dazu finden Sie in der *Sophos Endpoint Security and Control – Richtlinienanleitung*.

Die Firewall-Einstellungen werden im Sophos Support-Artikel 57756 (<http://www.sophos.de/support/knowledgebase/article/57756.html>) näher beschrieben.

Nähere Informationen zum Vermeiden von Netzwerkbrücken finden Sie unter *Device Control* (Seite 149).

Wichtig: Wenn Sie eine neue oder aktualisierte Richtlinie auf Computer übertragen, werden Anwendungen, die von der alten Richtlinie zugelassen wurden, eventuell kurzfristig gesperrt, bis die neue Richtlinie in vollem Umfang angewendet wird. Sie sollten die Benutzer im Netzwerk über die Einführung neuer Richtlinien benachrichtigen.

Hinweis: Bei rollenbasierter Verwaltung:

- Zum Konfigurieren einer Firewall-Richtlinie müssen Sie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Nähere Informationen zur rollenbasierten Verwaltung können Sie dem Abschnitt *Rollen und Teilverwaltungseinheiten* (Seite 13) entnehmen.

So konfigurieren Sie die Firewall mit dem **Firewall-Richtlinienassistenten**:

1. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Firewall**.
2. Doppelklicken Sie auf die **Standardrichtlinie**, um sie zu ändern.

Der **Firewall-Richtlinienassistent** wird geöffnet.

3. Klicken Sie auf der Startseite des Assistenten auf **Weiter**.

Wenn Sie weitere Konfigurationsoptionen wünschen, klicken Sie auf **Erweiterte Einstellungen**. Mehr dazu erfahren Sie unter *Öffnen der erweiterten Konfiguration* (Seite 127).

4. Machen Sie auf der Seite **Firewall konfigurieren** Angaben zum Standort:

- 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. Für Laptops empfiehlt sich die Auswahl mehrerer Standorte.

5. Wenn Sie auf der vorherigen Seite die Option **Zwei Standorte** ausgewählt haben, konfigurieren Sie auf der Seite **Netzwerkidentifizierung** DNS- oder Gateway-Netzwerkerkennung.
- Enterprise Console wendet unterschiedliche Einstellungen auf Computer an, je nachdem, ob Computer mit dem Netzwerk verbunden sind oder nicht.
6. Geben Sie auf der Seite **Arbeitsmodus** an, wie die Firewall eingehenden und ausgehenden Datenfluss behandeln soll.

Modus	Beschreibung
Eingehenden und ausgehenden Datenfluss blockieren	<ul style="list-style-type: none"> ■ Standard. Bietet den höchsten Grad an Sicherheit. ■ Nur der unbedingt erforderliche Datenfluss wird von der Firewall zugelassen, und die Identität der Anwendungen wird mittels Prüfsummen authentifiziert. ■ Klicken Sie zum Zulassen der Kommunikation häufig eingesetzter Anwendungen in Ihrem Unternehmen über die Firewall auf Vertrauen. Weitere Informationen finden Sie unter Informationen zum Zulassen von Anwendungen (Seite 122).
Eingehenden Datenfluss blockieren, ausgehenden Datenfluss erlauben	<ul style="list-style-type: none"> ■ Diese Option bietet weniger Sicherheit als Eingehenden und ausgehenden Datenfluss blockieren. ■ Computer können ohne die Erstellung besonderer Regeln auf das Netzwerk und Internet zugreifen. ■ Alle Anwendungen dürfen über die Firewall kommunizieren.
Überwachen	<ul style="list-style-type: none"> ■ Überträgt die erstellten Regeln auf Datenfluss im Netzwerk. Wenn dem Datenfluss keine passende Regel zugewiesen wurde, wird dies der Konsole gemeldet. Wenn es sich um ausgehenden Datenfluss handelt, wird er zugelassen. ■ Auf diese Weise können Sie sich einen Überblick über die Verkehrssituation im Netzwerk verschaffen und geeignete Regeln erstellen, bevor Sie die Firewall für alle Computer wirksam machen. Weitere Informationen finden Sie unter Informationen zum Überwachungsmodus (Seite 122).
Benutzerdefiniert	<ul style="list-style-type: none"> ■ Durch Auswahl dieser Option können Sie die Konfiguration an Ihre Bedürfnisse anpassen. ■ Klicken Sie auf Erweitert, um die Firewall-Richtlinie zu konfigurieren. Anweisungen hierzu entnehmen Sie bitte dem Abschnitt zur Konfiguration der Firewall der Hilfe zu Sophos Endpoint Security and Control, 9.5.

7. Wählen Sie auf der Seite **Datei- und Druckerfreigabe** die Option **Datei- und Druckerfreigabe zulassen**, wenn Sie anderen Computern den Zugriff auf Drucker und Freigaben im Netzwerk ermöglichen möchten.

8. Wenn Sie die Option **Zwei Standorte** ausgewählt haben, konfigurieren Sie den Arbeitsmodus und die Datei- und Druckerfreigabe für den zweiten Standort (nicht im Netzwerk).

Nach der Konfiguration der Firewall können Sie Firewall-Ereignisse (z.B. von der Firewall gesperrte Anwendungen) in der **Firewall – Ereignisanzeige** aufrufen. Mehr dazu erfahren Sie unter [Anzeige von Firewall-Ereignissen](#) (Seite 64).

Im Dashboard wird die Anzahl der Computer angezeigt, deren Ereignisanzahl in den vergangenen 7 Tagen einen festgelegten Höchstwert überschritten hat.

21.2 Informationen zum Überwachungsmodus

Sie können den Überwachungsmodus auf Testcomputern aktivieren, auf denen Sie in der Firewall-Ereignisanzeige den Datenfluss und die Nutzung von Anwendungen beobachten können.

In der Ereignisanzeige können Sie Regeln zum Zulassen oder Blockieren von Datenfluss, Anwendungen und Prozessen erstellen. Dies wird unter [Erstellen einer Firewall-Regel](#) (Seite 125) beschrieben.

Hinweis: Wenn Sie in der Firewall-Ereignisanzeige eine Regel erstellen und sie zur Firewall-Richtlinie hinzufügen, ändert sich der Firewall-Modus von **Überwachen** in **Benutzerdefiniert**.

Tipp: Wenn unbekannter Datenfluss nicht standardmäßig zugelassen werden soll, verwenden Sie die Firewall im Lernmodus (bzw. interaktiven Modus). Mehr dazu erfahren Sie unter [Lernmodus](#) (Seite 124).

21.3 Informationen zum Zulassen von Anwendungen

Die Firewall blockiert aus Sicherheitsgründen Datenverkehr von Anwendungen auf dem Computer, die nicht erkannt wurden. Häufig verwendete Anwendungen in Ihrem Unternehmen werden jedoch möglicherweise gesperrt und einige Benutzer könnten dadurch von ihrer Arbeit abgehalten werden.

Sie können diese Anwendungen *zulassen*, damit sie über die Firewall kommunizieren können. Vertrauenswürdige Anwendungen erhalten uneingeschränkten Vollzugriff auf das Netzwerk und das Internet.

Hinweis: Über Anwendungsregeln können Sie Bedingungen für die Ausführung der Anwendung festlegen und somit die Sicherheit erhöhen. Anweisungen hierzu entnehmen Sie bitte dem Abschnitt **Anwendungsregeln** der Hilfe zu **Sophos Endpoint Security and Control, 9.5**.

21.4 Zulassen einer Anwendung

Bei rollenbasierter Verwaltung:

- Zum Konfigurieren einer Firewall-Richtlinie müssen Sie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen.

- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

So können Sie Anwendungen zulassen:

1. Wenn auf der Seite **Arbeitsmodus des Firewall-Richtlinienassistenten** der Standardmodus **Eingehenden und ausgehenden Datenfluss blockieren** ausgewählt ist, klicken Sie auf **Vertrauen**.
2. Klicken Sie im Dialogfeld **Firewall-Richtlinie** auf die Registerkarte **Anwendungen** und dann auf **Hinzufügen**.
3. Wählen Sie im Dialogfeld **Firewall-Richtlinie – Zuverlässige Anwendung hinzufügen** im Feld **Ereignistyp**, ob Sie eine geänderte Anwendung, eine neue Anwendung oder eine Anwendung, für die es noch keine Anwendungsregel in der Firewall-Richtlinie gibt, hinzufügen möchten.
4. Wählen Sie einen Eintrag für die Anwendung aus, die als vertrauenswürdig zugelassen werden soll. Klicken Sie auf **OK**.

Die Anwendung wird der Liste der vertrauenswürdigen Anwendungen im Dialogfeld **Firewall-Richtlinie** hinzugefügt.

5. Klicken Sie im Feld **Firewall-Richtlinie** auf **OK**.
6. Beenden Sie den **Firewall-Richtlinienassistenten**.

21.5 Zulassen der Datei- und Druckerfreigabe

Bei rollenbasierter Verwaltung:

- Zum Konfigurieren einer Firewall-Richtlinie müssen Sie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

So lassen Sie die Drucker- und Dateifreigabe im Netzwerk zu:

1. Prüfen Sie, welche Firewall-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.
Mehr dazu erfahren Sie unter [Welche Richtlinien sind einer Gruppe zugewiesen?](#) (Seite 25).
2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Firewall**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.

Der **Firewall-Richtlinienassistent** wird geöffnet.

3. Befolgen Sie die Anweisungen des Assistenten. Übernehmen Sie die vorhandene Konfiguration oder ändern passen Sie die Einstellungen an.
4. Wählen Sie auf der Seite **Datei- und Druckerfreigabe** die Option **Datei- und Druckerfreigabe zulassen** aus.

Hinweis: Diese Option gilt nicht für Standorte außerhalb des Unternehmensgebäudes.

5. Beenden Sie den Assistenten.

21.6 Zulassen einer gemeldeten oder gesperrten Anwendung

Bei rollenbasierter Verwaltung:

- Zum Konfigurieren einer Firewall-Richtlinie müssen Sie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Wenn die Firewall auf einem Netzwerkcomputer eine unbekannte Anwendung meldet oder sperrt, wird in der Firewall-Ereignisanzeige ein entsprechendes Ereignis angezeigt. In diesem Abschnitt erfahren Sie, wie eine Anwendung aus der Firewall-Ereignisanzeige zugelassen wird und die neue Regel auf die ausgewählten Firewall-Richtlinien übertragen wird.

So finden Sie gemeldete und/oder gesperrte Anwendungen in der Firewall-Ereignisanzeige und lassen sie zu oder erstellen neue Regeln für sie:

1. Klicken Sie im Menü **Ansicht** 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**.

Hinweis: Mit den erweiterten Firewall-Richtlinienkonfigurationseinstellungen können Sie auch eine Anwendung als vertrauenswürdig einstufen und in die Firewall-Richtlinie aufnehmen. Mehr dazu erfahren Sie unter [Erstellen einer Anwendungsregel aus einer Firewall-Richtlinie](#) (Seite 128).

21.7 Lernmodus

Bei rollenbasierter Verwaltung:

- Zum Konfigurieren einer Firewall-Richtlinie müssen Sie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Sie können die Firewall im Lernmodus (auch interaktiver Modus genannt) betreiben. Der Benutzer wird dabei gefragt, wie mit dem erkannten Datenverkehr umgegangen werden soll. Im Lernmodus wird auf dem Endpoint ein Lerndialog angezeigt, wenn eine unbekannte Anwendung oder ein unbekannter Dienst Netzwerkzugriff anfordert. Der Benutzer kann

angeben, ob Datenfluss zugelassen oder gesperrt werden soll oder ob eine Regel dafür erstellt werden soll.

So können Sie auf Computergruppen den Lernmodus der Firewall aktivieren:

1. Prüfen Sie, welche Firewall-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.
Mehr dazu erfahren Sie unter [Welche Richtlinien sind einer Gruppe zugewiesen?](#) (Seite 25).
2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Firewall**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.
Der **Firewall-Richtlinienassistent** wird geöffnet.
3. Klicken Sie auf der Startseite des Assistenten auf **Erweiterte Einstellungen**.
Das Dialogfenster **Firewall-Richtlinie** wird angezeigt.
4. Je nachdem, welcher Standort konfiguriert werden soll, klicken Sie auf die entsprechende **Konfigurieren**-Schaltfläche.
Es wird entweder das Dialogfenster **Primärer Standort** oder **Sekundärer Standort** angezeigt.
5. Klicken Sie auf der Registerkarte **Allgemein** unter **Arbeitsmodus** auf **Interaktiv** und klicken Sie auf **OK**.
6. Klicken Sie im Fenster **Firewall-Richtlinie** auf **OK**.
7. Beenden Sie den **Firewall-Richtlinienassistenten**.

21.8 Erstellen einer Firewall-Regel

Bei rollenbasierter Verwaltung:

- Zum Konfigurieren einer Firewall-Richtlinie müssen Sie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Sie können Regeln für alle Firewall-Ereignisse erstellen. Eine Ausnahme bilden Ereignisse vom Typ „Modifizierter Speicher“.

So können Sie eine Firewall-Regel erstellen:

1. Klicken Sie im Menü **Ansicht** auf **Firewall-Ereignisse**.
2. Wählen Sie im Dialogfeld **Firewall – Ereignisanzeige** ein Ereignis für die Anwendung aus, für die eine Regel erstellt werden soll, und klicken Sie auf **Regel erstellen**.
3. Wählen Sie im Dialogfeld eine Option aus, die für die Anwendung übernommen werden soll.

4. Bestimmen Sie, ob die Regel nur für den primären, den sekundären, oder für beide Standorte gelten soll. Wenn Sie den sekundären Standort oder beide Standorte auswählen, wird die Regel nur auf Richtlinien übertragen, für die ein sekundärer Standort konfiguriert wurde. Klicken Sie auf **OK**.

Hinweis: Die Ereignisse vom Typ „Neue Anwendung“ und „Geänderte Anwendung“ sind standortunabhängig und fügen Prüfsummen hinzu, die von beiden Standorten genutzt werden. Für diese Ereignisse lässt sich kein Standort auswählen.

5. Wählen Sie aus der Liste der Firewall-Richtlinien die Richtlinie(n) aus, die Sie in die Regel aufnehmen möchten. Klicken Sie auf **OK**.

Hinweis: Einer Richtlinie, die außerhalb der aktiven Teilverwaltungseinheit wirksam ist, lässt sich keine Regel zuweisen.

Hinweis: Wenn Sie eine Anwendungsregel anhand der erweiterten Firewall-Richtlinieneinstellungen aus einer Firewall-Richtlinie heraus erstellen möchten, lesen Sie [Erstellen einer Anwendungsregel aus einer Firewall-Richtlinie](#) (Seite 128).

21.9 Vorübergehende Deaktivierung der Firewall

Bei rollenbasierter Verwaltung:

- Zum Konfigurieren einer Firewall-Richtlinie müssen Sie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Die Firewall ist standardmäßig deaktiviert. Unter bestimmten Umständen (z.B. aus Wartungsgründen oder zur Fehlersuche) muss die Firewall vorübergehend deaktiviert werden.

So deaktivieren Sie die Firewall für eine Computergruppe:

1. Prüfen Sie, welche Firewall-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.

Mehr dazu erfahren Sie unter [Welche Richtlinien sind einer Gruppe zugewiesen?](#) (Seite 25).

2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Firewall**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.

Der **Firewall-Richtlinienassistent** wird geöffnet.

3. Auf der Startseite führen Sie folgende Schritte durch:

- Wenn die Firewall sowohl an allen festgelegten Standorten (also primäre und sekundäre) deaktiviert werden soll, klicken Sie auf **Weiter**. Wählen Sie auf der Seite **Firewall konfigurieren** die Option **Gesamten Verkehr zulassen (Firewall deaktiviert)**. Beenden Sie den Assistenten.

- Wenn Sie die Firewall nur an einem Standort (primär oder sekundär) deaktivieren wollen, klicken Sie auf **Erweiterte Einstellungen**. Wählen Sie im Fenster **Firewall-Richtlinie** neben **Primärer Standort** oder **Sekundärer Standort** die Option **Gesamten Datenfluss zulassen**. Klicken Sie auf **OK**. Beenden Sie den **Firewall-Richtlinienassistenten**.

Die Computer bleiben so lange ungeschützt, bis die Firewall wieder aktiviert wird. Zum Aktivieren der Firewall deaktivieren Sie das Kontrollkästchen **Gesamten Datenfluss zulassen**.

21.10 Einsatz der erweiterten Firewall-Konfiguration

21.10.1 Öffnen der erweiterten Konfiguration

Bei rollenbasierter Verwaltung:

- Zum Konfigurieren einer Firewall-Richtlinie müssen Sie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Wenn Sie die Firewall ausführlicher konfigurieren möchten, nutzen Sie die erweiterten Konfigurationseinstellungen.

So gelangen Sie zur erweiterten Konfiguration:

1. Doppelklicken Sie auf die zu ändernde Firewall-Richtlinie.
2. Klicken Sie auf der Startseite des **Firewall-Richtlinienassistenten** auf **Erweiterte Einstellungen**.

Das Dialogfenster **Firewall-Richtlinie** wird angezeigt. In diesem Fenster können Sie eine Konfiguration für einen sekundären Standort angeben, eine Standorterkennungsmethode festlegen, Anwendungsprüfsummen zur Firewall-Richtlinie hinzufügen und die Firewall-Protokollierung konfigurieren.

3. Klicken Sie im Fenster **Firewall-Richtlinie** neben dem Standort, für den die Firewall konfiguriert werden soll, auf **Konfigurieren**.

Es wird entweder das Dialogfenster **Primärer Standort** oder **Sekundärer Standort** angezeigt. In diesem Fenster können Sie Optionen festlegen, die für den ausgewählten Standort gelten. So können Sie z.B. Filter für ICMP-Nachrichten festlegen, LAN-Datenverkehr zulassen, globale Regeln und Anwendungsregeln hinzufügen.

Die erweiterten Firewall-Einstellungen werden ausführlich im entsprechenden Abschnitt der Hilfe zur Sophos Endpoint Security and Control 9 beschrieben. Die folgenden Abschnitte behandeln nur die Optionen, die sich jeweils auf Enterprise Console und auf den Endpoints unterscheiden.

- [Erstellen einer Anwendungsregel aus einer Firewall-Richtlinie](#) (Seite 128)

- [Hinzufügen einer Anwendungsprüfsumme](#) (Seite 129)

21.10.2 Erstellen einer Anwendungsregel aus einer Firewall-Richtlinie

Bei rollenbasierter Verwaltung:

- Zum Konfigurieren einer Firewall-Richtlinie müssen Sie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Mit den erweiterten Firewall-Richtlinieneinstellungen können Sie eine Anwendungsregel direkt aus einer Firewall-Richtlinie heraus erstellen.

So erstellen Sie eine Anwendungsregel aus einer Firewall-Richtlinie:

1. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.
2. Klicken Sie auf der Startseite des **Firewall-Richtlinienassistenten** auf **Erweiterte Einstellungen**.
3. Klicken Sie im Fenster **Firewall-Richtlinie** neben dem Standort, für den die Firewall konfiguriert werden soll, auf **Konfigurieren**.
4. Führen Sie einen der folgenden Schritte aus:
 - Wenn Sie eine Anwendung zur Firewall-Richtlinie hinzufügen möchten, öffnen Sie die Registerkarte **Anwendungen** und klicken Sie auf **Hinzufügen**.
 - Wenn eine Anwendung versteckte Prozesse starten dürfen soll, öffnen Sie die Registerkarte **Prozesse** und klicken Sie im oberen Bereich auf **Hinzufügen**.
 - Wenn eine Anwendung über Rawsockets auf das Netzwerk zugreifen dürfen soll, öffnen Sie die Registerkarte **Prozesse** und klicken Sie im unteren Bereich auf **Hinzufügen**.

Das Dialogfenster **Firewall-Richtlinie – Anwendung hinzufügen** wird angezeigt.

5. Wenn Sie eine Anwendung hinzufügen, wählen Sie im Feld **Ereignistyp**, ob Sie eine geänderte Anwendung, eine neue Anwendung oder eine Anwendung hinzufügen möchten, für die es in der Firewall-Richtlinie keine Anwendungsregel gibt.
6. Wählen Sie einen Eintrag für die Anwendung aus, die Sie hinzufügen möchten oder der das Starten versteckter Prozesse oder die Verwendung von Rawsockets gestattet werden soll. Klicken Sie auf **OK**.

Die Anwendung wird zur Firewall-Richtlinie hinzugefügt.

Wenn Sie auf der Registerkarte **Anwendungen** eine Anwendung hinzugefügt haben, wird die Anwendung als vertrauenswürdig hinzugefügt. Sie können sie jetzt sperren oder eine benutzerdefinierte Regel dafür erstellen.

Genauere Informationen zu den erweiterten Firewall-Optionen entnehmen Sie bitte dem entsprechenden Abschnitt der Hilfe zu Sophos Endpoint Security and Control 9.

21.10.3 Hinzufügen einer Anwendungsprüfsumme

Bei rollenbasierter Verwaltung:

- Zum Konfigurieren einer Firewall-Richtlinie müssen Sie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Jede Version einer Anwendung umfasst eine andere Prüfsumme. Mit Hilfe der Prüfsumme kann die Firewall entscheiden, ob eine Anwendung zugelassen oder gesperrt werden soll.

Standardmäßig prüft die Firewall die Prüfsumme aller laufenden Prozesse. Wenn die Prüfsumme unbekannt ist oder sich geändert hat, wird sie von der Firewall blockiert.

So fügen Sie eine neue Prüfsumme hinzu:

1. Doppelklicken Sie auf die zu ändernde Firewall-Richtlinie.
2. Klicken Sie auf der Startseite des **Firewall-Richtlinienassistenten** auf **Erweiterte Einstellungen**.
3. Öffnen Sie im Dialogfeld **Firewall-Richtlinie** die Registerkarte **Prüfsummen** und klicken Sie auf **Hinzufügen**.
4. Bestimmen Sie im Dialogfeld **Firewall-Richtlinie – Anwendungsprüfsumme hinzufügen** im Feld **Ereignistyp**, ob Sie eine Prüfsumme für eine geänderte oder eine neue Anwendung hinzufügen möchten.
5. Wählen Sie einen Eintrag für die Anwendung aus, für die eine Prüfsumme hinzugefügt werden soll. Klicken Sie auf **OK**.

Die Anwendungsprüfsumme wird der Liste der zugelassenen Prüfsummen im Dialogfeld **Firewall-Richtlinie** hinzugefügt.

6. Klicken Sie im Feld **Firewall-Richtlinie** auf **OK**.
7. Beenden Sie den **Firewall-Richtlinienassistenten**.

21.10.4 Hilfe für erweiterte Optionen

Genauere Informationen zu den Firewall-Optionen entnehmen Sie bitte dem entsprechenden Abschnitt der Hilfe zu Sophos Endpoint Security and Control 9.

22 Konfigurieren der Application Control-Richtlinie

22.1 Application Control

Mit Enterprise Console 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.

Anwendungen können für verschiedene Computergruppen völlig flexibel gesperrt oder zugelassen werden. Beispielsweise kann VoIP für Computer im Unternehmen ausgeschaltet, für Remote-Computer aber zugelassen werden.

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>).

In diesem Abschnitt wird beschrieben, wie Sie die Anwendungen auswählen, die Sie in ihrem Netzwerk kontrollieren möchten und Scans für Controlled Applications einrichten.

Hinweis: Bei rollenbasierter Verwaltung:

- Zur Konfiguration einer Application Control-Richtlinie müssen Sie über die Berechtigung **Richtlinieneinstellungen – Application Control** verfügen.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Nähere Informationen zur rollenbasierten Verwaltung können Sie dem Abschnitt *Rollen und Teilverwaltungseinheiten* (Seite 13) entnehmen.

Application Control-Ereignisse

Application Control-Ereignisse (z.B. eine erkannte Controlled Application im Netzwerk) werden im Application Control-Ereignisprotokoll verzeichnet und können in Enterprise Console aufgerufen werden. Mehr dazu erfahren Sie unter *Anzeigen von Application Control-Ereignissen* (Seite 62).

Im Dashboard wird die Anzahl der Computer angezeigt, deren Ereignisanzahl in den vergangenen 7 Tagen 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 167).

22.2 Wählen der Controlled Applications

Bei rollenbasierter Verwaltung:

- Zur Konfiguration einer Application Control-Richtlinie müssen Sie über die Berechtigung **Richtlinieneinstellungen – Application Control** verfügen.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

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

1. Prüfen Sie, welche Application Control-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.
Mehr dazu erfahren Sie unter [Welche Richtlinien sind einer Gruppe zugewiesen?](#) (Seite 25).
2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Application Control**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.
3. Klicken Sie im Dialogfeld **Application Control-Richtlinie** auf die Registerkarte **Autorisierung**.
4. 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 zu diesem Typ in Zukunft hinzufügt, verschieben Sie **Von Sophos zukünftig hinzugefügt** in die Liste **Blockiert**.
- Wenn Sie alle Anwendungen dieses Typs blockieren möchten, verschieben Sie alle Anwendungen aus der Liste **Zugelassen** in die Liste **Gesperrt**, indem Sie auf die Schaltfläche „Alle hinzufügen“ klicken.



5. Stellen Sie sicher, dass auf der Registerkarte **Scans** im Dialogfeld **Application Control-Richtlinie** die Überprüfung auf Controlled Applications aktiviert ist. (Mehr dazu erfahren Sie im Abschnitt [Scannen auf Controlled Applications](#) (Seite 131).) Klicken Sie **OK**.

22.3 Scannen auf Controlled Applications

Bei rollenbasierter Verwaltung:

- Zur Konfiguration einer Application Control-Richtlinie müssen Sie über die Berechtigung **Richtlinieneinstellungen – Application Control** verfügen.

- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Sie können Sophos Endpoint Security and Control dazu konfigurieren, Ihr Netzwerk bei Zugriff auf Controlled Applications zu scannen.

1. Prüfen Sie, welche Application Control-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.

Mehr dazu erfahren Sie unter [Welche Richtlinien sind einer Gruppe zugewiesen?](#) (Seite 25).

2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Application Control**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.

Das Dialogfeld **Application Control-Richtlinie** wird angezeigt.

3. Legen Sie auf der Registerkarte **Scans** folgende Optionen fest:

- Zur Aktivierung von On-Access-Scans markieren Sie die Option **On-Access-Scans aktivieren**. Wenn gestartete Anwendungen erkannt, aber nicht gesperrt werden sollen, markieren Sie die Option **Erkennen, aber laufen lassen**.
- Zum Aktivieren von On-Demand-Scans und geplanten Scans aktivieren Sie das Kontrollkästchen **On-Demand-Scans und geplante Scans aktivieren**.

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

Wenn Sie Controlled Applications entfernen möchten, die auf Ihren Netzwerkcomputern gefunden wurden, folgen Sie den Anweisungen im Abschnitt [Deinstallieren unerwünschter Controlled Applications](#) (Seite 132).

Sie können auch Benachrichtigungen an bestimmte Benutzer senden, wenn auf einem der Computer in der Gruppe eine Controlled Application entdeckt wurde. Anweisungen hierzu finden Sie unter [Einrichten von Application Control-Alerts](#) (Seite 167).

22.4 Deinstallieren unerwünschter 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 Methoden zum Entfernen von Anwendungen:

- Führen Sie an das Deinstallationsprogramm für das Produkt auf allen Computern aus. Dies erfolgt gewöhnlich über das Programm "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.

23 Konfigurieren der Data Control-Richtlinie

23.1 Data Control

Data Control überwacht und reguliert Dateien mit sensiblen Daten und verhindert so ungewollte Datenverluste über Computer. Sie können Data Control-Regeln erstellen und sie in die **Data Control**-Richtlinien aufnehmen.

Sie können die Übertragung von Dateien auf bestimmte Speichermedien (z.B. Wechselmedien und optische Laufwerke) oder den Transfer von Dateien von bestimmten Anwendungen (z.B. E-Mail-Programmen oder Browser) überwachen und regeln.

Zur Gewährleistung der prompten Definition und Bereitstellung einer Data Control-Richtlinie verfügen die SophosLabs über eine Datenbank mit Definitionen sensibler Daten (Content Control Lists). Die Datenbank umfasst hauptsächlich personenbezogene Daten, beinhaltet jedoch auch andere gängige Datenstrukturen. Wie nachfolgend beschrieben, können Sie Content Control Lists in Enterprise Console integrieren.

23.2 Funktionsweise von Data Control

Durch Data Control lassen sich unerwünschte Datenverluste feststellen, die in der Regel durch den falschen Umgang mit sensiblen Daten im Unternehmen verursacht werden. Beispiel: Ein Benutzer versendet eine Datei mit sensiblen Daten über ein Internet-E-Mail-Programm an eine private E-Mail-Adresse.

Data Control ermöglicht die Überwachung und Kontrolle von Dateiübertragungen von Computern auf Speichergeräte und Anwendungen, die mit dem Internet verbunden sind.

- **Speichergeräte:** Data Control fängt alle Dateien ab, die mit Windows Explorer auf ein überwachtes Speichergerät kopiert werden (einschließlich des Windows-Desktops). Dateien, die jedoch direkt in einer Anwendung (z.B. Microsoft Word) gespeichert oder über die Befehlszeile übertragen werden, werden nicht erfasst.

Über die beiden folgenden Optionen können Sie erzwingen, dass alle Übertragungen auf ein überwachtes Speichergerät mit Windows Explorer erfolgen: **Benutzerbestätigte Übertragungen zulassen und Ereignis protokollieren** oder **Übertragung sperren und Ereignis protokollieren**. Bei Auswahl beider Optionen blockiert Data Control Versuche, Dateien direkt in einer Anwendung zu speichern oder über die Befehlszeile zu übertragen. Der Benutzer wird in einer Desktop-Benachrichtigung aufgefordert, die Übertragung mit Windows Explorer durchzuführen.

Wenn eine Data Control-Richtlinie nur Regeln mit der Maßnahme **Dateiübertragung zulassen und Ereignis protokollieren** umfasst, greift Data Control nicht beim Speichern in einer Anwendung oder der Übertragung über die Befehlszeile. Benutzer können Speichergeräte somit uneingeschränkt nutzen. Bei Übertragungen mit Windows Explorer werden jedoch weiterhin Data Control-Ereignisse protokolliert.

Hinweis: Diese Einschränkung gilt nicht für die Überwachung von Anwendungen.

- **Anwendungen:** Damit nur von Benutzern eingeleitete Dateiübertragungen überwacht werden, werden einige Systemdateiverzeichnisse von Data Control ausgeschlossen. Auf

diese Weise wird die Anzahl der Data Control-Ereignisse auf Dateiübertragungen vonseiten der Benutzer reduziert; von Anwendungen geöffnete Konfigurationsdateien lösen keine Data Control-Ereignisse mehr aus.

Wichtig: Sollte eine Anwendung beim Öffnen einer Konfigurationsdatei dennoch ein Ereignis auslösen, kann das Problem in der Regel durch das Ausschließen bestimmter Verzeichnisse oder durch Desensibilisierung der Data Control-Regel behoben werden. Weitere Informationen finden Sie im Support-Artikel 63016 (<http://www.sophos.de/support/knowledgebase/article/63016.html>).

Data Control-Richtlinien

Data Control dient der Überwachung und Kontrolle des Datenverkehrs durch Festlegen von Data Control-Richtlinien und deren Übertragung auf Netzwerkgruppen und -computer.

Wichtig: Data Control läuft nicht unter Windows 2008 Server Core. Daher muss diese Funktion auf Computern mit diesem Betriebssystem deaktiviert werden. Um Computer mit Windows 2008 Server Core von Data Control auszuschließen, gliedern Sie diese in eine Gruppe ein, in deren Data Control-Richtlinie diese Funktion deaktiviert ist. Mehr dazu erfahren Sie unter [Aktivieren/Deaktivieren von Data Control](#) (Seite 138).

Data Control-Richtlinien umfassen eine oder mehrere Data Control-Regeln, in denen die Zustände definiert werden, die Data Control erkennen soll. Außerdem sind die zu ergreifenden Maßnahmen für den Fall festgelegt, dass eine Übereinstimmung mit der Regel vorliegt. Eine Data Control-Regel kann mehreren Richtlinien angehören.

Wenn eine Data Control-Richtlinie mehrere Regeln umfasst, liegt bereits ein Richtlinienverstoß vor, wenn eine Datei die Kriterien *einer* Regel der Data Control-Richtlinie erfüllt.

Data Control-Regelbedingungen

Die Data Control-Richtlinien umfassen Ziel, Dateiname, Erweiterung, Dateityp und Inhalt der Datei.

Ziele umfassen Geräte (z.B. Wechselmedien wie etwa USB-Flashlaufwerke) und Anwendungen (z.B. Internet-Browser oder E-Mail-Clients).

Der Abgleich von Dateiinhalten wird über Content Control Lists definiert. Hierbei handelt es sich um die Beschreibung strukturierter Daten auf XML-Basis. SophosLabs stellen eine Vielzahl an Content Control Lists bereit, die sich in Data Control-Regeln integrieren lassen.

Weitere Informationen zu Data Control-Regeln und Bedingungen, die für Dateien gelten, finden Sie unter [Data Control-Regeln](#) (Seite 136).

Mehr zu Content Control Lists (CCLs) zur Definition von Dateiinhalten erfahren Sie unter [Content Control Lists](#) (Seite 136).

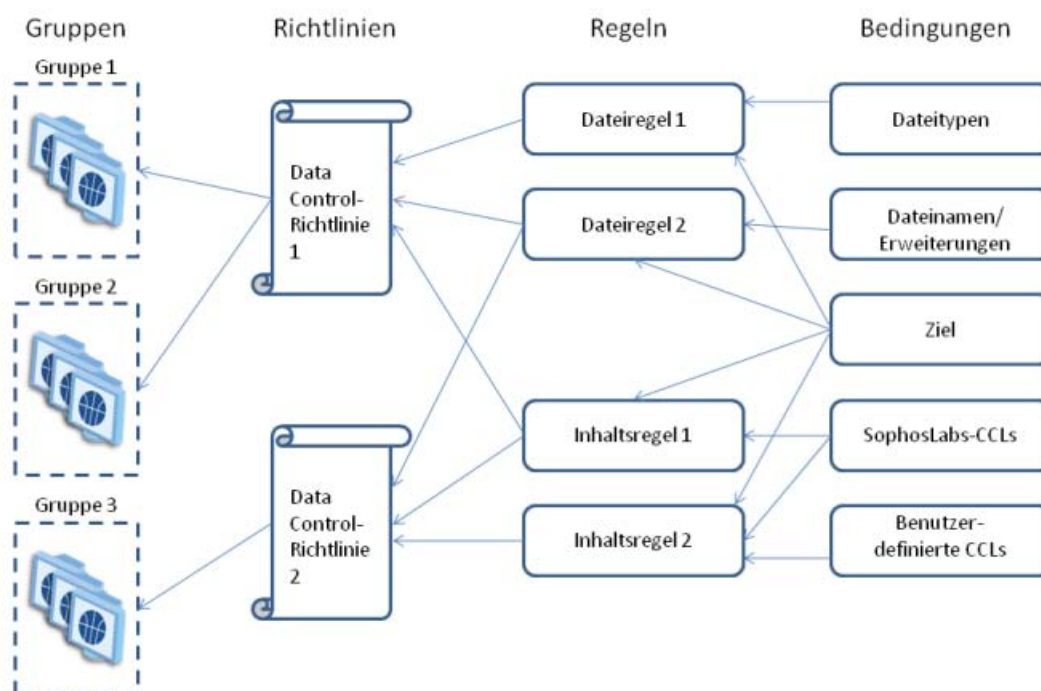


Abbildung 5: Data Control

Data Control-Regelmaßnahmen

Wenn Data Control alle in einer Regel festgelegten Bedingungen vorfindet, liegt eine Übereinstimmung mit der Regel vor. Data Control ergreift dann die in der Regel bestimmten Maßnahmen und verzeichnet das Ereignis im Protokoll. Sie können eine der folgenden Maßnahmen festlegen:

- Dateiübertragung zulassen und Ereignis protokollieren
- Benutzerbestätigte Übertragungen zulassen und Ereignis protokollieren
- Übertragung sperren und Ereignis protokollieren

Wenn eine Datei zwei Data Control-Regeln entspricht, greift die Regel mit der strengeren Maßnahme. Data Control-Regeln, die die Dateiübertragung blockieren, haben Vorrang vor Regeln, die die Dateiübertragung bei entsprechender Bestätigung durch den Benutzer erlauben. Regeln, die die Dateiübertragung bei entsprechender Bestätigung durch den Benutzer erlauben, haben wiederum Vorrang vor Regeln, die die Dateiübertragung zulassen.

Wenn eine Übereinstimmung mit einer Regel vorliegt und die Übertragung einer Datei gesperrt wird bzw. vom Benutzer bestätigt werden muss, wird standardmäßig eine Desktop-Benachrichtigung auf dem Endpoint angezeigt. Die Benachrichtigung weist auch auf die entsprechende Regel hin. Sie können Ihre eigenen Benachrichtigungen für blockierte Dateiübertragungen und für den Fall erstellen, dass der Benutzer die Dateiübertragung bestätigen soll. Weitere Informationen finden Sie unter [Einrichten von Data Control-Alerts](#) (Seite 167).

23.3 Data Control-Regeln

In Data Control-Regeln werden die Bedingungen festgelegt, die Data Control erkennen soll. Ferner werden bei Regelübereinstimmung zu ergreifende Maßnahmen definiert und bestimmt, welche Dateien ggf. von Scans ausgeschlossen werden sollen.

Sie können eigene Regeln erstellen oder die vordefinierten Data Control-Regeln von Sophos übernehmen. Sophos bietet vordefinierte Data Control-Regeln, die Sie nach Belieben an Ihre Bedürfnisse anpassen können. Die Regeln dienen lediglich der Veranschaulichung und werden nicht von Sophos aktualisiert.

Es wird zwischen *Dateiregeln* und *Inhaltsregeln* unterschieden.

Dateiregeln

In *Dateiregeln* wird die Maßnahme (z.B. Datenübertragung an Wechselmedien blockieren) festgelegt, die ergriffen wird, wenn ein Benutzer versucht, eine Datei eines bestimmten Namens oder Typs (True File Type, z.B. eine Tabelle) an ein angegebenes Ziel zu übertragen.

Data Control umfasst True-File-Type-Definitionen für über 150 verschiedene Dateiformate. Die Liste wird unter Umständen noch ergänzt. Neue Dateitypen werden automatisch in die Data Control-Regeln der entsprechenden True-File-Type-Kategorie aufgenommen.

Dateitypen, die nicht von der True-File-Type-Definiton erfasst werden, lassen sich anhand ihrer Erweiterung bestimmen.

Inhaltsregeln

Inhaltsregeln umfassen mindestens eine Content Control List. Hierin wird die Maßnahme festgelegt, die ergriffen wird, wenn ein Benutzer versucht, Daten, die mit allen Content Control Lists übereinstimmen, an den angegebenen Zielort zu übertragen.

23.4 Content Control Lists

Content Control Lists (CCL) umfassen Bedingungen zur Beschreibung strukturierter Dateiinhalte. Content Control Lists können sich auf einen Datentyp beschränken (z.B. eine Anschrift oder Sozialversicherungsnummer) oder eine Kombination verschiedener Daten umfassen (z.B. Projektnamen, die „vertraulich“ oder ähnlich lauten).

Sie können auf die von Sophos bereitgestellten *SophosLabs Content Control Lists* zurückgreifen oder eigene Content Control Lists erstellen.

SophosLabs Content Control Lists umfassen Definitionen zu gängigen finanziellen und personenbezogenen Datentypen (z.B. Kreditkartennummern, Sozialversicherungsnummern, Anschriften oder E-Mail-Adressen). Die Präzision der Erkennung sensibler Daten in SophosLabs Content Control Lists wird durch den Einsatz diverser Technologien, wie etwa Prüfsummen, optimiert.

SophosLabs Content Control Lists können nicht bearbeitet werden. Auf Wunsch können Sie jedoch die Erstellung einer neuen SophosLabs Content Control List bei Sophos beantragen.

Nähere Informationen finden Sie im Support-Artikel **51976** (<http://www.sophos.de/support/knowledgebase/article/51976.html>).

Hinweis: Double-Byte-Zeichen (z.B. japanische oder chinesische Zeichen) werden in der aktuellen Version der Content Control Lists nicht offiziell unterstützt. Im Content Control List Editor können Sie jedoch Double-Byte-Zeichen eingeben.

Mengenfestlegung für SophosLabs Content Control Lists

Den meisten SophosLabs Content Control Lists wurden *Mengenwerte* zugewiesen.

Mengen definieren sich als der Umfang an Content Control List-Schlüsseldaten, die eine Datei umfassen muss, damit eine Übereinstimmung mit der Content Control List vorliegt. Sie können den Mengenwert einer SophosLabs Content Control List in einer Dateiregel ändern, die die Content Control List umfasst.

Mit Mengenwerten können Sie Data Control an Ihre Bedürfnisse anpassen und so vermeiden, dass Dokumente gesperrt werden, die keine sensiblen Daten enthalten (z.B. ein Dokument, das eine Anschrift und eine oder zwei Telefonnummern in der Kopf- oder Fußzeile umfasst). Wenn Sie nur nach einer Anschrift suchen, liegt möglicherweise bei zahlreichen Dokumenten eine Regelübereinstimmung vor, und es werden entsprechend viele Data Control-Ereignisse angezeigt. Um jedoch den Verlust wichtiger Kundendaten zu vermeiden, empfiehlt sich etwa, lediglich die Übertragung von Dokumenten mit 50 Anschriften und mehr zu sperren. In anderen Fällen kann es sich wiederum anbieten, nur nach einem Datenvorkommen zu suchen (z.B. einer Kreditkartennummer).

23.5 Data Control-Ereignisse

Data Control-Ereignisse (z.B. Kopieren einer Datei mit sensiblen Daten auf ein USB-Flash-Laufwerk) werden an Enterprise Console übermittelt und können in der **Ereignisanzeige von Data Control** angezeigt werden. Die Ereignisse werden auch auf dem Endpoint protokolliert. Benutzer, die über die erforderlichen Rechte verfügen, können die Ereignisse in Endpoint Security and Control aufrufen.

Hinweis: Endpoints können bis zu 50 Data Control-Ereignisse pro Stunde an Enterprise Console senden. Alle Ereignisse werden lokal auf dem Endpoint protokolliert.

Im Dialogfeld **Data Control – Ereignisanzeige** können Sie Filter anlegen und sich nur Ereignisse anzeigen lassen, die für Sie relevant sind. Außerdem können Sie die Liste der Data Control-Ereignisse in eine Datei exportieren oder in die Zwischenablage kopieren. Mehr dazu können Sie im Abschnitt „Anzeige von Ereignissen“ nachlesen.

Auf dem Dashboard wird die Anzahl der Computer angezeigt, auf denen die Summe der Data Control-Ereignisse in den vergangenen 7 Tagen den angegebenen Höchstwert überschritten hat. Nähere Informationen zum Festlegen des Höchstwerts finden Sie im Abschnitt [Konfigurieren des Dashboards](#) (Seite 51).

Zudem können Sie festlegen, dass die gewählten Empfänger über Data Control-Ereignisse benachrichtigt werden. Mehr dazu erfahren Sie unter [Einrichten von Data Control-Alerts](#) (Seite 167).

23.6 Aktivieren/Deaktivieren von Data Control

Bei rollenbasierter Verwaltung:

- Zum Konfigurieren einer Device Control-Richtlinie ist die Berechtigung **Richtlinieneinstellung – Data Control** erforderlich.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Data Control ist standardmäßig deaktiviert und die Dateiübertragung im Netzwerk wird nicht durch Regeln überwacht bzw. eingeschränkt.

So aktivieren Sie Data Control:

1. Prüfen Sie, welche Data Control-Richtlinie von der/den Computergruppe/n verwendet wird, die Sie konfigurieren möchten.
Mehr dazu erfahren Sie unter [Welche Richtlinien sind einer Gruppe zugewiesen?](#) (Seite 25).
2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Data Control**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.
Das Dialogfeld **Data Control-Richtlinie** wird angezeigt.
3. Aktivieren Sie auf der Registerkarte **Richtlinienregeln** das Kontrollkästchen **Data Control aktivieren**.
4. Klicken Sie auf die Schaltfläche **Regel hinzufügen**. Wählen Sie im Dialogfeld **Verwaltung der Data Control-Regeln** die Regeln aus, die Sie zu der Richtlinie hinzufügen möchten und klicken Sie auf **OK**.

Wichtig: Solange Sie keine Data Control-Regeln hinzufügen, werden Dateien nicht von Data Control überwacht.

Wenn Sie Data Control zu einem späteren Zeitpunkt deaktivieren möchten, deaktivieren Sie das Kontrollkästchen **Data Control aktivieren**.

23.7 Erstellen einer Dateiregel

Bei rollenbasierter Verwaltung:

- Zum Erstellen bzw. Ändern von Dateiregeln für Data Control müssen Sie über die Berechtigung **Data Control – Anpassung** verfügen.
- Zum Einrichten von Data Control-Richtlinien müssen Sie über die Berechtigung **Richtlinieneinstellungen – Data Control** verfügen.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Eine Übersicht über Dateiregeln finden Sie unter [Data Control-Regeln](#) (Seite 136).

So können Sie eine Dateiregel erstellen und zu einer Data Control-Richtlinie hinzufügen:

1. Prüfen Sie, welche Data Control-Richtlinie von der/den Computergruppe/n verwendet wird, die Sie konfigurieren möchten.
Mehr dazu erfahren Sie unter [Welche Richtlinien sind einer Gruppe zugewiesen?](#) (Seite 25).
Sie können jedoch auch eine Regel im Menü **Extras** erstellen und sie zu einem späteren Zeitpunkt zu einer oder mehreren Richtlinien hinzufügen. Richten Sie den Mauszeiger im **Extras**-Menü auf **Data Control**. Klicken Sie anschließend auf die Option **Data Control-Regeln** und führen Sie die Schritte 4 bis 10 durch.
2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Data Control**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.
3. Öffnen Sie im Dialogfeld **Data Control-Richtlinie** die Registerkarte **Richtlinienregeln**. Wählen Sie die Option **Data Control aktivieren** und klicken Sie anschließend auf **Regeln verwalten**.
4. Klicken Sie im Dialogfeld **Verwaltung der Data Control-Regeln** auf die Option **Dateiregel hinzufügen**.
5. Geben Sie im Dialogfeld **Dateiregel erstellen** unter **Regelname** einen Regelnamen ein.
6. Im Bereich **Beschreibung der Regel (optional)** können Sie die Regel auf Wunsch beschreiben.
7. Legen Sie im Bereich **Regelbedingungen**: die gewünschten Regelbedingungen fest.
Die Zielbedingung ist vordefiniert und muss Bestandteil der Regel sein.
Standardmäßig werden alle Dateitypen gescannt. Wenn nur bestimmte Dateitypen gescannt werden sollen, klicken Sie auf **Dateityp ist**. Nun können Sie die Bedingung an Ihre Wünsche anpassen (siehe Schritt 10).
8. Wählen Sie im Bereich **Maßnahme bei erfüllter Regelbedingung**: die gewünschte Maßnahme aus.
9. Wenn Dateien nicht von Data Control erfasst werden sollen, aktivieren Sie im Bereich **Dateiausschlüsse**: das Kontrollkästchen **Datei deckt sich mit** oder **Dateityp ist**.

10. Klicken Sie im Bereich **Regelinhalt** alle unterstrichenen Werte an und legen Sie die Regelbedingungen fest.
Wenn Sie beispielsweise auf **Ziel auswählen** klicken, öffnet sich das Dialogfeld **Zieltypbedingung**. In diesem Feld können Sie Geräte und/oder Anwendungen auswählen, zu denen der Datenverkehr eingeschränkt werden soll.

Wählen Sie Bedingungen für alle unterstrichenen Werte aus bzw. geben Sie diese ein.

Klicken Sie auf **OK**.

Die neue Regel wird im Dialogfeld **Verwaltung der Data Control-Regeln** angezeigt.

11. Aktivieren Sie zum Hinzufügen der Regel zur Richtlinie das Kontrollkästchen neben dem Regelnamen und klicken Sie auf **OK**.

Die Regel wird zur Data Control-Richtlinie hinzugefügt.

Sie können Alerts und Benachrichtigungen an den Benutzer senden, wenn eine Übereinstimmung mit einer Regel in der Data Control-Richtlinie vorliegt. Mehr dazu erfahren Sie unter [Einrichten von Data Control-Alerts](#) (Seite 167).

23.8 Erstellen einer Inhaltsregel

Bei rollenbasierter Verwaltung:

- Zum Erstellen bzw. Ändern von Dateiregeln und Content Control Lists für Data Control müssen Sie über die Berechtigung **Data Control – Anpassung** verfügen.

- Zum Einrichten von Data Control-Richtlinien müssen Sie über die Berechtigung **Richtlinieneinstellungen – Data Control** verfügen.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Eine Übersicht über Inhaltsregeln und Content Control Lists finden Sie unter [Data Control-Regeln](#) (Seite 136).

So können Sie eine Inhaltsregel erstellen und zu einer Data Control-Richtlinie hinzufügen:

1. Prüfen Sie, welche Data Control-Richtlinie von der/den Computergruppe/n verwendet wird, die Sie konfigurieren möchten.
Mehr dazu erfahren Sie unter [Welche Richtlinien sind einer Gruppe zugewiesen?](#) (Seite 25).
Sie können jedoch auch eine Regel im Menü **Extras** erstellen und sie zu einem späteren Zeitpunkt zu einer oder mehreren Richtlinien hinzufügen. Richten Sie den Mauszeiger im **Extras**-Menü auf **Data Control**. Klicken Sie anschließend auf die Option **Data Control-Regeln** und führen Sie die Schritte 4 bis 13 durch.
2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Data Control**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.
3. Öffnen Sie im Dialogfeld **Data Control-Richtlinie** die Registerkarte **Richtlinienregeln**. Wählen Sie die Option **Data Control aktivieren** und klicken Sie anschließend auf **Regeln verwalten**.
4. Klicken Sie im Dialogfeld **Verwaltung der Data Control-Regeln** auf die Option **Inhaltsregel hinzufügen**.
5. Geben Sie im Dialogfeld **Dateiregel erstellen** unter **Regelname** einen Regelnamen ein.
6. Im Bereich **Beschreibung der Regel (optional)** können Sie die Regel auf Wunsch beschreiben.
7. Im Bereich **Regelbedingungen** sind die Dateinhalt- und Zielbedingungen bereits ausgewählt. Für eine Inhaltsregel müssen Sie beide Bedingungen festlegen.
8. Wählen Sie im Bereich **Maßnahme bei erfüllter Regelbedingung**: die gewünschte Maßnahme aus.
9. Wenn Dateien nicht von Data Control erfasst werden sollen, aktivieren Sie im Bereich **Dateiausschlüsse**: das Kontrollkästchen **Datei deckt sich mit** oder **Dateityp ist**.
10. Klicken Sie im Bereich **Regelinhalt** auf den unterstrichenen Wert „Dateinhalt auswählen“.
11. Wählen Sie im Dialogfeld **Content Control List – Verwaltung** die Content Control Lists aus, die Sie in die Regel aufnehmen möchten.
Wenn Sie eine SophosLabs Content Control-Liste erstellen möchten, wählen Sie die Liste für Ihr Land oder eine globale Content Control List aus.
Anweisungen zum Erstellen einer neuen Content Control List finden Sie unter [Erstellen/Ändern einer einfachen Content Control List](#) (Seite 145) und [Erstellen/Ändern einer komplexen Content Control List](#) (Seite 146).
Klicken Sie auf **OK**.

12. Wenn Sie die Menge ändern möchten, die einer SophosLabs Content Control List zugewiesen ist, klicken Sie unter **Regelinhalt** auf den unterstrichenen „Menge“-Wert, den Sie ändern möchten. Geben Sie im Dialogfeld **Mengen-Editor** einen neuen Mengenwert ein.
13. Wählen Sie im Bereich **Regelinhalt** Bedingungen für die verbleibenden unterstrichenen Werte aus bzw. geben Sie sie ein.

Klicken Sie auf **OK**.

Die neue Regel wird im Dialogfeld **Verwaltung der Data Control-Regeln** angezeigt.

14. Aktivieren Sie zum Hinzufügen der Regel zur Richtlinie das Kontrollkästchen neben dem Regelnamen und klicken Sie auf **OK**.

Die Regel wird zur Data Control-Richtlinie hinzugefügt.

Sie können Alerts und Benachrichtigungen an den Benutzer senden, wenn eine Übereinstimmung mit einer Regel in der Data Control-Richtlinie vorliegt. Mehr dazu erfahren Sie unter [Einrichten von Data Control-Alerts](#) (Seite 167).

23.9 Hinzufügen einer Data Control-Regel zu einer Richtlinie

Bei rollenbasierter Verwaltung:

- Hierzu müssen Sie über die Berechtigung **Richtlinieneinstellung – Data Control** verfügen.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

So fügen Sie einer Richtlinie eine Data Control-Regel hinzu:

1. Prüfen Sie, welche Data Control-Richtlinie von der/den Computergruppe/n verwendet wird, die Sie konfigurieren möchten.
Mehr dazu erfahren Sie unter [Welche Richtlinien sind einer Gruppe zugewiesen?](#) (Seite 25).
2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Data Control**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.
Das Dialogfeld **Data Control-Richtlinie** wird angezeigt.
3. Klicken Sie im Fenster **Richtlinienregeln** auf **Hinzufügen**.
Das Dialogfeld **Verwaltung der Data Control-Regeln** wird angezeigt.
4. Wählen Sie die gewünschten Regeln aus und klicken Sie auf **OK**.

23.10 Entfernen einer Data Control-Regel aus einer Richtlinie

Bei rollenbasierter Verwaltung:

- Hierzu müssen Sie über die Berechtigung **Richtlinieneinstellung – Data Control** verfügen.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

So entfernen Sie eine Data Control-Regel aus einer Richtlinie:

1. Prüfen Sie, welche Data Control-Richtlinie von der/den Computergruppe/n verwendet wird, die Sie konfigurieren möchten.
Mehr dazu erfahren Sie unter [Welche Richtlinien sind einer Gruppe zugewiesen?](#) (Seite 25).
2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Data Control**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.
Das Dialogfeld **Data Control-Richtlinie** wird angezeigt.
3. Wählen Sie auf der Registerkarte **Richtlinienregeln** die Regel aus, die Sie löschen möchten, und klicken Sie auf **Entfernen**.

23.11 Ausschließen von Dateien oder Dateitypen aus Data Control

Bei rollenbasierter Verwaltung gilt als Voraussetzung für das Ausschließen von Dateien aus Data Control die Berechtigung **Data Control – Anpassung**. Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Wenn Sie Dateien und Dateitypen von Data Control ausschließen möchten, müssen Sie in einer Data Control-Regel Ausnahmen definieren.

Schließen Sie Dateien bzw. Dateitypen in Regeln mit höchster Priorität (d.h. mit den strengsten Maßnahmen) aus.

So schließen Sie Dateien oder Dateitypen aus Data Control aus:

1. Wählen Sie im Menü **Extras** unter **Data Control** die Option **Data Control-Regeln**.
2. Wählen Sie im Dialogfeld **Verwaltung der Data Control-Regeln** die zu ändernde Regel aus und klicken Sie auf **Ändern**. Sie können jedoch auch per Klick auf **Dateiregel hinzufügen** oder **Inhaltsregel hinzufügen** eine neue Regel erstellen.
3. Aktivieren Sie im **Regel-Editor** unter **Dateiausschlüsse** das Kontrollkästchen **Datei deckt sich mit**.
4. Klicken Sie im Bereich **Regelinhalt** auf den unterstrichenen Wert, um die Namen der auszuschließenden Dateien anzugeben.
5. Klicken Sie im Dialogfeld **Dateinamensbedingung ausschließen** auf **Hinzufügen** und geben Sie die Namen der Dateien an, die Sie ausschließen möchten.

Sie können die Platzhalter * und ? benutzen.

Der Platzhalter ? kann nur für Dateinamen oder Erweiterungen benutzt werden. Er ersetzt in der Regel ein einziges Zeichen. Am Ende eines Dateinamens kann das Fragezeichen jedoch auch ein fehlendes Zeichen ersetzen. Beispiel: Die Eingabe von „datei?.txt“ dient als Ersatz für „datei.txt“, „datei1.txt“ sowie „datei12.txt“, jedoch nicht „datei123.txt“.

Der Platzhalter * kann nur für Dateinamen oder -erweiterungen in der Form *[Dateiname].** oder **.[Erweiterung]* verwendet werden. Beispiel: Die Eingabe von „datei*.txt“, „datei.txt*“ und „datei.*txt“ ist nicht zulässig.

6. Aktivieren Sie im **Regel-Editor** unter **Dateiausschlüsse** das Kontrollkästchen **Dateityp ist**.
7. Klicken Sie im Bereich **Regelinhalt** auf den unterstrichenen Wert, um die auszuschließenden Dateitypen anzugeben.
8. Wählen Sie im Dialogfeld **Dateinamensbedingung ausschließen** die auszuschließenden Dateitypen und klicken Sie auf **OK**.

23.12 Importieren/Exportieren einer Data Control-Regel

Bei rollenbasierter Verwaltung gilt als Voraussetzung für das Importieren/Exportieren einer Data Control-Regel die Berechtigung **Data Control – Anpassung**. Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Data Control-Regeln können als XML-Dateien importiert bzw. exportiert werden.

So importieren/exportieren Sie eine Data Control-Regel:

1. Richten Sie den Mauszeiger im Menü **Extras** auf **Data Control**. Klicken Sie anschließend auf die Option **Data Control-Regeln**.
2. Klicken Sie im Dialogfeld **Verwaltung der Data Control-Regeln** auf die Option **Importieren** oder **Exportieren**.
 - Suchen Sie zum Importieren einer Regel die gewünschte Regel im Dialogfeld **Importieren**, wählen Sie die Regel aus und klicken Sie auf **Öffnen**.
 - Wählen Sie zum Exportieren einer Regel im Dialogfeld **Exportieren** einen Speicherort für die Datei aus, geben Sie der Datei einen Namen und klicken Sie auf **Speichern**.

23.13 Erstellen/Ändern einer einfachen Content Control List

Bei rollenbasierter Verwaltung gilt als Voraussetzung für die Erstellung einer Content Control List die Berechtigung **Data Control – Anpassung**. Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Eine Übersicht über Content Control Lists finden Sie unter [Content Control Lists](#) (Seite 136).

So erstellen/ändern Sie eine Content Control List:

1. Wählen Sie im Menü **Extras** unter **Data Control** die Option **Data Control Content Control Lists**.
2. Klicken Sie im Dialogfeld **Content Control List - Verwaltung** auf **Hinzufügen**, um eine neue Content Control List zu erstellen, oder wählen Sie eine vorhandene Content Control List aus und klicken Sie auf **Ändern**.
3. Geben Sie im Dialogfeld **Neue Content Control List** in das Feld **Name** eine Bezeichnung für die Content Control List ein.
4. Im Feld **Beschreibung** können Sie die Content Control List auf Wunsch beschreiben.
5. Sie können einer Content Control List Kriterien zuweisen oder vorhandene Kriterien bearbeiten. Klicken Sie hierzu neben dem Feld **Kriterien** auf **Ändern**.
Anhand von Kriterien können Content Control Lists nach Typ und Geltungsbereich filtern.
6. Wählen Sie im Dialogfeld **Content Control List-Kriterien ändern** die gewünschten Kriterien aus der Liste **Verfügbare Kriterien** aus und verschieben Sie sie in die Liste **Gewählte Kriterien**. Klicken Sie auf **OK**.
7. Wählen Sie im Bereich **Nach Inhaltsübereinstimmung scannen** eine Suchbedingung aus („Beliebiger Ausdruck“, „Alle Ausdrücke“ oder „Dieser Ausdruck“) und geben Sie die gewünschten Suchbegriffe durch Leerzeichen voneinander getrennt ein. Klicken Sie auf **OK**.

Hinweis: Bei der Suche wird zwischen Groß- und Kleinschreibung unterschrieben.

Anführungszeichen sind in einfachen Content Control Lists nicht zulässig. Wenn Sie nach einem genauen Wortlaut suchen, wählen Sie die Bedingung „Dieser Ausdruck“.

Zum Auffinden komplexer Ausdrücke empfiehlt sich die Suche über den Advanced Content Control List Editor, der im Abschnitt [Erstellen/Ändern einer komplexen Content Control List](#) (Seite 146) beschrieben wird.

Die neue Content Control List wird im Dialogfeld **Content Control List – Verwaltung** angezeigt.

Beispiele

Suchbedingung	Beispiel	Beschreibung
Nach einem der Begriffe	vertraulich geheim	Suche nach Dokumenten, die die Begriffe „vertraulich“ oder „geheim“ beinhalten.

Suchbedingung	Beispiel	Beschreibung
Nach allen Begriffen	Projekt vertraulich	Suche nach Dokumenten, die die Begriffe „Projekt“ und „vertraulich“ beinhalten.
Genaue Entsprechung	nur für den internen Gebrauch	Suche nach Dokumenten, die den Ausdruck „nur für den internen Gebrauch“ beinhalten.

Jetzt können Sie die neue Content Control List einer Inhaltsregel zuweisen.

23.14 Erstellen/Ändern einer komplexen Content Control List

Bei rollenbasierter Verwaltung gilt als Voraussetzung für die Erstellung einer Content Control List die Berechtigung **Data Control – Anpassung**. Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Eine Übersicht über Content Control Lists finden Sie unter [Content Control Lists](#) (Seite 136).

Sie können eine Content Control List erstellen, die einen oder mehrere reguläre Ausdrücke und einen Schwellenwert enthält. Verwenden Sie hierzu den Advanced Content Control List Editor.

So erstellen/bearbeiten Sie eine Content Control List mit dem Advanced Content Control List Editor:

1. Wählen Sie im Menü **Extras** unter **Data Control** die Option **Data Control Content Control Lists**.
2. Klicken Sie im Dialogfeld **Content Control List - Verwaltung** auf **Hinzufügen**, um eine neue Content Control List zu erstellen, oder wählen Sie eine vorhandene Content Control List aus und klicken Sie auf **Ändern**.
3. Geben Sie im Dialogfeld **Neue Content Control List** in das Feld **Name** eine Bezeichnung für die Content Control List ein.
4. Im Feld **Beschreibung** können Sie die Content Control List auf Wunsch beschreiben.
5. Sie können einer Content Control List Kriterien zuweisen oder vorhandene Kriterien bearbeiten. Klicken Sie hierzu neben dem Feld **Kriterien** auf **Ändern**.
Anhand von Kriterien können Content Control Lists nach Typ und Geltungsbereich filtern.
6. Wählen Sie im Dialogfeld **Content Control List-Kriterien ändern** die gewünschten Kriterien aus der Liste **Verfügbare Kriterien** aus und verschieben Sie sie in die Liste **Gewählte Kriterien**. Klicken Sie auf **OK**.
7. Klicken Sie auf **Erweitert**.
8. Klicken Sie im Bereich **Erweitert** auf **Erstellen**, um einen neuen Ausdruck zu erstellen, oder wählen Sie einen vorhandenen Ausdruck aus und klicken Sie auf **Ändern**.

9. Geben Sie in das Dialogfeld **Content Control List – Erweiterte Funktionen** einen regulären Ausdruck mit Perl 5-Syntax ein.

Nähere Informationen hierzu finden Sie im Begleitmaterial zu Perl oder unter http://www.boost.org/doc/libs/1_34_1/libs/regex/doc/syntax_perl.html.

10. Geben Sie in das Feld **Wert** die Zahl ein, die zum Gesamtwert einer Content Control List addiert wird, wenn eine Übereinstimmung mit einem regulären Ausdruck vorliegt.
11. Geben Sie in das Feld **Höchstzahl** die maximal zugelassenen Übereinstimmungen eines regulären Ausdrucks ein, die in die Gesamtbewertung eingehen.
Bei einem Ausdruck mit der Bewertung 5 und der maximalen Anzahl 2 wird höchstens 10 zur Gesamtbewertung der Content Control List hinzugefügt. Wird der Ausdruck dreimal gefunden, wird dennoch 10 zur Gesamtbewertung addiert.

Klicken Sie auf **OK**.

12. Wiederholen Sie die Schritte 5 bis 11, wenn Sie weitere reguläre Ausdrücke in die Content Control List aufnehmen möchten.
13. Geben Sie im Feld **Schwellenwert** die erforderliche Trefferanzahl eines regulären Ausdrucks an, damit eine Übereinstimmung mit der Content Control List vorliegt.

Als Beispiel soll eine Content Control List mit der Schwellenbewertung 8 und drei Ausdrücken (A, B und C) sowie der folgenden Bewertung und maximalen Anzahl betrachtet werden:

Ausdruck	Bewertung	Höchstzahl
Ausdruck A	5	2
Ausdruck B	3	1
Ausdruck C	1	5

Übereinstimmung mit der Content Control List liegt vor, wenn Data Control zwei Übereinstimmungen mit Ausdruck A oder eine Übereinstimmung mit Ausdruck A und eine Übereinstimmung mit Ausdruck B oder eine Übereinstimmung mit Ausdruck B und fünf Übereinstimmungen mit Ausdruck C findet.

Klicken Sie auf **OK**.

Die neue Content Control List wird im Dialogfeld **Content Control List-Verwaltung** angezeigt.

Beispiel eines regulären Ausdrucks

```
(?i)\b[a-ceghj-pr-tw-z][a-ceghj-npr-tw-z]\s?\d{2}\s?\d{2}\s?\d{2}\s?[abcd]?b
```

Dieser reguläre Ausdruck stimmt mit Sozialversicherungsnummern aus Großbritannien überein, z.B. AA 11 11 11 A.

(?i)	Groß- und Kleinschreibung wird ignoriert.
------	---

\b	Sucht nach dem Übergang von einem Wortzeichen zu einem Nicht-Wort-Zeichen.
[a-ceghj-pr-tw-z]	Sucht innerhalb des Buchstabenbereichs (A bis C E G H J bis P R bis T W bis Z) nach einem einzelnen Zeichen.
?	Keine oder eine Übereinstimmung mit dem vorherigen Element.
\s?	Entspricht Null oder Leerschritt.
\d{2}	Entspricht zwei Ziffern.
[abcd]	Sucht in der Liste nach einem einzelnen Zeichen (A, B, C oder D).

Jetzt können Sie die neue Content Control List einer Inhaltsregel zuweisen.

23.15 Importieren/Exportieren einer Content Control List

Bei rollenbasierter Verwaltung gilt als Voraussetzung für das Importieren/Exportieren einer Content Control List die Berechtigung **Data Control – Anpassung**. Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Content Control Lists können als XML-Dateien importiert bzw. exportiert werden. Sie können Content Control Lists zwischen Sophos Produkten austauschen, die sie unterstützen.

Hinweis: SophosLabs Content Control Lists können nicht exportiert werden.

So importieren/exportieren Sie eine Content Control List:

1. Wählen Sie im Menü **Extras** unter **Data Control** die Option **Data Control Content Control Lists**.
2. Klicken Sie im Dialogfeld **Content Control List – Verwaltung** auf die Option **Importieren** oder **Exportieren**.
 - Wählen Sie zum Importieren einer Content Control List im Dialogfeld **Importieren** die gewünschte Liste aus und klicken Sie auf **Öffnen**.
 - Wählen Sie zum Exportieren einer Content Control List im Dialogfeld **Exportieren** einen Speicherort für die Datei aus, geben Sie der Datei einen Namen und klicken Sie auf **Speichern**.

24 Konfigurieren der Device Control-Richtlinie

24.1 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.

Mit Device Control können Sie das Risiko von Netzwerkbrücken zwischen einem Unternehmensnetzwerk und einem unternehmensfremden Netzwerk minimieren. 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.

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.
- Die **Device Control-Ereignisse** können Ihnen die Entscheidung erleichtern, welche Gerätearten gesperrt oder von Device Control nicht berücksichtigt werden sollen.
- Lassen Sie Device Control Speichermedien erkennen und blockieren oder schreibschützen Sie sie.

Nähere Informationen zu den empfohlenen Einstellungen zu Device Control entnehmen Sie bitte der *Richtlinienanleitung* zu *Sophos Endpoint Security and Control*.

Hinweis: Bei rollenbasierter Verwaltung:

- Sie müssen über die Berechtigung **Richtlinieneinstellung – Device Control** verfügen, um eine Device Control-Richtlinie konfigurieren zu können.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

24.2 Device Control-Ereignisse

Device Control-Ereignisse (z.B. Sperren eines Wechselmediums) werden im Dialogfeld **Device Control – Ereignisanzeige** angezeigt.

Im Dialogfeld **Device Control – Ereignisanzeige** können Sie Filter anlegen und sich nur Ereignisse anzeigen lassen, die für Sie relevant sind. Außerdem können Sie die Liste der Device Control-Ereignisse in eine Datei exportieren oder in die Zwischenablage kopieren. Mehr dazu können Sie im Abschnitt „Anzeige von Ereignissen“ nachlesen.

Mit Device Control-Ereignissen können Sie bestimmte Geräte oder Gerätearten als Ausnahmen in die Device Control-Richtlinien aufnehmen. Nähere Informationen zum Erstellen von Ausnahmen für Geräte können Sie dem Abschnitt [Ausschließen von Geräten von einer einzelnen Richtlinie](#) (Seite 154) oder [Ausschließen eines Geräts von allen Richtlinien](#) (Seite 153) entnehmen.

Auf dem Dashboard wird die Anzahl der Computer angezeigt, auf denen die Summe der Device Control-Ereignisse in den vergangenen 7 Tagen den angegebenen Höchstwert überschritten hat. Nähere Informationen zum Festlegen des Höchstwerts finden Sie im Abschnitt [Konfigurieren des Dashboards](#) (Seite 51).

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 169).

24.3 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)
- 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. Eine aktuelle Liste der unterstützten sicheren Wechselmedien entnehmen Sie bitte dem Sophos Support-Artikel 63102 (<http://www.sophos.de/support/knowledgebase/article/63102.html>).

Netzwerkgeräte

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

Für Netzwerkschnittstellen können Sie zudem den Modus **Netzwerkbrücken sperren** auswählen, in dem das Risiko von Netzwerkbrücken zwischen einem Unternehmensnetzwerk und einem unternehmensfremden Netzwerk minimiert wird. 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. Eine Richtlinie zum Sperren von Bluetooth blockiert beispielsweise:

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

24.4 Auswählen von Geräten für Device Control

Bei rollenbasierter Verwaltung:

- Sie müssen über die Berechtigung **Richtlinieneinstellung – Device Control** verfügen, um eine Device Control-Richtlinie bearbeiten zu können.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Wichtig: Sie sollten keine Drahtlosverbindungen auf Computern trennen, die auf diese Weise über Enterprise Console verwaltet werden.

1. Prüfen Sie, welche Device Control-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.
Mehr dazu erfahren Sie unter [Welche Richtlinien sind einer Gruppe zugewiesen?](#) (Seite 25).
2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Device Control**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.
3. Rufen Sie im Dialogfeld **Device Control-Richtlinie** die Registerkarte **Konfiguration** auf. Wählen Sie im Bereich **Speicher** das Speichermedium aus, das Sie steuern möchten.
4. Klicken Sie in der Spalte **Status** neben den Gerätetyp und öffnen Sie das Dropdown-Menü. 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.
5. Wählen Sie im Bereich **Netzwerk** die Art des zu sperrenden Netzwerkgeräts aus.
6. Klicken Sie in der Spalte **Status** neben den Netzwerkgerätetyp und öffnen Sie das Dropdown-Menü.
 - Wählen Sie „Gesperrt“ aus, wenn der Gerätetyp gesperrt werden soll.
 - Wählen Sie „Netzwerkbrücken sperren“ aus, um Netzwerkbrücken zwischen einem Unternehmensnetzwerk und einem unternehmensfremden Netzwerk zu verhindern. Der Gerätetyp wird blockiert, wenn ein Endpoint an ein physisches Netzwerk angeschlossen wird (in der Regel über eine Ethernet-Verbindung). Wenn der Endpoint vom physischen Netzwerk abgetrennt wird, wird der Gerätetyp wieder aktiviert.

7. Wählen Sie im Bereich **Kurze Reichweite** den Gerätetyp mit kurzer Reichweite aus, der gesperrt werden soll. Wählen Sie in der Spalte **Status** neben dem Gerätetyp „Gesperrt“ aus. Klicken Sie auf **OK**.

24.5 Erkennen und Zulassen von Geräten

Bei rollenbasierter Verwaltung:

- Sie müssen über die Berechtigung **Richtlinieneinstellung – Device Control** verfügen, um eine Device Control-Richtlinie bearbeiten zu können.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Sie können Geräte erkennen lassen, die jedoch nicht gesperrt werden sollen. Diese Option bietet sich an, wenn Sie Geräte künftig sperren möchten, erforderliche Geräte jedoch zunächst erkennen und zulassen möchten.

Wenn Sie Geräte erkennen, jedoch nicht sperren möchten, aktivieren Sie Device Control-Scans in einer Device Control-Richtlinie und aktivieren Sie den Modus *Nur Erkennen*. Ändern Sie den Status der zu erkennenden Geräte um in „Gesperrt“. Hierbei werden Ereignisse für Geräte auf Endpoints erstellt, wenn zwar Richtlinienverstöße vorliegen, die entsprechenden Geräte jedoch nicht gesperrt werden.

Nähere Informationen zur Anzeige von Device Control-Ereignissen finden Sie im Abschnitt [Anzeige von Device Control-Ereignissen](#) (Seite 63).

So können Sie Geräte anzeigen, ohne Sie zu sperren:

1. Prüfen Sie, welche Device Control-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.
Mehr dazu erfahren Sie unter [Welche Richtlinien sind einer Gruppe zugewiesen?](#) (Seite 25).
2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Device Control**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.
3. Rufen Sie im Dialogfeld **Device Control-Richtlinie** die Registerkarte **Konfiguration** auf und wählen Sie die Option **Device Control-Scans aktivieren** aus.
4. Wählen Sie die Option **Geräte erkennen, aber nicht sperren**.
5. Sofern Sie dies nicht bereits erledigt haben, ändern Sie den Status der zu erkennenden Geräte um in „Gesperrt“. (Mehr dazu erfahren Sie unter [Auswählen von Geräten für Device Control](#) (Seite 151).)
Klicken Sie auf **OK**.

24.6 Erkennen und Sperren von Geräten

Bei rollenbasierter Verwaltung:

- Sie müssen über die Berechtigung **Richtlinieneinstellung – Device Control** verfügen, um eine Device Control-Richtlinie bearbeiten zu können.

- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

1. Prüfen Sie, welche Device Control-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.
Mehr dazu erfahren Sie unter [Welche Richtlinien sind einer Gruppe zugewiesen?](#) (Seite 25).
2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Device Control**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.
3. Rufen Sie im Dialogfeld **Device Control-Richtlinie** die Registerkarte **Konfiguration** auf und aktivieren Sie das Kontrollkästchen **Device Control-Scans aktivieren**.
4. Deaktivieren Sie die Option **Geräte erkennen, aber nicht sperren**.
5. Sofern Sie dies nicht bereits erledigt haben, ändern Sie den Status der zu sperrenden Geräte um in „Gesperrt“. (Mehr dazu erfahren Sie unter [Auswählen von Geräten für Device Control](#) (Seite 151).)
Klicken Sie auf **OK**.

24.7 Ausschließen eines Geräts von allen Richtlinien

Bei rollenbasierter Verwaltung:

- Sie müssen über die Berechtigung **Richtlinieneinstellung – Device Control** verfügen, um eine Device Control-Richtlinie bearbeiten zu können.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Sie können ein Gerät von allen Richtlinien, inklusive der Standardrichtlinie, ausschließen. Der Ausschluss wird dann zu allen neuen Richtlinien, die Sie erstellen, hinzugefügt.

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 von allen Device Control-Richtlinien ausschließen:

1. Klicken Sie im Menü **Ansicht** auf **Device Control-Ereignisse**.
Das Dialogfenster **Device Control – Ereignisanzeige** wird geöffnet.
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 63).

3. Wählen Sie das Gerät aus, das von den Richtlinien ausgeschlossen werden soll und klicken Sie anschließend auf **Gerät ausschließen**.

Das Dialogfeld **Gerät ausschließen** wird angezeigt. Im Bereich **Geräte-Details** werden Typ, Modell und Kennung des Geräts angezeigt. Im Bereich **Ausschluss-Details, Bereich** wird der Text „Alle Richtlinien.“ angezeigt.

Hinweis: Wenn keine Ereignisse für das Gerät, das ausgeschlossen werden soll, vorhanden sind, (z.B. ein internes CD-/DVD-Laufwerk eines Endpoints), gehen Sie zu dem Computer mit dem Gerät und aktivieren Sie das Gerät im Geräte-Manager. (Rechtsklicken Sie zum Aufrufen des Geräte-Managers auf **Arbeitsplatz, Verwalten** und anschließend auf **Geräte-Manager**.) Im Dialogfeld **Device Control – Ereignisanzeige** wird ein neues „Sperr“-Ereignis angezeigt. Sie können das Gerät anhand der Anweisungen oben ausschließen.

4. Sie können auswählen, ob Sie nur dieses Gerät oder alle Geräte dieses Typs ausschließen möchten.
5. Weisen Sie dem Gerät Vollzugriff oder Lesezugriff zu.
6. Geben Sie in das Feld **Bemerkung** bei Bedarf einen Kommentar ein. So können Sie etwa angeben, wer den Geräteausschluss beantragt hat.
7. Klicken Sie auf **OK**.

24.8 Ausschließen von Geräten von einer einzelnen Richtlinie

Bei rollenbasierter Verwaltung:

- Sie müssen über die Berechtigung **Richtlinieneinstellung – Device Control** verfügen, um eine Device Control-Richtlinie bearbeiten zu können.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Sie können bestimmte Geräte von einer Device Control-Richtlinie 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 von einer Richtlinie ausschließen:

1. Prüfen Sie, welche Device Control-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.
Mehr dazu erfahren Sie unter [Welche Richtlinien sind einer Gruppe zugewiesen?](#) (Seite 25).
2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Device Control**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.
3. Rufen Sie im Dialogfeld **Device Control-Richtlinie** die Registerkarte **Konfiguration** auf und klicken Sie auf **Ausschluss hinzu**.

Das Dialogfeld **Device Control – Ereignisanzeige** wird angezeigt.

4. 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 63).
5. Wählen Sie das Gerät aus, das von der Richtlinie ausgeschlossen werden soll, und klicken Sie anschließend auf **Gerät ausschließen**.
Das Dialogfeld **Gerät ausschließen** wird angezeigt. Im Bereich **Geräte-Details** werden Typ, Modell und Kennung des Geräts angezeigt. Im Bereich **Ausschluss-Details, Bereich** wird der Text „Nur diese Richtlinie.“ angezeigt.
Hinweis: Wenn keine Ereignisse für das Gerät, das ausgeschlossen werden soll, vorhanden sind, (z.B. ein internes CD-/DVD-Laufwerk eines Endpoints), gehen Sie zu dem Computer mit dem Gerät und aktivieren Sie das Gerät im Geräte-Manager. (Rechtsklicken Sie zum Aufrufen des Geräte-Managers auf **Arbeitsplatz, Verwalten** und anschließend auf **Geräte-Manager**.) Im Dialogfeld **Device Control – Ereignisanzeige** wird ein neues „Sperr“-Ereignis angezeigt. Sie können das Gerät anhand der Anweisungen oben ausschließen.
6. Sie können auswählen, ob Sie nur dieses Gerät oder alle Geräte dieses Typs ausschließen möchten.
7. Weisen Sie dem Gerät Vollzugriff oder Lesezugriff zu.
8. Geben Sie in das Feld **Bemerkung** bei Bedarf einen Kommentar ein. So können Sie etwa angeben, wer den Geräteausschluss beantragt hat.
9. Klicken Sie auf **OK**.

24.9 Anzeigen/Ändern der Liste der ausgeschlossenen Geräte

Bei rollenbasierter Verwaltung:

- Sie müssen über die Berechtigung **Richtlinieneinstellung – Device Control** verfügen, um eine Device Control-Richtlinie bearbeiten zu können.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

So können Sie sich die Liste der ausgeschlossenen Geräte anzeigen lassen:

1. Prüfen Sie, welche Device Control-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.
Mehr dazu erfahren Sie unter [Welche Richtlinien sind einer Gruppe zugewiesen?](#) (Seite 25).
2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Device Control**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.
3. Wählen Sie im Dialogfeld **Device Control-Richtlinie** auf der Registerkarte **Konfiguration** den Gerätetyp aus, für den Ausschlüsse festgelegt werden sollen (z.B. optisches Laufwerk). Klicken Sie auf **Ausschlüsse anzeigen**.

Das Dialogfeld **<Gerätetyp> Ausschlüsse** wird angezeigt. Wenn ein Ausschluss für alle Geräte des Modells angezeigt wird, ist das Feld **Geräte-ID** leer.

4. Verfahren Sie zum Bearbeiten der Liste ausgeschlossener Geräte wie folgt:

- Wenn Sie einen Ausschluss hinzufügen möchten, klicken Sie auf **Hinzufügen**. Weitere Informationen finden Sie unter [Ausschließen von Geräten von einer einzelnen Richtlinie](#) (Seite 154).
- Wenn Sie einen Ausschluss bearbeiten möchten, wählen Sie den Ausschluss aus, und klicken Sie auf **Ändern**. Ändern Sie die Einstellungen im Dialogfeld **Gerät ausschließen** nach Belieben.
- Wenn Sie einen Ausschluss entfernen möchten, wählen Sie das entsprechende Gerät aus und klicken Sie auf **Entfernen**.

Dadurch wird das ausgeschlossene Gerät aus der Richtlinie entfernt, die Sie ändern. Wenn Sie das Gerät aus weiteren Richtlinien entfernen möchten, wiederholen Sie die genannten Schritte für alle Richtlinien.

25 Konfigurieren der NAC-Richtlinie

25.1 NAC

Sie können Network Access Control (NAC) so konfigurieren, dass Computer nur auf das Netzwerk zugreifen können, wenn sie die von Ihnen bestimmten Voraussetzungen erfüllen. Standardmäßig wird Computern der Netzwerkzugriff gewährt.

Enterprise Console schützt das Netzwerk in Kombination mit NAC Manager. Sie müssen Folgendes installiert haben:

- NAC Manager. Dieser Server wird unabhängig von Enterprise Console installiert.
- NAC Agent. NAC Manager wird auf Ihren Computern im Netzwerk installiert, um die Kommunikation mit NAC Manager zu gewährleisten. Den Agenten können Sie über den **Assistenten zum Schutz von Computern** installieren. Mehr dazu erfahren Sie unter [Schützen von Computern](#) (Seite 45).

Hier wird davon ausgegangen, dass Sie beide Komponenten installiert haben.

Hinweis: Bei rollenbasierter Verwaltung müssen Sie zum Bearbeiten einer NAC-Richtlinie über die Berechtigung **Richtlinieneinstellung – NAC** verfügen. Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

25.2 Einrichten der NAC-Server-URL

Wenn Sie mit NAC arbeiten möchten, müssen Sie die URL des NAC-Servers (d.h. des Computers, auf dem NAC Manager installiert wurde) in Enterprise Console angeben. Dies erfüllt folgende Zwecke:

- Ihre Computer können mit NAC Manager kommunizieren und die richtige NAC-Richtlinie empfangen.
- In NAC Manager können Sie NAC-Richtlinien konfigurieren.

Enterprise Console versucht nach der Erstinstallation, den NAC-Server zu finden und sich damit zu verbinden. Wenn dies nicht gelingt oder sich der Standort des NAC-Servers geändert hat, müssen Sie die URL ggf. selbst angeben.

So geben Sie die URL ein:

1. Wählen Sie im Menü **Extras** die Option **NAC-URL konfigurieren**.
2. Geben Sie im Dialogfeld **URL des Sophos NAC-Servers** die URL des NAC-Servers ein (z.B. http://server).

Hinweis: Wenn Sophos NAC auf mehr als einem Server installiert ist, geben Sie statt der Adresse des Computers mit der Datenbank die Adresse des Computers ein, auf dem die Anwendung läuft.

3. Um zu testen, ob Enterprise Console eine Verbindung über die angegebene URL mit dem NAC-Server herstellen kann, klicken Sie auf **Test**.

25.3 Starten von NAC Manager

NAC Manager ist das Programm, mit dem Sie die NAC-Richtlinien ändern können.

So starten Sie NAC Manager:

1. Klicken Sie in der Symbolleiste auf **NAC**.
Sie können stattdessen auch im Menü **Extras** die Option **NAC verwalten** wählen.
Hinweis: Wenn die URL des NAC-Servers noch nicht erkannt oder eingegeben wurde, werden Sie dazu jetzt aufgefordert.
2. Geben Sie zur Anmeldung Ihre Benutzerdaten für Sophos NAC ein, die Sie von Ihrem Sophos NAC Administrator erhalten haben.

Wie dieses Programm genau funktioniert, erfahren Sie in der Hilfe zu Sophos NAC Manager oder *Sophos NAC für Endpoint Security and Control NAC Manager-Anleitung*.

25.4 NAC-Voreinstellungen

Als Voreinstellung wird die **Standard**-NAC-Richtlinie auf Computer mit Sophos NAC übertragen. Wenn Sie den „Richtlinien-Modus“ nicht geändert haben, gilt Folgendes:

- Die Computer haben Netzwerkzugriff.
- NAC wird im Modus „Report Only“ ausgeführt.

Nähere Informationen zu **verwalteten** und **unverwalteten** Richtlinien finden Sie im Abschnitt [Voreingestellte NAC-Richtlinien](#) (Seite 158)

25.5 Voreingestellte NAC-Richtlinien

Es gibt drei voreingestellte Richtlinien. Im Abschnitt [Ändern einer NAC-Richtlinie](#) (Seite 159) erfahren Sie, wie Sie die Einstellungen dieser Richtlinien ändern können.

Default

Diese Richtlinie wird standardmäßig auf Computer übertragen, auf denen Sophos NAC installiert ist. Wenn Sie die Einstellungen dieser Richtlinie nicht geändert haben, sind alle Computer mit Netzwerkzugriffsrechten ausgestattet. NAC wird im Modus „Report Only“ ausgeführt.

Managed

Diese Richtlinie bietet sich für Computer mit NAC an, die von Enterprise Console verwaltet werden. Die Voreinstellungen entsprechen denen der Standardrichtlinie.

Not managed

Diese Richtlinie kann für Computer an einem Remote-Standort verwendet werden, die nicht von Enterprise Console verwaltet werden und nicht über Sophos NAC verfügen. Temporäre Netzwerkbenutzer können zur Verbindungsherstellung mit einer Website aufgefordert werden,

die den entsprechenden Remote-Computer über einen Web-Agenten mit der Richtlinie vergleicht, bevor er den Zugriff auf das Unternehmensnetzwerk freigibt.

25.6 Ändern einer NAC-Richtlinie

Bei rollenbasierter Verwaltung müssen Sie zum Bearbeiten einer NAC-Richtlinie über die Berechtigung **Richtlinieneinstellung – NAC** verfügen. Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Sie können die Einstellungen der voreingestellten NAC-Richtlinien an Ihre Bedürfnisse anpassen. Sie können die Richtlinien in NAC Manager bearbeiten, um den Richtlinienmodus, die Profile der Richtlinie oder die der Richtlinie zugewiesenen Network Access Templates zu ändern.

So können Sie eine NAC-Richtlinie ändern:

1. Doppelklicken Sie im Bereich **Richtlinien** auf **NAC**. Doppelklicken Sie auf die Richtlinie, die Sie konfigurieren möchten.

NAC Manager wird gestartet.

2. Melden Sie sich mit Ihren Benutzerdaten an.
3. Passen Sie auf der Richtlinienseite die gewünschten Optionen an.

Näheres zum Updaten vorhandener Richtlinie erfahren Sie in der *Konfigurationsanleitung zu Sophos NAC Manager*.

26 Konfigurieren der Manipulationsschutz-Richtlinie

26.1 Allgemeine Informationen

Mit dem Manipulationsschutz können Sie verhindern, dass nicht autorisierte Benutzer (lokale Administratoren und Benutzer ohne hinreichende Fachkenntnisse) und bekannte Malware Sophos Sicherheitssoftware deinstallieren bzw. über Sophos Endpoint Security and Control deaktivieren.

Hinweis: Der Manipulationsschutz schützt nicht vor Benutzern mit ausgeprägtem Technikverständnis. Auch bietet die Funktion keinen Schutz vor Malware, die eigens dafür konzipiert wurde, das Betriebssystem zu untergraben und die Erkennung zu umgehen. Diese Malware-Art wird ausschließlich von Scans auf Threats und verdächtigem Verhalten erkannt. Nähere Informationen entnehmen Sie bitte dem Abschnitt „Konfigurieren der Anti-Virus- und HIPS-Richtlinie“.

Nach der Aktivierung des Manipulationsschutzes und der Erstellung eines Manipulationsschutz-Kennworts können Mitglieder der Gruppe **SophosAdministrators** folgende Aktionen nur unter Angabe des Kennworts vornehmen:

- Konfigurieren Sie die Einstellungen von On-Access-Scans bzw. der Erkennung verdächtigen Verhaltens in Sophos Endpoint Security and Control neu.
- Deaktivieren des Manipulationsschutzes.
- Deinstallation von Komponenten von Sophos Endpoint Security and Control (Sophos Anti-Virus, Sophos Client Firewall, Sophos AutoUpdate oder Sophos Remote Management System).
- Deinstallation von Sophos SafeGuard Disk Encryption.

Wenn Sie Mitgliedern der Gruppe **SophosAdministrators** das Ausführen dieser Aufgaben gewähren möchten, geben Sie diesen das Manipulationsschutzkennwort, damit sie sich authentifizieren können.

Der Manipulationsschutz betrifft Mitglieder der Gruppe **SophosUsers** und **SophosPowerUsers** nicht. Auch bei aktiviertem Manipulationsschutz können diese Benutzer weiterhin ohne Eingabe von Kennwörtern die Aufgaben ausführen, zu deren Ausführung sie berechtigt sind.

Hinweis: Bei rollenbasierter Verwaltung:

- Zum Konfigurieren einer Manipulationsschutz-Richtlinie ist die Berechtigung **Richtlinieneinstellung – Manipulationsschutz** erforderlich.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Manipulationsschutz-Ereignisse

Manipulationsschutz-Ereignisse (z.B. der unbefugte Versuch, Sophos Anti-Virus von einem Endpoint zu entfernen, wurde unterbunden) werden im Ereignisprotokoll festgehalten und können mit Enterprise Console angezeigt werden. Mehr dazu erfahren Sie unter [Anzeige von Manipulationsschutz-Ereignissen](#) (Seite 65).

Es wird zwischen den folgenden Manipulationsschutz-Ereignissen unterschieden:

- Erfolgreiche Manipulationsschutz-Ereignisse (Anzeige des Namens des authentifizierten Benutzers sowie des Authentifizierungszeitpunkts).
- Nicht erfolgreiche Manipulationsschutz-Ereignisse (Anzeige des Zielprodukts/der Zielkomponente, des Manipulationszeitpunkts und der Daten des Benutzers, der den Manipulationsversuch unternommen hat).

26.2 Aktivieren/Deaktivieren des Manipulationsschutzes

Bei rollenbasierter Verwaltung:

- Zum Konfigurieren einer Manipulationsschutz-Richtlinie ist die Berechtigung **Richtlinieneinstellung – Manipulationsschutz** erforderlich.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

So aktivieren/deaktivieren Sie den Manipulationsschutz:

1. Prüfen Sie, welche Manipulationsschutz-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.
Mehr dazu erfahren Sie unter [Welche Richtlinien sind einer Gruppe zugewiesen?](#) (Seite 25).
2. Doppelklicken Sie im Bereich **Richtlinien** auf **Manipulationsschutz**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.
3. Wählen Sie im Dialogfeld **Manipulationsschutz-Richtlinie** das Kontrollkästchen **Manipulationsschutz aktivieren** aus bzw. ab.
Wenn Sie den Manipulationsschutz zum ersten Mal aktivieren, klicken Sie auf **Festlegen** unter dem Feld **Kennwort**. Geben Sie das Kennwort in das Feld **Manipulationsschutz-Kennwort** ein und bestätigen Sie es.

Tipp: Das Kennwort sollte mindestens 8 Zeichen umfassen und sich aus Buchstaben und Zahlen zusammensetzen.

26.3 Ändern des Manipulationsschutz-Kennworts

Bei rollenbasierter Verwaltung:

- Zum Konfigurieren einer Manipulationsschutz-Richtlinie ist die Berechtigung **Richtlinieneinstellung – Manipulationsschutz** erforderlich.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

So ändern Sie das Manipulationsschutz-Kennwort:

1. Prüfen Sie, welche Manipulationsschutz-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.
Mehr dazu erfahren Sie unter [Welche Richtlinien sind einer Gruppe zugewiesen?](#) (Seite 25).
2. Doppelklicken Sie im Bereich **Richtlinien** auf **Manipulationsschutz**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.
3. Klicken Sie im Dialogfeld **Manipulationsschutz-Richtlinie** unter dem Feld **Kennwort** auf **Ändern**. Geben Sie ein neues Kennwort in das Feld **Manipulationsschutz-Kennwort** ein und bestätigen Sie es.

Tipp: Das Kennwort sollte mindestens 8 Zeichen umfassen und sich aus Buchstaben und Zahlen zusammensetzen.

27 Alerts

27.1 Allgemeine Informationen

In Enterprise Console werden mehrere Benachrichtigungsmethoden verwendet.

■ In der Konsole angezeigte Alerts

Wenn ein Objekt auf einem Computer gefunden wird, das bearbeitet werden muss, oder ein Fehler aufgetreten ist, sendet Sophos Endpoint Security and Control einen Alert an Enterprise Console. Der Alert wird in der Computerliste angezeigt. Details können Sie dem Abschnitt „Umgang mit Alerts“ entnehmen.

Diese Alerts werden immer angezeigt. Sie müssen nicht eingerichtet werden.

■ In der Konsole angezeigte Ereignisse

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

■ Von der Konsole an die ausgewählten Empfänger gesendete Alerts

Wenn ein Objekt auf einem Computer gefunden wird, erscheint auf dem Computer-Desktop standardmäßig eine Meldung und zum Windows Ereignisprotokoll wird ein Eintrag hinzugefügt. Bei Application Control-, Data Control- oder Device Control-Ereignissen erscheint eine Nachricht auf dem Desktop.

Sie können außerdem E-Mail-Benachrichtigungen oder SNMP-Benachrichtigungen für Administratoren einrichten.

In diesem Abschnitt wird die Einrichtung von Benachrichtigungen erläutert, die an die von Ihnen gewählten Empfänger gesendet werden.

27.2 Einrichten von Abonnement-Alerts

Bei rollenbasierter Verwaltung müssen Sie hierzu über die Berechtigung **Systemkonfiguration** verfügen. Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Update Manager-Alerts werden in Enterprise Console in der Spalte **Alerts** in der Ansicht **Update Manager** angezeigt. Wenn Sie eine bestimmte Softwareversion abonniert haben, wird ein Alert angezeigt, wenn die Version demnächst eingestellt wird oder eingestellt wurde.

Wenn Sie die Option **Nicht mehr unterstützte Software einer bestimmten Version automatisch updaten** gewählt haben, wird das Abonnement automatisch aktualisiert.

Wenn Sie sich nicht für automatische Upgrades entschieden haben, werden Sie zur Änderung Ihres Abonnements aufgefordert.

Wichtig: Wenn Sie nicht unterstützte Software nutzen, sind Ihre Computer vor neuen Threats nicht sicher. Sophos rät daher zu umgehenden Upgrades auf eine unterstützte Version.

Sie können Ihre gewählten Empfänger per E-Mail über (baldige) Produkteinstellungen benachrichtigen lassen.

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 in das 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 Fensterbereich **Abonnements** die E-Mail-Benachrichtigungen unter „Update Manager“, die Sie an diesen Empfänger senden möchten. Sie können sich über folgende Ereignisse benachrichtigen lassen:
 - Eine von Ihnen abonnierte Produktversion wird demnächst von Sophos eingestellt.
 - Eine von Ihnen abonnierte Produktversion wurde von Sophos eingestellt.

27.3 Einrichten von Antivirus- und HIPS-E-Mail-Benachrichtigungen

Bei rollenbasierter Verwaltung:

- Zur Ausführung dieses Tasks ist die Berechtigung **Richtlinieneinstellung – Virenschutz und HIPS** erforderlich.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Wenn auf einem Computer in einer Gruppe ein Virus, verdächtiges Verhalten oder eine unerwünschte Anwendung erkannt wurde oder ein Fehler aufgetreten ist, kann an diesen Computer eine entsprechende E-Mail-Benachrichtigung gesendet werden.

Wichtig: Mac OS X Computer können E-Mail-Benachrichtigungen nur an eine Adresse senden.

1. Doppelklicken Sie im Fensterbereich **Richtlinien** auf die Antivirus- und HIPS-Richtlinie, die Sie ändern möchten.

2. Klicken Sie im Dialogfeld **Antivirus- und HIPS-Richtlinie** im Bereich **Antivirus- und HIPS-Konfiguration** auf **Benachrichtigungen**.
3. Öffnen Sie im Dialogfeld **Benachrichtigungen** die Registerkarte **E-Mail-Benachrichtigungen** und wählen Sie **E-Mail-Benachrichtigungen aktivieren**.
4. 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.

5. 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.

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

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

27.4 Einrichten von Antivirus- und HIPS-SNMP-Benachrichtigungen

Bei rollenbasierter Verwaltung:

- Zur Ausführung dieses Tasks ist die Berechtigung **Richtlinieneinstellung – Virenschutz und HIPS** erforderlich.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Sie können SNMP-Benachrichtigungen an bestimmte Benutzer senden, wenn auf einem der Computer in der Gruppe ein Virus erkannt wurde oder ein Fehler aufgetreten ist.

Hinweis: Diese Einstellungen gelten nur für Systeme unter Windows 2000 und aufwärts.

1. Doppelklicken Sie im Fensterbereich **Richtlinien** auf die Antivirus- und HIPS-Richtlinie, die Sie ändern möchten.
2. Klicken Sie im Dialogfeld **Antivirus- und HIPS-Richtlinie** im Bereich **Antivirus- und HIPS-Konfiguration** auf **Benachrichtigungen**.
3. Öffnen Sie im Dialogfeld **Benachrichtigungen** die Registerkarte **SNMP-Benachrichtigungen** und wählen Sie **SNMP-Benachrichtigungen aktivieren**.
4. Wählen Sie im Bereich **Bei folgenden Ereignissen eine Benachrichtigung senden**: die Ereignisse aus, bei deren Eintritt SNMP-Benachrichtigungen gesendet werden sollen.
5. Geben Sie im Textfeld **SNMP-Trapziel**: die IP-Adresse des Empfängers an.
6. Geben Sie im Textfeld **SNMP-Community**: den Namen der SNMP-Community an.

27.5 Konfigurieren von Antivirus- und HIPS-Desktop-Benachrichtigungen

Bei rollenbasierter Verwaltung:

- Zur Ausführung dieses Tasks ist die Berechtigung **Richtlinieneinstellung – Virenschutz und HIPS** erforderlich.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Standardmäßig werden Benachrichtigungen auf dem Computer angezeigt, auf dem ein Virus, verdächtiges Objekt oder eine potenziell unerwünschte Anwendung gefunden wurde. Diese Benachrichtigungen lassen sich konfigurieren.

1. Doppelklicken Sie im Fensterbereich **Richtlinien** auf die Antivirus- und HIPS-Richtlinie, die Sie ändern möchten.
2. Klicken Sie im Dialogfeld **Antivirus- und HIPS-Richtlinie** im Bereich **Antivirus- und HIPS-Konfiguration** auf **Benachrichtigungen**.
3. Klicken Sie im Dialogfeld **Benachrichtigungen** auf die Registerkarte **Desktop-Benachrichtigungen**.

Standardmäßig ist **Desktop-Benachrichtigungen aktivieren** mitsamt allen Optionen im Bereich **Bei folgenden Ereignissen eine Benachrichtigung senden** ausgewählt. Ändern Sie diese Einstellungen gegebenenfalls.

Hinweis: Die Einstellungen zur **Erkennung verdächtigen Verhaltens**, **Erkennung verdächtiger Dateien** und zur **Erkennung von Adware und PUA** gelten nur für Windows 2000 und aufwärts.

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

27.6 Einrichten von Application Control-Alerts

Bei rollenbasierter Verwaltung:

- Zur Konfiguration einer Application Control-Richtlinie müssen Sie über die Berechtigung **Richtlinieneinstellungen – Application Control** verfügen.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Ausgewählte Benutzer können benachrichtigt werden, wenn auf einem Computer eine Controlled Application erkannt wird.

1. Doppelklicken Sie im Fensterbereich **Richtlinien** auf die gewünschte Application Control-Richtlinie.
2. Öffnen Sie im Dialogfeld **Application Control-Richtlinie** die Registerkarte **Benachrichtigung**.

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.

3. Sie können im Feld **Text** eine Meldung eingeben, die an eine Desktop-Benachrichtigung angehängt wird.
4. Aktivieren Sie die Option **E-Mail-Benachrichtigung aktivieren**, wenn zu erkannten Controlled Applications eine E-Mail-Benachrichtigung gesendet werden soll.
5. Wenn SNMP-Benachrichtigungen gesendet werden sollen, wählen Sie die Option **SNMP-Benachrichtigungen aktivieren**.

Hinweis: Ihre Antivirus- und HIPS-Richtlinieneinstellungen legen die Konfiguration und die Empfänger von E-Mail- und SNMP-Benachrichtigungen fest. Weitere Informationen finden Sie unter [Einrichten von Antivirus- und HIPS-SNMP-Benachrichtigungen](#) (Seite 165).

27.7 Einrichten von Data Control-Alerts

Bei rollenbasierter Verwaltung:

- Zum Konfigurieren einer Device Control-Richtlinie ist die Berechtigung **Richtlinieneinstellung – Data Control** erforderlich.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Enterprise Console meldet die Erkennung bzw. Blockierung sensibler Daten mit Hilfe von Ereignissen und Benachrichtigungen.

Nähere Informationen zu Data Control-Richtlinien und -Ereignissen finden Sie im Abschnitt „Konfigurieren der Data Control-Richtlinie“.

Wenn Data Control aktiv ist, werden die folgenden Ereignisse und Benachrichtigungen standardmäßig protokolliert oder angezeigt:

- Data Control-Ereignisse werden auf dem Arbeitsplatzrechner protokolliert.
- Data Control-Ereignisse werden an Enterprise Console gesendet und können in der **Data Control – Ereignisanzeige** angezeigt werden. (Klicken Sie im Menü **Ansicht** auf **Data Control-Ereignisse**.)

Hinweis: Endpoints können bis zu 50 Data Control-Ereignisse pro Stunde an Enterprise Console senden.

- Auf dem Dashboard wird die Anzahl der Computer angezeigt, auf denen die Summe der Data Control-Ereignisse in den vergangenen 7 Tagen den angegebenen Höchstwert überschritten hat.
- Desktop-Benachrichtigungen werden auf dem Arbeitsplatzrechner angezeigt.

In Enterprise Console lassen sich folgende Benachrichtigungen einrichten:

E-Mail-Benachrichtigungen	E-Mail-Benachrichtigungen werden an die von Ihnen gewählten Empfänger gesendet.
SNMP-Benachrichtigungen	SNMP-Benachrichtigungen werden an die von Ihnen in den Einstellungen der Anti-Virus- und HIPS-Richtlinie festgelegten Empfänger gesendet.

So richten Sie Data Control-Alerts ein:

1. Prüfen Sie, welche Data Control-Richtlinie von der/den Computergruppe/n verwendet wird, die Sie konfigurieren möchten.
Mehr dazu erfahren Sie unter [Welche Richtlinien sind einer Gruppe zugewiesen?](#) (Seite 25).
2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Data Control**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.
Das Dialogfeld **Data Control-Richtlinie** wird angezeigt.
3. Öffnen Sie im Dialogfeld **Data Control-Richtlinie** die Registerkarte **Benachrichtigungen**. Desktop-Benachrichtigungen und die Option **Passende Regeln in Benachrichtigungen einbeziehen** sind standardmäßig aktiviert.
4. Sie können Ihre eigenen Meldungen zu den Standardmeldungen hinzufügen. Diese werden angezeigt, wenn der Benutzer zur Bestätigung von Dateiübertragung oder von blockiertem Datenverkehr aufgefordert wird.
5. Wenn Sie E-Mail-Benachrichtigungen wünschen, aktivieren Sie das Kontrollkästchen **E-Mail-Benachrichtigungen aktivieren**. Geben Sie in das Feld **E-Mail-Empfänger** die E-Mail-Adressen der gewünschten Empfänger ein. Trennen Sie die Adressen durch ein Semikolon (;) voneinander ab.

6. Wenn Sie SNMP-Benachrichtigungen aktivieren möchten, markieren Sie das Kontrollkästchen **SNMP-Benachrichtigungen aktivieren**.

Die Einstellungen für E-Mail-Server und SNMP-Traps werden über die Anti-Virus- und HIPS-Richtlinie vorgenommen.

27.8 Einrichten von Device Control-Alerts

Bei rollenbasierter Verwaltung:

- Sie müssen über die Berechtigung **Richtlinieneinstellung – Device Control** verfügen, um eine Device Control-Richtlinie bearbeiten zu können.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Enterprise Console meldet die Erkennung bzw. Blockierung gesteuerter Geräte mit Hilfe von Ereignissen und Benachrichtigungen.

Nähere Informationen zu Device Control-Richtlinien und -Ereignissen finden Sie im Abschnitt „Konfigurieren der Device Control-Richtlinie“.

Wenn Device Control aktiv ist, werden die folgenden Ereignisse und Benachrichtigungen standardmäßig protokolliert oder angezeigt:

- Device Control-Ereignisse werden auf dem Arbeitsplatzrechner protokolliert.
- Device Control-Ereignisse werden an Enterprise Console gesendet und können in der **Device Control – Ereignisanzeige** angezeigt werden. (Klicken Sie im Menü **Ansicht** auf **Device Control-Ereignisse**.)
- Auf dem Dashboard wird die Anzahl der Computer angezeigt, auf denen die Summe der Device Control-Ereignisse in den vergangenen 7 Tagen den angegebenen Höchstwert überschritten hat.
- Desktop-Benachrichtigungen werden auf dem Arbeitsplatzrechner angezeigt.

In Enterprise Console lassen sich folgende Benachrichtigungen einrichten:

E-Mail-Benachrichtigungen	E-Mail-Benachrichtigungen werden an die von Ihnen gewählten Empfänger gesendet.
SNMP-Benachrichtigungen	SNMP-Benachrichtigungen werden an die von Ihnen in den Einstellungen der Anti-Virus- und HIPS-Richtlinie festgelegten Empfänger gesendet.

So können Sie Device Control-Alerts einrichten:

1. Prüfen Sie, welche Device Control-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.
Mehr dazu erfahren Sie unter [Welche Richtlinien sind einer Gruppe zugewiesen?](#) (Seite 25).

2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Device Control**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.
3. Desktop-Benachrichtigungen sind im Dialogfeld **Device Control-Richtlinie** auf der Registerkarte **Benachrichtigungen** standardmäßig aktiviert. Wenn Sie weitere Änderungen an der Konfiguration von Benachrichtigungen vornehmen möchten, verfahren Sie wie folgt:
 - *Verfassen eines Texts für Desktop-Benachrichtigungen:* Geben Sie in das Feld **Text** den gewünschten Text ein. Der Text wird an das Ende einer Standard-Benachrichtigung angehängt.
 - *Aktivieren von E-Mail-Benachrichtigungen:* Aktivieren Sie das Kontrollkästchen **E-Mail-Benachrichtigungen aktivieren**. Geben Sie in das Feld **E-Mail-Empfänger** die E-Mail-Adressen der gewünschten Empfänger ein. Trennen Sie die Adressen durch ein Semikolon (;) voneinander ab.
 - *Aktivieren von SNMP-Benachrichtigungen:* Aktivieren Sie das Kontrollkästchen **SNMP-Benachrichtigungen aktivieren**.

Die Einstellungen für E-Mail-Server und SNMP-Traps werden über die Anti-Virus- und HIPS-Richtlinie vorgenommen.

27.9 Einrichten von Netzwerkstatus-E-Mail-Benachrichtigungen

Bei rollenbasierter Verwaltung müssen Sie zum Konfigurieren der Netzwerkstatus-E-Mail-Benachrichtigungen über die Berechtigung **Systemkonfiguration** verfügen. Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Sie können E-Mail-Benachrichtigungen einrichten, die an die gewählten Empfänger gesendet werden sollen, wenn eine Warnstufe oder eine kritische Stufe für einen Dashboard-Bereich überschritten wird.

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 in das 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. Im Fensterbereich **Abonnements** wählen Sie unter „Warnstufe überschritten“ und „Kritische Stufe überschritten“ die E-Mail-Benachrichtigungen, die Sie an diesen Empfänger senden möchten.

27.10 Einrichten von E-Mail-Benachrichtigungen für Active Directory-Synchronisierung

Bei rollenbasierter Verwaltung müssen Sie zum Konfigurieren der Active Directory-E-Mail-Benachrichtigungen zur Synchronisierung über die Berechtigung **Systemkonfiguration** verfügen. Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Sie können E-Mail-Benachrichtigungen über neue Computer und Gruppen, die bei der Synchronisierung mit Active Directory gefunden werden, an gewählte Empfänger senden lassen. Wenn Sie Computer in synchronisierten Gruppen automatisch schützen möchten, können Sie außerdem Benachrichtigungen für das Fehlschlagen des automatischen Schutzes 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 im 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 Fensterbereich **Abonnements** die E-Mail-Benachrichtigungen unter „Synchronisierung mit Active Directory“, die Sie an diesen Empfänger senden möchten.
E-Mail-Benachrichtigungen unter „Synchronisierung mit Active Directory“:
 - Neue Gruppen erkannt
 - Neue Computer erkannt
 - Automatischer Schutz nicht möglich

27.11 Konfigurieren des Windows-Ereignisprotokolls

Bei rollenbasierter Verwaltung:

- Zur Ausführung dieses Tasks ist die Berechtigung **Richtlinieneinstellung – Virenschutz und HIPS** erforderlich.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Standardmäßig schreibt Sophos Endpoint Security and Control alle Informationen bezüglich der Erkennung und/oder Bereinigung von Viren/Spyware, verdächtigem Verhalten und verdächtigen Dateien, Adware und PUA in das Ereignisprotokoll von Windows 2000 (und aufwärts).

Dies lässt sich jedoch ändern:

1. Doppelklicken Sie im Fensterbereich **Richtlinien** auf die Antivirus- und HIPS-Richtlinie, die Sie ändern möchten.
2. Klicken Sie im Dialogfeld **Antivirus- und HIPS-Richtlinie** im Bereich **Antivirus- und HIPS-Konfiguration** auf **Benachrichtigungen**.
3. Klicken Sie im Dialogfeld **Benachrichtigungen** auf die Registerkarte **Ereignisprotokoll**. Standardmäßig ist das Ereignisprotokoll aktiviert. Ändern Sie diese Einstellungen gegebenenfalls.
Ein **Scan-Fehler** liegt beispielsweise auch dann vor, wenn Sophos Endpoint Security and Control auf ein Objekt nicht zugreifen konnte.

28 Erstellen von Reports

28.1 Reports

Reports liefern Informationen (in Form von Text und Grafiken) zu diversen Aspekten der Netzwerksicherheit.

Reports können Sie im **Report Manager** aufrufen. Mit dem **Report Manager** können Sie auf der Basis vorhandener Vorlagen schnell Reports erstellen, die Konfiguration eines Reports ändern und die Reporterstellung zeitlich planen. Die Reportergebnisse werden den gewählten Empfängern als E-Mail-Anhang zugesandt. Sie können Reports ausdrucken und in unterschiedlichen Formaten exportieren.

Sophos bietet vordefinierte Reports, die Sie nach Belieben an Ihre Bedürfnisse anpassen können. Folgende Reports sind vorhanden:

- Alert- und Ereignisverlauf
- Alert-Übersicht
- Alerts und Ereignisse nach Objektname
- Alerts und Ereignisse nach Zeit
- Alerts und Ereignisse nach Ort
- Endpoint-Richtlinienabweichung
- Ereignisse nach Benutzer
- Schutz verwalteter Endpoints
- Update-Hierarchie

Reports und rollenbasierte Administration

Bei rollenbasierter Administration müssen Sie zum Erstellen, Bearbeiten und Löschen von Reports über die Berechtigung **Report-Konfiguration** verfügen. Wenn Sie die Berechtigung nicht besitzen, können Sie Reports lediglich ausführen. Nähere Informationen zur rollenbasierten Verwaltung können Sie dem Abschnitt [Rollen und Teilverwaltungseinheiten](#) (Seite 13) entnehmen.

Reports können nur Daten aus der aktiven Teilverwaltungseinheit umfassen. Sie können Reports nicht auf andere Teilverwaltungseinheiten übertragen. Die Standardreports werden nicht von der Teilverwaltungseinheit **Default** in neu erstellte Teilverwaltungseinheiten kopiert.

Beim Löschen einer Teilverwaltungseinheit gehen auch die darin enthaltenen Reports verloren.

28.2 Erstellen eines neuen Reports

Bei rollenbasierter Verwaltung müssen Sie hierzu über die Berechtigung **Report-Konfiguration** verfügen. Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

So können Sie einen Report erstellen:

1. Klicken Sie in der Symbolleiste auf das Symbol **Reports**.
2. Klicken Sie im Dialogfeld **Report Manager** auf **Erstellen**.
3. Wählen Sie im Dialogfeld **Neuen Report erstellen** eine Report-Vorlage aus und klicken Sie auf **OK**.

Ein Assistent leitet Sie durch die Report-Erstellung und richtet sich dabei nach der gewählten Vorlage.

Wenn Sie den Assistenten nicht verwenden möchten, deaktivieren Sie im Dialogfeld **Neuer Report** die Option **Report mit Assistent erstellen**. Sie können den neuen Report im Dialogfeld „Report-Eigenschaften“ konfigurieren. Nähere Informationen finden Sie in den Abschnitten, die den jeweiligen Report thematisieren.

28.3 Konfigurieren des Reports „Alert- und Ereignisverlauf“

Bei rollenbasierter Verwaltung müssen Sie hierzu über die Berechtigung **Report-Konfiguration** verfügen. Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Im Report **Alert- und Ereignisverlauf** werden alle Alerts und Ereignisse in einem bestimmten Zeitraum angezeigt.

1. Klicken Sie in der Symbolleiste auf das Symbol **Reports**.
2. Wählen Sie im Dialogfeld **Report Manager** die Option **Alert- und Ereignisverlauf** aus und klicken Sie auf **Eigenschaften**.
3. Rufen Sie im Dialogfeld **Alert- und Ereignisverlauf – Eigenschaften** die Registerkarte **Konfiguration** auf und nehmen Sie die gewünschten Einstellungen vor.
 - a) Im Fenster **Report-Details** können Sie auf Wunsch den Namen und die Beschreibung des Reports bearbeiten.
 - b) Klicken Sie im Fenster **Reporting-Zeitraum** im Textfeld **Zeitraum** auf den Pfeil des Dropdown-Menüs und wählen Sie den gewünschten Zeitraum aus.

Sie können entweder einen festen Zeitraum (z.B. **Letzter Monat**) angeben oder die Option **Benutzerdefiniert** wählen und den gewünschten Zeitraum in die Textfelder **Start** und **Ende** eingeben.
 - c) Klicken Sie im Dialogfeld **Erfassungsbereich** auf **Computergruppe** oder **Einzelcomputer**. Klicken Sie dann auf den Dropdown-Pfeil, um eine Gruppe oder einen Computernamen anzugeben.
 - d) Wählen Sie im Fenster **Einzubeziehende Alerts und Ereignisse** die Alert- und Ereignis-Arten aus, die von dem Report erfasst werden sollen.

Standardmäßig berücksichtigt der Report alle Alert- und Ereignis-Arten.

Sie können den Report auch so konfigurieren, dass nur Orte angegeben werden, für die ein bestimmter Alert oder ein Ereignis gemeldet wurde. Klicken Sie hierzu auf **Erweitert** und klicken Sie auf einen Alert- oder Ereignisnamen in der Liste. Wenn Sie mehrere Alerts oder Ereignisse angeben möchten, tragen Sie unter Verwendung von Platzhaltern einen Namen in das Textfeld ein. ? 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 **Anzeigoptionen** die gewünschte Sortieroption für die Alerts und Ereignisse aus.
Standardmäßig werden Alerts und Ereignisse nach **Namen** sortiert. Reports können jedoch auch nach **Computernamen**, **Gruppennamen** oder **Zeitstempel** angeordnet werden.
5. Wählen Sie auf der Registerkarte **Zeitplan** die Option **Zeitplan für diesen Report erstellen** aus, wenn der Report regelmäßig durchgeführt werden soll. Die Report-Ergebnisse werden als E-Mail-Anhang an die gewählten Empfänger gesendet. Geben Sie den Start-Zeitpunkt des Reports an (Datum und die Uhrzeit). Geben Sie außerdem die gewünschte Report-Häufigkeit, das Datei-Format und die Sprache sowie die E-Mail-Adressen der gewünschten Empfänger an.

28.4 Konfigurieren des Reports „Alert-Übersicht“

Bei rollenbasierter Verwaltung müssen Sie hierzu über die Berechtigung **Report-Konfiguration** verfügen. Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Der Report **Alert-Übersicht** liefert statistische Informationen über den allgemeinen Netzwerkszustand.

1. Klicken Sie in der Symbolleiste auf das Symbol **Reports**.
2. Wählen Sie im Dialogfeld **Report Manager** die Option **Alert-Übersicht** aus und klicken Sie auf **Eigenschaften**.
3. Wählen Sie im Dialogfeld **Alert-Übersicht – Eigenschaften** auf der Registerkarte **Konfiguration** die gewünschten Optionen aus.
 - a) Im Fenster **Report-Details** können Sie auf Wunsch den Namen und die Beschreibung des Reports bearbeiten.
 - b) Klicken Sie im Fenster **Reporting-Zeitraum** im Textfeld **Zeitraum** auf den Pfeil des Dropdown-Menüs und wählen Sie den gewünschten Zeitraum aus.
Sie können entweder einen festen Zeitraum (z.B. **Letzter Monat**) angeben oder die Option **Benutzerdefiniert** wählen und den gewünschten Zeitraum in die Textfelder **Start** und **Ende** eingeben.
4. Geben Sie auf der Registerkarte **Anzeigoptionen** unter **Häufigkeit der Ergebnisanzeige** an, wie oft Nichtkonformität festgestellt werden soll (z.B. jede Stunde oder jeden Tag). Klicken Sie auf den Dropdown-Pfeil und wählen Sie ein Intervall aus.
5. Wählen Sie auf der Registerkarte **Zeitplan** die Option **Zeitplan für diesen Report erstellen** aus, wenn der Report regelmäßig durchgeführt werden soll. Die Report-Ergebnisse werden als E-Mail-Anhang an die gewählten Empfänger gesendet. Geben Sie den Start-Zeitpunkt des Reports an (Datum und die Uhrzeit). Geben Sie außerdem die gewünschte Report-Häufigkeit, das Datei-Format und die Sprache sowie die E-Mail-Adressen der gewünschten Empfänger an.

28.5 Konfigurieren des Reports „Alerts und Ereignisse nach Objektname“

Bei rollenbasierter Verwaltung müssen Sie hierzu über die Berechtigung **Report-Konfiguration** verfügen. Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 13).

Der Report **Alerts nach Objekt** liefert statistische Informationen zu allen Alerts und Ereignissen, die auf allen Computern in einem festgelegten Zeitraum angezeigt wurden. Die Alerts sind nach dem Objektnamen sortiert.

So können Sie den Report konfigurieren:

1. Klicken Sie in der Symbolleiste auf das Symbol **Reports**.
2. Wählen Sie im Dialogfeld **Report Manager** die Option **Alerts und Ereignisse nach Objektname** aus und klicken Sie auf **Eigenschaften**.
3. Rufen Sie im Dialogfeld **Alerts und Ereignisse nach Objektname – Eigenschaften** die Registerkarte **Konfiguration** auf und nehmen Sie die gewünschten Einstellungen vor.
 - a) Im Fenster **Report-Details** können Sie auf Wunsch den Namen und die Beschreibung des Reports bearbeiten.
 - b) Klicken Sie im Fenster **Reporting-Zeitraum** im Textfeld **Zeitraum** auf den Pfeil des Dropdown-Menüs und wählen Sie den gewünschten Zeitraum aus.
Sie können entweder einen festen Zeitraum (z.B. **Letzter Monat**) angeben oder die Option **Benutzerdefiniert** wählen und den gewünschten Zeitraum in die Textfelder **Start** und **Ende** eingeben.
 - c) Klicken Sie im Dialogfeld **Erfassungsbereich** auf **Computergruppe** oder **Einzelcomputer**. Klicken Sie dann auf den Dropdown-Pfeil, um eine Gruppe oder einen Computernamen anzugeben.
 - d) Wählen Sie im Fenster **Einzubeziehende Alerts und Ereignisse** die Alert- und Ereignis-Arten aus, die von dem Report erfasst werden sollen.
Standardmäßig berücksichtigt der Report alle Alert- und Ereignis-Arten.
4. Wählen Sie auf der Registerkarte **Anzeige-Optionen** unter **Anzeige** die Alerts und Ereignisse aus, die im Report aufgeführt werden sollen.
Standardmäßig zeigt der Report alle Alerts und Ereignisse und deren Häufigkeit an.
Sie können den Report auch dazu konfigurieren, nur Folgendes anzuzeigen:
 - die ersten n Alerts und Ereignisse (wobei n eine von Ihnen festgelegte Anzahl ist) oder
 - Alerts und Ereignisse mit mindestens m Vorkommnissen (wobei m eine von Ihnen festgelegte Anzahl ist).
5. Wählen Sie unter **Sortieren nach** aus, ob Alerts und Ereignisse nach Häufigkeit oder Name sortiert werden sollen.
Als Standard listet der Report Alerts und Ereignisse in absteigender Reihenfolge nach ihrer Häufigkeit auf.

6. Wählen Sie auf der Registerkarte **Zeitplan** die Option **Zeitplan für diesen Report erstellen** aus, wenn der Report regelmäßig durchgeführt werden soll. Die Report-Ergebnisse werden als E-Mail-Anhang an die gewählten Empfänger gesendet. Geben Sie den Start-Zeitpunkt des Reports an (Datum und die Uhrzeit). Geben Sie außerdem die gewünschte Report-Häufigkeit, das Datei-Format und die Sprache sowie die E-Mail-Adressen der gewünschten Empfänger an.

28.6 Konfigurieren des Reports „Alerts und Ereignisse nach Zeit“

Bei rollenbasierter Verwaltung müssen Sie hierzu über die Berechtigung **Report-Konfiguration** verfügen. Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Im Report **Alerts nach Zeit** werden Alerts und Ereignisse in regelmäßigen Abständen zusammengefasst.

1. Klicken Sie in der Symbolleiste auf das Symbol **Reports**.
2. Wählen Sie im Dialogfeld **Report Manager** die Option **Alerts und Ereignisse nach Zeit** aus und klicken Sie auf **Eigenschaften**.
3. Rufen Sie im Dialogfeld **Alerts und Ereignisse nach Zeit – Eigenschaften** die Registerkarte **Konfiguration** auf und nehmen Sie die gewünschten Einstellungen vor.
 - a) Im Fenster **Report-Details** können Sie auf Wunsch den Namen und die Beschreibung des Reports bearbeiten.
 - b) Klicken Sie im Fenster **Reporting-Zeitraum** im Textfeld **Zeitraum** auf den Pfeil des Dropdown-Menüs und wählen Sie den gewünschten Zeitraum aus.
Sie können entweder einen festen Zeitraum (z.B. **Letzter Monat**) angeben oder die Option **Benutzerdefiniert** wählen und den gewünschten Zeitraum in die Textfelder **Start** und **Ende** eingeben.
 - c) Klicken Sie im Dialogfeld **Erfassungsbereich** auf **Computergruppe** oder **Einzelcomputer**. Klicken Sie dann auf den Dropdown-Pfeil, um eine Gruppe oder einen Computernamen anzugeben.
 - d) Wählen Sie im Fenster **Einzubeziehende Alerts und Ereignisse** die Alert- und Ereignis-Arten aus, die von dem Report erfasst werden sollen.
Standardmäßig berücksichtigt der Report alle Alert- und Ereignis-Arten.
Sie können den Report auch so konfigurieren, dass nur Orte angegeben werden, für die ein bestimmter Alert oder ein Ereignis gemeldet wurde. Klicken Sie hierzu auf **Erweitert** und klicken Sie auf einen Alert- oder Ereignisnamen in der Liste. Wenn Sie mehrere Alerts oder Ereignisse angeben möchten, tragen Sie unter Verwendung von Platzhaltern einen Namen in das Textfeld ein. ? steht für ein einzelnes Zeichen im Namen und * für eine Zeichenfolge. Zum Beispiel steht W32/* für alle Viren, deren Namen mit W32/ beginnen.
4. Geben Sie auf der Registerkarte **Anzeigeoptionen** Zeitintervalle an, in denen die Häufigkeit von Alerts und Ereignissen gemessen wird, z.B. jede Stunde oder jeden Tag, klicken Sie auf den Dropdown-Pfeil und wählen ein Intervall aus.

5. Wählen Sie auf der Registerkarte **Zeitplan** die Option **Zeitplan für diesen Report erstellen** aus, wenn der Report regelmäßig durchgeführt werden soll. Die Report-Ergebnisse werden als E-Mail-Anhang an die gewählten Empfänger gesendet. Geben Sie den Start-Zeitpunkt des Reports an (Datum und die Uhrzeit). Geben Sie außerdem die gewünschte Report-Häufigkeit, das Datei-Format und die Sprache sowie die E-Mail-Adressen der gewünschten Empfänger an.

28.7 Konfigurieren des Reports „Alerts und Ereignisse nach Ort“

Bei rollenbasierter Verwaltung müssen Sie hierzu über die Berechtigung **Report-Konfiguration** verfügen. Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 13).

Der Report **Alerts nach Ort und Ereignissen** liefert statistische Informationen zu allen Alerts, die auf allen Computern in einem festgelegten Zeitraum angezeigt wurden. Die Alerts sind nach dem Ort sortiert.

1. Klicken Sie in der Symbolleiste auf das Symbol **Reports**.
2. Wählen Sie im Dialogfeld **Report Manager** die Option **Alerts nach Ort und Ereignissen** aus und klicken Sie auf **Eigenschaften**.
3. Rufen Sie im Dialogfeld **Alerts und Ereignisse nach Ort – Eigenschaften** die Registerkarte **Konfiguration** auf und nehmen Sie die gewünschten Einstellungen vor.
 - a) Im Fenster **Report-Details** können Sie auf Wunsch den Namen und die Beschreibung des Reports bearbeiten.
 - b) Klicken Sie im Fenster **Reporting-Zeitraum** im Textfeld **Zeitraum** auf den Pfeil des Dropdown-Menüs und wählen Sie den gewünschten Zeitraum aus.
Sie können entweder einen festen Zeitraum (z.B. **Letzter Monat**) angeben oder die Option **Benutzerdefiniert** wählen und den gewünschten Zeitraum in die Textfelder **Start** und **Ende** eingeben.
 - c) Klicken Sie im Fenster **Report-Verzeichnis** auf **Computer**, um sich die Alerts pro Computer anzeigen zu lassen oder auf **Gruppe**, um sich die Alerts für jede Computergruppe anzeigen zu lassen.
 - d) Wählen Sie im Fenster **Einzubeziehende Alerts und Ereignisse** die Alert- und Ereignis-Arten aus, die von dem Report erfasst werden sollen.
Standardmäßig berücksichtigt der Report alle Alert- und Ereignis-Arten.
Sie können den Report auch so konfigurieren, dass nur Orte angegeben werden, für die ein bestimmter Alert oder ein Ereignis gemeldet wurde. Klicken Sie hierzu auf **Erweitert** und klicken Sie auf einen Alert- oder Ereignisnamen in der Liste. Wenn Sie mehrere Alerts oder Ereignisse angeben möchten, tragen Sie unter Verwendung von Platzhaltern einen Namen in das Textfeld ein. ? 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 **Anzeige-Optionen** unter **Anzeige** die Orte aus, die im Report aufgeführt werden sollen.
Standardmäßig zeigt der Report alle Computer und Gruppen und die Häufigkeit der jeweiligen Alerts an. Sie können den Report aber auch so konfigurieren, dass nur Folgendes angezeigt wird:
 - die obersten n Orte, für die die meisten Alerts und Ereignisse verzeichnet wurden (wobei n eine von Ihnen festgelegte Anzahl ist) oder
 - Orte, die m Mal oder öfter vorkommen (wobei m eine von Ihnen festgelegte Anzahl ist)
5. Wählen Sie unter **Sortieren nach** aus, ob Sie die Orte nach der Anzahl der erkannten Objekte oder nach Namen sortieren möchten.
Als Standard listet der Report die Orte absteigend nach der Anzahl der Alerts und Ereignisse pro Ort auf. Markieren Sie den **Ort**, wenn die erkannten Objekte alphabetisch nach Namen sortiert werden sollen.
6. Wählen Sie auf der Registerkarte **Zeitplan** die Option **Zeitplan für diesen Report erstellen** aus, wenn der Report regelmäßig durchgeführt werden soll. Die Report-Ergebnisse werden als E-Mail-Anhang an die gewählten Empfänger gesendet. Geben Sie den Start-Zeitpunkt des Reports an (Datum und die Uhrzeit). Geben Sie außerdem die gewünschte Report-Häufigkeit, das Datei-Format und die Sprache sowie die E-Mail-Adressen der gewünschten Empfänger an.

28.8 Konfigurieren des Reports „Endpoint-Richtlinienabweichung“

Bei rollenbasierter Verwaltung müssen Sie hierzu über die Berechtigung **Report-Konfiguration** verfügen. Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Im Report **Endpoint-Richtlinienabweichung** wird der prozentuale Anteil oder die Anzahl der Computer, die nicht mit der Gruppenlichtlinie konform sind, in regelmäßigen Abständen zusammengefasst.

1. Klicken Sie in der Symbolleiste auf das Symbol **Reports**.
2. Wählen Sie im Dialogfeld **Report Manager** die Option **Endpoint-Richtlinienabweichung** aus und klicken Sie auf **Eigenschaften**.
3. Wählen Sie im Dialogfeld **Endpoint-Richtlinienabweichung – Eigenschaften** auf der Registerkarte **Konfiguration** die gewünschten Optionen aus.
 - a) Im Fenster **Report-Details** können Sie auf Wunsch den Namen und die Beschreibung des Reports bearbeiten.
 - b) Klicken Sie im Fenster **Reporting-Zeitraum** im Textfeld **Zeitraum** auf den Pfeil des Dropdown-Menüs und wählen Sie den gewünschten Zeitraum aus.
Sie können entweder einen festen Zeitraum (z.B. **Letzter Monat**) angeben oder die Option **Benutzerdefiniert** wählen und den gewünschten Zeitraum in die Textfelder **Start** und **Ende** eingeben.
 - c) Wählen Sie im Fenster **Anzeigen** die Richtlinien aus, die im Report aufgeführt werden sollen. Standardmäßig ist nur die **Anti-Virus- und HIPS**-Richtlinie ausgewählt.

4. Geben Sie auf der Registerkarte **Anzeigeoptionen** unter **Häufigkeit der Ergebnisanzeige** an, wie oft Nichtkonformität festgestellt werden soll (z.B. jede Stunde oder jeden Tag). Klicken Sie auf den Dropdown-Pfeil und wählen Sie ein Intervall aus.
5. Wählen Sie im Bereich **Ergebnisse anzeigen als**, ob die Ergebnisse prozentual oder in Zahlen angezeigt werden sollen.
6. Wählen Sie auf der Registerkarte **Zeitplan** die Option **Zeitplan für diesen Report erstellen** aus, wenn der Report regelmäßig durchgeführt werden soll. Die Report-Ergebnisse werden als E-Mail-Anhang an die gewählten Empfänger gesendet. Geben Sie den Start-Zeitpunkt des Reports an (Datum und die Uhrzeit). Geben Sie außerdem die gewünschte Report-Häufigkeit, das Datei-Format und die Sprache sowie die E-Mail-Adressen der gewünschten Empfänger an.

28.9 Konfigurieren des Reports „Ereignisse nach Benutzer“

Bei rollenbasierter Verwaltung müssen Sie hierzu über die Berechtigung **Report-Konfiguration** verfügen. Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Im Report **Ereignisse nach Benutzer** werden Application Control-, Firewall-, Data Control- und Device Control-Ereignisse sowie gesperrte Websites nach Benutzer gruppiert.

1. Klicken Sie in der Symbolleiste auf das Symbol **Reports**.
2. Wählen Sie im Dialogfeld **Report Manager** die Option **Ereignisse nach Benutzer** aus und klicken Sie auf **Eigenschaften**.
3. Rufen Sie im Dialogfeld **Ereignisse nach Benutzer – Eigenschaften** die Registerkarte **Konfiguration** auf und nehmen Sie die gewünschten Einstellungen vor.
 - a) Im Fenster **Report-Details** können Sie auf Wunsch den Namen und die Beschreibung des Reports bearbeiten.
 - b) Klicken Sie im Fenster **Reporting-Zeitraum** im Textfeld **Zeitraum** auf den Pfeil des Dropdown-Menüs und wählen Sie den gewünschten Zeitraum aus.
Sie können entweder einen festen Zeitraum (z.B. **Letzter Monat**) angeben oder die Option **Benutzerdefiniert** wählen und den gewünschten Zeitraum in die Textfelder **Start** und **Ende** eingeben.
 - c) Wählen Sie im Bereich **Einzubeziehende Ereignisse** die Funktionen aus, für die Ereignisse angezeigt werden sollen.
4. Wählen Sie auf der Registerkarte **Anzeige-Optionen** unter **Anzeige** die Benutzer aus, die im Report aufgeführt werden sollen.

Standardmäßig zeigt der Report alle Benutzer und die zugehörigen Ereignisse an. Sie können den Report aber auch so konfigurieren, dass nur Folgendes angezeigt wird:

- die obersten n Benutzer, für die die meisten Ereignisse verzeichnet wurden (wobei n eine von Ihnen festgelegte Anzahl ist) oder
- Benutzer mit mindestens m Ereignissen (wobei m eine von Ihnen festgelegte Anzahl ist).

5. Wählen Sie unter **Sortieren nach** aus, ob Sie die Benutzer nach der Ereignisanzahl oder nach Namen sortieren möchten.
Als Standard listet der Report die Benutzer absteigend nach der Anzahl der zugehörigen Ereignisse auf. Markieren Sie **Benutzer**, wenn die Benutzer alphabetisch aufgelistet werden sollen.
6. Wählen Sie auf der Registerkarte **Zeitplan** die Option **Zeitplan für diesen Report erstellen** aus, wenn der Report regelmäßig durchgeführt werden soll. Die Report-Ergebnisse werden als E-Mail-Anhang an die gewählten Empfänger gesendet. Geben Sie den Start-Zeitpunkt des Reports an (Datum und die Uhrzeit). Geben Sie außerdem die gewünschte Report-Häufigkeit, das Datei-Format und die Sprache sowie die E-Mail-Adressen der gewünschten Empfänger an.

28.10 Konfigurieren des Reports „Schutz verwalteter Endpoints“

Bei rollenbasierter Verwaltung müssen Sie hierzu über die Berechtigung **Report-Konfiguration** verfügen. Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Im Report **Schutz verwalteter Endpoints** wird der prozentuale Anteil oder die Anzahl der geschützten Computern in regelmäßigen Abständen zusammengefasst.

1. Klicken Sie in der Symbolleiste auf das Symbol **Reports**.
2. Wählen Sie im Dialogfeld **Report Manager** die Option **Schutz verwalteter Endpoints** aus und klicken Sie auf **Eigenschaften**.
3. Wählen Sie im Dialogfeld **Schutz verwalteter Endpoints – Eigenschaften** auf der Registerkarte **Konfiguration** die gewünschten Optionen aus.
 - a) Im Fenster **Report-Kennung** können Sie auf Wunsch den Namen und die Beschreibung des Reports bearbeiten.
 - b) Klicken Sie im Fenster **Reporting-Zeitraum** im Textfeld **Zeitraum** auf den Pfeil des Dropdown-Menüs und wählen Sie den gewünschten Zeitraum aus.
Sie können entweder einen festen Zeitraum (z.B. **Letzter Monat**) angeben oder die Option **Benutzerdefiniert** wählen und den gewünschten Zeitraum in die Textfelder **Start** und **Ende** eingeben.
 - c) Wählen Sie im Fenster **Anzeigen** die Funktionen aus, die im Report aufgeführt werden sollen.
4. Geben Sie auf der Registerkarte **Anzeigeoptionen** unter **Häufigkeit der Ergebnisanzeige** an, wie oft Nichtkonformität festgestellt werden soll (z.B. jede Stunde oder jeden Tag). Klicken Sie auf den Dropdown-Pfeil und wählen Sie ein Intervall aus.
5. Wählen Sie im Bereich **Ergebnisse anzeigen als**, ob die Ergebnisse prozentual oder in Zahlen angezeigt werden sollen.

6. Wählen Sie auf der Registerkarte **Zeitplan** die Option **Zeitplan für diesen Report erstellen** aus, wenn der Report regelmäßig durchgeführt werden soll. Die Report-Ergebnisse werden als E-Mail-Anhang an die gewählten Empfänger gesendet. Geben Sie den Start-Zeitpunkt des Reports an (Datum und die Uhrzeit). Geben Sie außerdem die gewünschte Report-Häufigkeit, das Datei-Format und die Sprache sowie die E-Mail-Adressen der gewünschten Empfänger an.

28.11 Update Hierarchie-Reports

Im **Update-Hierarchie**-Report werden die Update Manager im Netzwerk, die entsprechenden Update-Freigaben sowie die Anzahl der Computer, die von diesen Freigaben Updates beziehen, angezeigt.

Der **Update-Hierarchie**-Report ist nicht konfigurierbar. Sie können den Report anhand der Anweisungen im Abschnitt [Ausführen von Reports](#) (Seite 182) durchführen.

28.12 Report-Zeitpläne

Bei rollenbasierter Verwaltung müssen Sie hierzu über die Berechtigung **Report-Konfiguration** verfügen. Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Sie können einstellen, dass Reports in regelmäßigen Abständen ausgeführt werden. Die Ergebnisse werden als E-Mail-Anhang an die gewählten Empfänger gesendet.

1. Klicken Sie in der Symbolleiste auf das Symbol **Reports**.
2. Wählen Sie im Dialogfeld **Report Manager** den Report aus, für den ein Zeitplan erstellt werden soll und klicken Sie auf **Zeitplan**.
3. Rufen Sie in dem Dialogfeld, das angezeigt wird, die Registerkarte **Zeitplan** auf und wählen Sie die Option **Zeitplan für diesen Report erstellen** aus.
4. Geben Sie einen Startzeitpunkt für die Reporterstellung (Datum und Uhrzeit) sowie die Häufigkeit der Report-Erstellung an.
5. Geben Sie das Format und die Sprache für die Reporterstellung an.
6. Geben Sie die E-Mail-Adressen der Report-Empfänger an.

28.13 Ausführen von Reports

1. Klicken Sie in der Symbolleiste auf das Symbol **Reports**.
2. Wählen Sie im Dialogfeld **Report Manager** den gewünschten Report aus und klicken Sie auf **Ausführen**.

Das **Reports-Fenster** wird angezeigt.

Sie können das Layout des Reports ändern, den Report ausdrucken oder in eine Datei exportieren.

28.14 Report-Tabellen und -Diagramme

Sie können bestimmte Reports als Tabelle und Diagramme darstellen. Wenn dies der Fall ist, sind im **Report-Fenster**, in dem der Report angezeigt wird, zwei Registerkarten vorhanden: **Tabelle** und **Diagramm**.

1. Klicken Sie in der Symbolleiste auf das Symbol **Reports**.
2. Wählen Sie im Dialogfeld **Report Manager** den gewünschten Report aus, z.B. **Alerts und Ereignisse nach Ort** und klicken Sie anschließend auf **Ausführen**.

Das **Reports-Fenster** wird angezeigt.

3. Wenn der Report als Tabelle oder Diagramm dargestellt werden soll, wählen Sie die entsprechende Registerkarte aus.

28.15 Drucken von Reports

Klicken Sie zum Drucken eines Reports auf das **Drucker**-Symbol in der Symbolleiste im oberen Bereich des Reports.



28.16 Exportieren eines Reports in eine Datei

So exportieren Sie einen Report in eine Datei:

1. Klicken Sie in der Symbolleiste im oberen Bereich des Reports auf das **Export**-Symbol.



2. Wählen Sie im Dialogfeld **Export-Report** das Dokumenten- oder Tabellenformat, in das Sie den Report exportieren möchten.

Folgende Optionen stehen zur Verfügung:

- PDF (Acrobat)
 - HTML
 - Microsoft Excel
 - Microsoft Word
 - Rich Text Format (RTF)
 - Comma Separated Values (CSV)
 - XML
3. Klicken Sie auf die Schaltfläche neben dem Feld **Dateiname**, um einen Speicherort auszuwählen. Geben Sie dann einen Namen ein. Klicken Sie **OK**.

28.17 Ändern des Report-Layouts

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

1. Klicken Sie auf das Seitenlayout-Symbol in der Symbolleiste im oberen Seitenbereich.



2. Geben Sie im Dialogfeld **Seite einrichten** die Seitengröße, die Ränder und die Ausrichtung an. Klicken Sie **OK**.

Der Report wird im gewählten Format angezeigt.

Das Format wird auch beim Drucken oder Exportieren von Reports übernommen.

29 Kopieren und Drucken von Daten mit Enterprise Console

29.1 Kopieren von Daten aus der Computerliste

Sie können Daten aus der Computerliste der Ansicht **Endpoints** über die Zwischenablage in ein anderes Dokument kopieren. Die Daten werden durch Tabulatoren voneinander getrennt.

1. Wählen Sie in der Ansicht **Endpoints** im Bereich **Gruppen** die Computergruppe, deren Details kopiert werden sollen.
2. Wählen Sie im Dropdown-Menü **Ansicht** die gewünschten Computer aus, z.B. **Computer mit potenziellen Problemen**.
3. Wenn die Gruppe auch Untergruppen enthält, wählen Sie, ob Computer **Nur auf dieser Ebene** oder **Diese Ebene und abwärts** angezeigt werden sollen.
4. Wählen Sie in der Computerliste die gewünschte Kategorie, z.B. **Antivirus-Details**.
5. Klicken Sie in die Liste, um sie in den Vordergrund zu bringen.
6. Klicken Sie im Menü **Ändern** auf **Kopieren**. Die Daten werden nun in die Zwischenablage kopiert.

29.2 Drucken von Daten aus der Computerliste

Die Informationen der Computerliste in der Ansicht **Endpoints** lassen sich auch ausdrucken.

1. Wählen Sie in der Ansicht **Endpoints** im Bereich **Gruppen** die Computergruppe, deren Details gedruckt sollen.
2. Wählen Sie im Dropdown-Menü **Ansicht** die gewünschten Computer aus, z.B. **Computer mit potenziellen Problemen**.
3. Wenn die Gruppe auch Untergruppen enthält, wählen Sie, ob Computer **Nur auf dieser Ebene** oder **Diese Ebene und abwärts** angezeigt werden sollen.
4. Wählen Sie in der Computerliste die gewünschte Kategorie, z.B. **Antivirus-Details**.
5. Klicken Sie in die Liste, um sie in den Vordergrund zu bringen.
6. Klicken Sie im Menü **Datei** auf **Drucken**.

29.3 Kopieren der Computer-Details eines Computers

Sie können die Daten aus dem Dialogfeld **Computer-Details** in die Zwischenablage kopieren und in ein anderes Dokument einfügen. Aus den Computer-Details gehen der Computername, das Betriebssystem des Computers, die Versionen der installierten Sicherheitssoftware, ausstehende Alerts und Fehler, der Update-Statusversionen usw. hervor.

1. Doppelklicken Sie in der Ansicht **Endpoints** in der Computerliste auf den Computer, dessen Daten kopiert werden sollen.
2. Klicken Sie im Dialogfeld **Computer-Details** auf **Kopieren**, um die Daten in die Zwischenablage zu kopieren.

29.4 Drucken der Computer-Details eines Computers

Sie können die Informationen des Dialogfelds **Computer-Details**. Aus den Computer-Details gehen der Computername, das Betriebssystem des Computers, die Versionen der installierten Sicherheitssoftware, ausstehende Alerts und Fehler, der Update-Statusversionen usw. hervor.

1. Doppelklicken Sie in der Ansicht **Endpoints** in der Computerliste auf den Computer, dessen Daten ausgedruckt werden sollen.
2. Klicken Sie im Dialogfeld **Computer-Details** auf **Drucken**.

30 Wie kann ein anderer Anwender Enterprise Console nutzen?

Mitglieder der Gruppe **Sophos Full Administrators** besitzen uneingeschränkten Zugriff auf Enterprise Console.

Sie können anderen Benutzern Zugriff auf Enterprise Console gewähren. Benutzer müssen zum Öffnen von Enterprise Console folgende Voraussetzungen erfüllen:

- Mitglied der Gruppe „Sophos Console Administrators“ sein.
- Mindestens eine Rolle in Enterprise Console wahrnehmen.
- Mindestens einer Teilverwaltungseinheit in Enterprise Console angehören.

Fügen Sie Benutzer mit Windows-Tools zu einer „Sophos Console Administrators“-Gruppe hinzu.

Klicken Sie zum Zuweisen eines Benutzers zu Rollen oder Teilverwaltungseinheiten in Enterprise Console im Menü **Extras** auf **Rollen und Teilverwaltungseinheiten**. Nähere Informationen zu Rollen und Teilverwaltungseinheiten finden Sie im Abschnitt [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Benutzer müssen zum Zugriff auf eine Remote-Enterprise Console oder eine zusätzliche Instanz von Enterprise Console folgende Voraussetzungen erfüllen:

- Mitglied der Gruppe „Sophos Console Administrators“ auf dem Server sein, auf dem die Enterprise Console-Verwaltungskonsole installiert ist.
- Mitglied der Gruppe „Distributed COM-Benutzer“ auf dem Server sein, auf dem die Enterprise Console-Verwaltungskonsole installiert ist. (Die Gruppe „Distributed COM-Benutzer“ befindet sich im vordefinierten Container des Active Directory-Benutzer und -Computer-Tools.)
- Mindestens eine Rolle in Enterprise Console wahrnehmen.
- Mindestens einer Teilverwaltungseinheit in Enterprise Console angehören.
- Zur Reporterstellung müssen Sie der Gruppe „Sophos DB Users“ auf dem Server angehören, auf dem die Enterprise Console-Datenbank installiert ist.

31 Aktivieren/Deaktivieren von Reports an Sophos

Bei rollenbasierter Verwaltung müssen Sie zum Aktivieren/Deaktivieren von Reports an Sophos über die Berechtigung **Systemkonfiguration** verfügen. Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Sie können Sophos Enterprise Console erlauben, Reports über die Anzahl verwalteter Computer und Informationen über die Arten und Versionen von Betriebssystemen und die verwendeten Sophos Produkte jede Woche an Sophos zu senden. Sophos verwendet diese Informationen, um besseren Support zu leisten und mehr Einblicke in die Produktnutzung der Kunden zu gewinnen. Die an Sophos gesendeten Informationen über Ihre Computer identifizieren keine Personen oder spezifischen Computer. Sophos verwendet diese Informationen nicht dazu, Ihr Unternehmen zu identifizieren, es sei denn, Sie geben uns Ihren Sophos Benutzernamen und/oder Ihre E-Mail-Adresse.

Reports an Sophos sind standardmäßig aktiviert. Sie können Reports an Sophos deaktivieren, wenn Sie die Konsole über den Installations-Assistenten von Sophos Enterprise Console installieren oder aktualisieren.

Wenn Sie Reports an Sophos nach der Installation ein- oder ausschalten möchten, gehen Sie folgendermaßen vor:

1. Wählen Sie im Menü **Extras** die Option **Report an Sophos**.
2. Im Dialogfeld **Report an Sophos** können Sie an Reports an Sophos aktivieren/deaktivieren.
 - *Wenn Sie Reports an Sophos aktivieren möchten*, lesen Sie die Zustimmungserklärung und aktivieren Sie das Kontrollkästchen **Ich stimme zu**, wenn Sie mit den Bedingungen einverstanden sind.
 - *Wenn Sie Reports an Sophos deaktivieren wollen*, deaktivieren Sie das Kontrollkästchen **Ich stimme zu**.

Wenn Sie möchten, dass der technische Support von Sophos Sie (beispielsweise bei Betriebssystem- oder Versionsproblemen) direkt kontaktiert, geben Sie Ihren Sophos Benutzernamen und/oder Ihre E-Mail-Adresse ein.

Wenn Sie die Reports zwar aktivieren möchten, Ihre Anonymität jedoch gewahrt werden soll, geben Sie Benutzernamen oder E-Mail-Adresse nicht an.

32 Fehlerbehebung

32.1 Keine Durchführung von On-Access-Scans

Verfahren Sie wie folgt, wenn On-Access-Scans nicht auf Computern durchgeführt werden:

1. Stellen Sie fest, welche Anti-Virus- und HIPS-Richtlinie von den Computern genutzt wird. Mehr dazu erfahren Sie unter [Welche Richtlinien sind einer Gruppe zugewiesen?](#) (Seite 25).
2. Stellen Sie sicher, dass On-Access-Scans in der Richtlinie aktiviert sind und die Computer richtlinienkonform sind.
Nähere Informationen hierzu finden Sie unter [Aktivieren/Deaktivieren der On-Access-Scans](#) (Seite 97) und [Durchsetzen von Gruppenrichtlinien](#) (Seite 31).

32.2 Die Firewall ist deaktiviert

Wenn die Firewall auf einigen Computern deaktiviert ist:

1. Prüfen Sie, welche Firewall-Richtlinie von den Computern verwendet wird. Mehr dazu erfahren Sie unter [Welche Richtlinien sind einer Gruppe zugewiesen?](#) (Seite 25).
2. Stellen Sie sicher, dass die Firewall in der Richtlinie aktiviert wird und die Computer richtlinienkonform sind.
Nähere Informationen hierzu finden Sie unter [Vorübergehende Deaktivierung der Firewall](#) (Seite 126) und [Durchsetzen von Gruppenrichtlinien](#) (Seite 31).

32.3 Firewall nicht installiert

Hinweis: Bei rollenbasierter Administration ist zur Installation der Firewall die Berechtigung **Computersuche, -schutz und -gruppen** erforderlich. Weitere Informationen finden Sie unter [Rollen und Teilverwaltungseinheiten](#) (Seite 13).

Vor der Installation der Client-Firewall stellen Sie Folgendes sicher:

- Die Firewall ist im Umfang Ihrer Lizenz enthalten.
- Auf den Computern läuft Windows 2000 oder höher.

Hinweis: Sie können die Firewall nicht auf Computern mit Server-Betriebssystemen oder Windows Vista Starter installieren.

Verfahren Sie wie folgt, wenn Sie die Firewall auf Computern installieren möchten:

1. Wählen Sie die gewünschten Computer aus, rechtsklicken Sie auf die Auswahl und wählen Sie **Computer schützen**.
Der **Assistent zum Schutz für Computer** wird gestartet. Klicken Sie auf **Weiter**.
2. Wählen Sie bei entsprechender Aufforderung die Option **Firewall**. Beenden Sie den Assistenten.

Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support von Sophos.

32.4 Computer mit ausstehenden Alerts

- Befindet sich auf Computern ein Virus oder eine unerwünschte Anwendung, verfahren Sie anhand der Anweisungen im Abschnitt [Sofortiges Bereinigen von Computern](#) (Seite 58).
- Wenn Computer jedoch Adware oder eine potenziell unerwünschte Anwendung umfassen, die *erwünscht* ist, befolgen Sie die Anweisungen im Abschnitt [Zulassen von Adware und PUA](#) (Seite 90).
- Bei nicht aktuellen Computern finden Sie im Abschnitt [Updaten nicht aktueller Computer](#) (Seite 68) Anweisungen zur Fehlersuche und Problembehebung.

Hinweis: Wenn der Alert nicht mehr angezeigt werden soll, können Sie ihn löschen. Markieren Sie die Computer mit Alerts, rechtsklicken Sie auf die Auswahl und wählen Sie **Alerts und Fehler löschen**. Sie müssen zur **Korrektur – Bereinigung** berechtigt sein, um Fehler und Alerts löschen zu können.

32.5 Computer werden nicht von der Konsole verwaltet

Windows-, Mac-, Linux und UNIX-Computer sollten von Enterprise Console verwaltet werden, so dass sie aktualisiert und überwacht werden können.

Hinweis: Wenn Sie keine Synchronisierung über Active Directory durchgeführt haben (siehe [Informationen zur Synchronisierung mit Active Directory](#) (Seite 36)), werden neue Netzwerkcomputer nicht automatisch von der Konsole angezeigt bzw. verwaltet. Klicken Sie in der Symbolleiste auf **Computer suchen**, um nach diesen Computern zu suchen und sie in der Gruppe **Nicht zugewiesen** abzulegen.

Wenn ein Computer nicht verwaltet wird, werden seine Details auf der Registerkarte **Status** grau angezeigt.

So können nicht verwaltete Computer verwaltet werden:

1. Wählen Sie im Dropdown-Menü **Ansicht** die Option **Nicht verwaltete Computer**.
2. Markieren Sie alle aufgelisteten Computer. Rechtsklicken Sie auf die Auswahl und wählen Sie **Computer schützen**, um eine verwaltete Version von Sophos Endpoint Security and Control zu installieren.
3. Führen Sie auf Computern, auf denen Enterprise Console Endpoint Security and Control nicht automatisch installieren kann, eine manuelle Installation durch.
Mehr dazu erfahren Sie in der *Erweiterten Startup-Anleitung für Sophos Endpoint Security and Control*.

32.6 Schutz von Computern in der Gruppe „Nicht zugewiesen“ nicht möglich

Die Gruppe **Nicht zugewiesen** ist für Computer gedacht, die noch in keine Gruppe eingegliedert wurden und auf die sich Richtlinien übertragen lassen. Computer werden erst geschützt, wenn sie sich in einer Gruppe befinden.

32.7 Sophos Endpoint Security and Control konnte nicht installiert werden

Wenn der **Assistent zum Schutz von Computern** Sophos Endpoint Security and Control nicht auf Computern installieren kann, kann dies folgende Ursache haben:

- Enterprise Console konnte das Betriebssystem der Computer nicht ermitteln. Sie haben wahrscheinlich bei der Computersuche Ihren Benutzernamen nicht im Format **Domäne\Benutzer** eingegeben.
- Auf dem Betriebssystem ist eine automatische Installation nicht möglich. Führen Sie eine manuelle Installation durch. Anweisungen hierzu entnehmen Sie bitte der *Erweiterten Startup-Anleitung* zu Sophos Endpoint Security and Control.
- Die Computer werden von einer Firewall geschützt.
- Die „Einfache Dateifreigabe“ wurde auf Windows XP-Computern nicht deaktiviert.
- Die Option **Freigabe-Assistent verwenden** wurde unter Windows Vista nicht deaktiviert.
- Sie haben eine Funktion ausgewählt, die nicht auf diesem Betriebssystem unterstützt wird.

Wenn die Installation von Compliance Agent nicht durchgeführt werden kann oder ein Fehler auftritt, können Sie das Compliance Agent-Installationsprotokoll aufrufen. Das Protokoll befindet sich im Ordner %tmp%.

Die Systemvoraussetzungen für Sophos Endpoint Security and Control entnehmen Sie bitte der Sophos Website: <http://www.sophos.de/products/all-sysreqs.html>.

32.8 Computer werden nicht upgedatet

Im Abschnitt *Updaten nicht aktueller Computer* (Seite 68) finden Sie Hinweise zur Fehlersuche und Problembeseitigung.

32.9 Virenschutzeinstellungen werden von Macs nicht übernommen

Manche Virenschutzeinstellungen können von Macintosh-Computern nicht übernommen werden. In diesem Fall wird auf der entsprechenden Seite eine Warnung angezeigt.

Sie können Virenschutzeinstellungen auf Mac-Computern mithilfe des Sophos Update Managers ändern, einem Dienstprogramm, das mit Sophos Anti-Virus für Mac OS X geliefert wird. So öffnen Sie den Sophos Update Manager: Öffnen Sie auf einem Mac ein **Finder**-Fenster und rufen Sie den Ordner **Sophos Anti-Virus:ESOSX** auf. Doppelklicken Sie auf **Sophos Update Manager**. Weitere Details werden in der Hilfe zu Sophos Update Manager aufgeführt.

32.10 Virenschutzeinstellungen werden von Linux oder UNIX nicht übernommen

Manche Virenschutzeinstellungen können von Linux- oder UNIX-Computern nicht übernommen werden. In diesem Fall wird auf der entsprechenden Seite eine Warnung angezeigt.

Sie können die Virenschutzeinstellungen unter Linux über die Befehle **savconfig** und **savscan** ändern. Nähere Anweisungen hierzu finden Sie im *Benutzerhandbuch zu Sophos Anti-Virus für Linux*. Sie können Virenschutzeinstellungen unter UNIX über den Befehl **savscan** ändern. Nähere Anweisungen hierzu finden Sie im *Benutzerhandbuch für Sophos Anti-Virus für UNIX*.

32.11 Linux- oder UNIX-Computer stimmt nicht mit Richtlinie überein

Wenn Sie eine Unternehmens-Konfigurationsdatei im zentralen Installationsverzeichnis verwenden und die Datei einen Konfigurationseintrag enthält, der mit der Richtlinie in Konflikt steht, wird der Computer als nicht richtlinienkonform angezeigt.

Wenn Sie die Option **Konformität mit Richtlinie** wählen, wird der Computer nur vorübergehend in Übereinstimmung gebracht, bis die CID-basierte Konfiguration erneut übertragen wird.

Prüfen Sie die Unternehmens-Konfigurationsdatei und ersetzen Sie die Konsolen-basierte Konfiguration, falls möglich.

32.12 Keine Übernahme der Einstellungen von On-Access-Scans

Unter Umständen sind Änderungen an Einstellungen von On-Access-Scans unter Windows 95 und 98 wirkungslos. Auf den entsprechenden Seiten wird dazu eine Warnung angezeigt.

In diesem Fall werden Änderungen an den Einstellungen für geplante Scans auch für On-Access-Scans übernommen. Der Grund dafür liegt am Design von Sophos Anti-Virus für ältere Windows-Versionen.

32.13 Unerwarteter Scan unter Windows 2000 oder höher

Bei einer lokalen Version von Sophos Anti-Virus unter Windows 2000 oder höher wird eventuell ein „verfügbarer Scan“ in der Liste aufgeführt, obwohl der Benutzer keinen erstellt hat.

Bei dem neuen Scan handelt es sich eigentlich um einen geplanten Scan, den Sie von der Konsole aus eingerichtet haben. Löschen Sie den Scan nicht.

32.14 Verbindungs- und Zeitüberschreitungsprobleme

Wenn die Kommunikation zwischen Enterprise Console und einem Computer im Netzwerk langsam wird oder der Computer nicht reagiert, kann ein Verbindungsproblem bestehen.

Sehen Sie im Sophos Netzwerkkommunikations-Report nach, der einen Überblick des aktuellen Kommunikationsstatus zwischen einem Computer und Enterprise Console gibt. Um den Report anzusehen, gehen Sie zu dem Computer, auf dem das Problem aufgetreten ist. Klicken Sie in der Taskleiste auf die Schaltfläche **Start** und wählen Sie dann **Programme > Sophos > Sophos Endpoint Security and Control** und klicken Sie auf **Sophos Netzwerkkommunikations-Report ansehen**.

Der Report zeigt mögliche Problemursachen an. Wenn ein Problem erkannt wird, werden Abhilfemaßnahmen vorgeschlagen.

32.15 Adware/PUA werden nicht erkannt

Wenn Adware und andere potenziell unerwünschte Anwendungen (PUA) nicht erkannt werden, prüfen Sie Folgendes:

- Die Erkennung wurde aktiviert. Mehr dazu erfahren Sie unter [Scannen auf Adware und PUA](#) (Seite 89).
- Anwendungen werden auf einem Computer unter Windows 2000 oder höher ausgeführt.

32.16 Zum Teil erkanntes Objekt

Sophos Endpoint Security and Control kann melden, dass ein Objekt (z.B. ein Trojaner oder eine potenziell unerwünschte Anwendung) zum Teil erkannt wurde. Das bedeutet, dass Sophos Anti-Virus nicht alle Komponenten dieser Anwendung gefunden hat.

Die verbleibenden Komponenten können Sie über eine vollständige Systemüberprüfung der betroffenen Computer auffinden. Auf Computern unter Windows 2000 und höher können Sie hierzu den/die Computer auswählen, darauf rechtsklicken und **Vollständige Systemüberprüfung** wählen. Sie können außerdem einen **geplanten Scan** zur Erkennung von Adware und anderen potenziell unerwünschten Anwendungen einrichten. Mehr dazu erfahren Sie unter [Scannen auf Adware und PUA](#) (Seite 89).

Wenn die Anwendung noch immer nicht vollständig erkannt wurde, kann es dafür folgende Gründe geben:

- Sie haben keine ausreichenden Zugriffsrechte.
- Einige Laufwerke oder Ordner auf dem Computer, die die Komponenten der Anwendung enthalten, sind vom Scan ausgeschlossen.

In letzterem Fall prüfen Sie die **Liste der vom Scan ausgeschlossenen Objekte** (mehr dazu erfahren Sie unter [Ausschließen von Objekten von On-Access-Scans](#) (Seite 92)). Wenn die Liste Objekte enthält, entfernen Sie diese und wiederholen Sie den Scan-Vorgang.

Sophos Endpoint Security and Control kann Adware und potenziell unerwünschte Anwendungen, deren Komponenten auf Netzlaufwerken installiert wurden, eventuell nicht vollständig erkennen oder entfernen.

Wenn Sie Hilfe benötigen, wenden Sie sich bitte an den technischen Support von Sophos.

32.17 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.

Ursache dafür kann sein, dass einige Arten potenziell unerwünschter Anwendungen Dateien "überwachen" und versuchen, häufig auf sie zuzugreifen. Bei aktiviertem On-Access-Scanning erkennt Sophos Endpoint Security and Control jeden Dateizugriff und gibt einen Alert aus.

Führen Sie einen der folgenden Schritte durch:

- Deaktivieren Sie On-Access-Scans auf Adware/PUA. Sie können stattdessen eine geplanten Scan verwenden.
- Lassen Sie die Anwendung zu (wenn sie auf Ihren Computern ausgeführt werden soll). Mehr dazu erfahren Sie unter [Zulassen von Adware und PUA](#) (Seite 90).
- Bereinigen Sie die Computer, indem Sie Anwendungen entfernen, die Sie nicht zugelassen haben. Mehr dazu erfahren Sie unter [Sofortiges Bereinigen von Computern](#) (Seite 58).

32.18 Bereinigung fehlgeschlagen

Wenn Endpoint Security and Control Objekte nicht bereinigen kann („Bereinigung fehlgeschlagen“), kann es dafür folgenden Grund geben:

- Sophos Anti-Virus hat nicht alle Komponenten eines aus mehreren Komponenten bestehenden Objekts gefunden. Führen Sie eine vollständige Systemüberprüfung der Computer durch, um die anderen Komponenten zu suchen. Mehr dazu erfahren Sie unter [Sofort-Scans](#) (Seite 67).
- Einige Laufwerke oder Ordner, die Komponenten des Objekts enthalten, wurden vom Scan-Vorgang ausgeschlossen. Prüfen Sie die von der Scan-Vorgang ausgeschlossenen Objekte. Anweisungen hierzu Sie unter [Ausschließen von Objekten von On-Access-Scans](#) (Seite 92). Wenn sich Objekte in der Liste befinden, entfernen Sie diese.
- Sie haben keine ausreichenden Zugriffsrechte.
- Die Software kann diese Objektart nicht bereinigen.
- Die Software hat nur ein Virenfragment erkannt.
- Das Objekt befindet sich auf einer schreibgeschützten Diskette oder CD.
- Das Objekt befindet sich auf einem schreibgeschützten NTFS-Volumen (Windows 2000 oder höher).

32.19 Wiederherstellung bei Folgeerscheinungen von Viren

Eine Bereinigung kann zwar einen Virus vom Computer entfernen, aber nicht immer die Folgeerscheinungen rückgängig machen.

Bei einigen Viren treten keine Folgeerscheinungen auf. Andere können Änderungen vornehmen oder Daten so beschädigen, dass sie schwer zu erkennen sind. Gehen Sie damit folgendermaßen um:

- Klicken Sie im **Hilfe**-Menü auf **Objekt-Infos**. Dadurch werden Sie mit der Sophos Website verbunden, auf der Sie die Virenanalyse lesen können.
- Ersetzen Sie infizierte Programme durch Sicherungskopien oder Original-Programme. Wenn Sie vor dem Virenbefall keine Sicherungskopien angefertigt haben, sollten Sie diese jetzt auf jeden Fall für die Zukunft erstellen.

Manchmal lassen sich jedoch noch Daten auf von Viren beschädigten Festplatten retten. Sophos verfügt über Tools zur Behebung bestimmter Virenschäden. Der technische Support kann Ihnen bei der Problembekämpfung behilflich sein.

32.20 Wiederherstellung nach Folgeerscheinungen unerwünschter Anwendungen

Eine Bereinigung kann zwar unerwünschte Anwendungen von dem Computer entfernen aber nicht immer die Folgeerscheinungen rückgängig machen.

Durch bestimmte Anwendungen werden Änderungen am Betriebssystem vorgenommen (z.B. werden Einstellungen der Internetverbindung modifiziert). Sophos Endpoint Security and Control kann nicht immer alle Einstellungen wiederherstellen. Wenn beispielsweise eine Anwendung die Browser-Startseite geändert hat, kennt Sophos Endpoint Security and Control die vorherige Einstellung nicht.

Einige Anwendungen installieren Dienstprogramme auf Ihrem Computer, wie z.B. .dll- oder .ocx-Dateien. Wenn ein Dienstprogramm harmlos (d.h. dass es nicht die Eigenschaften einer potenziell unerwünschten Anwendung besitzt), z.B. eine Sprach-Library, und kein wesentlicher Teil der Anwendung ist, erkennt es Sophos Endpoint Security and Control möglicherweise nicht als Teil der Anwendung. In diesem Fall wird die Datei durch eine Bereinigung nicht aus Ihrem Computer entfernt.

Manchmal ist eine Anwendung, wie Adware, Teil eines Programms, das Sie absichtlich installiert haben, und für die Funktion des Programms erforderlich. Wenn Sie die Anwendung entfernen, funktioniert das Programm auf Ihrem Computer möglicherweise nicht mehr.

Gehen Sie folgendermaßen vor:

- Klicken Sie im **Hilfe**-Menü auf **Objekt-Infos ansehen**. Dadurch werden Sie mit der Sophos Website verbunden, auf der Sie die Anwendungsanalyse lesen können.
- Stellen Sie die gewünschten Systemeinstellungen oder Programme über Sicherungskopien wieder her. Wenn Sie noch keine Sicherungskopien erstellt haben, sollten Sie diese jetzt auf jeden Fall für die Zukunft erstellen.

Der technische Support von Sophos kann Ihnen Hilfe oder weitere Hinweise zur Wiederherstellung bei Folgeerscheinungen von Adware/potenziell unerwünschten Anwendungen bereitstellen.

32.21 Data Control erkennt keine Dateien, die über integrierte Browser hochgeladen wurden

Data Control fängt Dokumente ab, die über eigenständige Browser hochgeladen werden. Dokumente, die über in Fremdsoftware integrierte Browser (z.B. Lotus Notes) hochgeladen werden, werden jedoch nicht erkannt. Wenn Sie über Software mit einem integrierten Browser arbeiten und hochgeladene Dokumente überprüfen möchten, müssen Sie in Ihrer Software einstellen, dass die Anwendung in einem externen Browser geöffnet wird.

32.22 Der deinstallierte Update Manager wird in der Konsole angezeigt

Wenn Sie einen weiteren Update Manager deinstalliert haben, wird er bisweilen noch in der Ansicht **Update Manager** in Enterprise Console angezeigt.

Um den Update Manager aus der Konsole zu entfernen, rechtsklicken Sie darauf und wählen Sie **Löschen**.

33 Glossar

Active Directory-Synchronisierungsereignis	Ereignis, das bei einer Active Directory-Synchronisierung auftritt.
Advanced Content Control List Editor	Editor zum Erstellen benutzerdefinierter „Content Control Lists“. „Content Control Lists“ umfassen die Komponenten: „Bewertung“, „Höchstzahl“, „regulärer Ausdruck“ sowie die sog. „Schwellenbewertung“, die erzielt werden muss, damit eine Übereinstimmung mit der Content Control List vorliegt.
Aktive Teilverwaltungseinheit	Eine im Gruppenfenster angezeigte Teilverwaltungseinheit.
Alte Update-Richtlinie	Eine vor dem Upgrade von Sophos Enterprise Console von Version 3.x auf Version 4.0 verwendete Update-Richtlinie, die nach dem Upgrade noch so lange eingesetzt wird, bis eine neue Update-Richtlinie eingerichtet wird.
Application Manager	In diesem Fenster lassen sich neue Regeln für von Sophos Client Firewall gesperrte Anwendungen erstellen.
Ausdruck	Siehe unter „regulärer Ausdruck“.
Automatischer Schutz	Installation von Sicherheitssoftware und Richtliniendurchsetzung auf allen Computern in einem Active Directory-Container nach Synchronisierung mit Enterprise Console.
Beispielregel	Regel, die Sophos als Beispiel zur Verfügung stellt. Diese Regeln werden nicht von Sophos aktualisiert.
Benutzerdefinierte Content Control List	Von einem Sophos Kunden erstellte Content Control List. Benutzerdefinierte Content Control Lists können wie folgt erstellt werden: Erstellen Sie eine einfache Liste mit Suchbegriffen und einem Suchparameter (z.B. „nach allen Begriffen“). Sie können jedoch auch den „Advanced Content Control List Editor“ verwenden.
Bewertung	Zahl, die zur Gesamtbewertung einer Content Control List addiert wird, wenn eine Übereinstimmung zu einem regulären Ausdruck vorliegt.
Content Control List (CCL)	Eine Kombination von Bedingungen zur Bestimmung des Inhalts von Dateien (z.B. Kreditkarten- oder Kontodaten oder andere

	personenbezogenen Daten). Es wird zwischen zwei Arten von „Content Control Lists“ unterschieden: „SophosLabs Content Control Lists“ und „benutzerdefinierte Content Control Lists“.
Controlled Application	Anwendung, die aus Gründen der Produktivitätsbeeinträchtigung oder Netzwerkbelastung als unerwünscht betrachtet wird und deshalb gesperrt werden soll.
Controlled Data	Dateien, die Data Control-Bedingungen erfüllen.
Controlled Device	Ein von der Funktion „Device Control“ überwachtes Gerät.
Dashboard	Übersichtliche Darstellung der Netzwerksicherheit.
Dashboard-Ereignis	Auf dem Dashboard angezeigtes Ereignis, wenn eine kritische Sicherheitsstufe überschritten wurde. In diesem Fall wird eine E-Mail-Benachrichtigung erzeugt und verschickt.
Data Control	Kontrollfunktion zur Verhinderung, dass ungewollt Daten von Computern übertragen werden. Der Mechanismus greift, wenn ein Benutzer eine Datei versenden oder anderweitig übertragen möchte, die die Kriterien der „Data Control“-Richtlinie und der entsprechenden Regeln erfüllt. Wird beispielsweise eine Tabelle mit Kundendaten auf einen Wechseldatenträger kopiert oder ein vertrauliches Dokument in einem webbasierten E-Mail-Konto hochgeladen, wird die Übertragung bei entsprechender Konfiguration verhindert.
Dateiregel	Regel zum Bestimmen der zu ergreifenden Maßnahme, wenn ein Benutzer eine Datei mit dem festgelegten Namen oder Typ an das festgelegte Ziel übertragen möchte (z.B. Verhindern der Übertragung von Datenbanken an Wechseldatenträger).
Datenbanken	Komponente von Sophos Enterprise Console, in der alle Daten über die Netzwerkcomputer gespeichert werden.
Device Control	Eine Funktion zur Reduzierung ungewünschter Datenverluste über Computer und Einschränkung der Einführung von Software in das Netzwerk von außerhalb. Diese Funktion spricht an bei Zugriff auf ein nicht zugelassenes Speicher- oder

	Netzwerkgerät auf einem verwalteten Computer im Netzwerk.
Echter Dateityp	Dateityp, der durch Strukturanalyse und nicht anhand der Dateierweiterung ermittelt wird. Diese Methode liefert bessere Ergebnisse.
Geräte-Ausschluss	Ein von der Funktion „Device Control“ nicht zu berücksichtigendes Gerät.
Gesamtbewertung	Alle Bewertungen einer Content Control List, je nach berücksichtigtem Content.
Gruppe	Gruppe von Sophos Enterprise Console verwalteter Computer.
Höchstzahl	Maximal zugelassene Übereinstimmungen eines regulären Ausdrucks, die in die Gesamtbewertung eingehen.
Inhaltsregel	Eine Inhaltsregel umfasst mindestens eine Content Control List. Hierin wird die Maßnahme festgelegt, die bei der Übertragung von Daten, die alle Bedingungen der Content Control Lists der Regel erfüllen, an den festgelegten Zielort ergriffen werden soll.
IT-Verwaltungseinheit	IT-Umgebung eines Unternehmens, u.a. bestehend aus Computern und Netzwerkinfrastruktur.
Kategorie	Kriterium zur Kategorisierung von Control Lists der SophosLabs Content nach Typ, Content-Regulierung oder Region.
Kriterium	Deskriptor einer SophosLabs Content Control List zum Bestimmen der Inhalte oder des Umfangs der Liste. Es gibt drei Kriterien: Typ, Regulierung und Region.
Kritische Stufe	Dieser Wert ändert den Sicherheitsstatus eines Objekts in „kritisch“.
Management-Konsole	Die Komponente von Sophos Enterprise Console zur Verwaltung und zum Schutz von Computern.
Management-Server	Die Komponente von Sophos Enterprise Console zur Abwicklung der Updates und der Kommunikation zwischen Netzwerkcomputern.
Manipulationsschutz	Mit dem Manipulationsschutz können Sie verhindern, dass bekannte Malware sowie nicht autorisierte Benutzer (lokale Administratoren und Benutzer ohne hinreichende Fachkenntnisse) Sophos Sicherheitssoftware deinstallieren bzw. mit

	Sophos Endpoint Security and Control deaktivieren.
Menge	Anzahl der Content Control List-Schlüsseldaten, die eine Datei umfassen muss, damit eine Übereinstimmung mit der Content Control List vorliegt.
Mengenschlüssel	In der Content Control List festgelegte Schlüsseldaten, deren Menge bestimmt wird. Wenn eine Content Control List beispielsweise Kreditkarten- oder Bankdaten enthält, bestimmen die Mengeneinstellungen, wie viele Daten maximal in der Datei vorhanden sein können, ohne dass eine Übereinstimmung mit der Content Control List vorliegt.
Recht	Ein Satz von Berechtigungen zum Ausführen bestimmter Aufgaben über Enterprise Console.
Regel	In Regeln werden die Maßnahmen festgelegt, die ergriffen werden, wenn Dateien bestimmte Bedingungen erfüllen. Es wird zwischen Dateiregeln und Inhaltsregeln unterschieden.
Region	Geltungsbereich einer SophosLabs Content Control List. Hier wird das Land festgelegt, auf das sich die Content Control List bezieht (bei länderspezifischen Content Control Lists). Länderunspezifische Content Control Lists werden als „global“ ausgewiesen.
Regulärer Ausdruck	Suchzeichenfolge, die Textmuster in Dateien mit bestimmten Zeichen abgleicht. Data Control arbeitet mit regulärer Ausdruckssyntax von Perl 5.
Richtlinie	Eine Ansammlung von Einstellungen für einen bestimmten Zweck, die auf Computergruppen übertragen werden.
Rolle	Ein Satz von Rechten zur Bestimmung des Zugriffs auf Enterprise Console.
Rollenbasierte Verwaltung	Verteilung von Zugriffsrechten auf bestimmte Computer und Prozesse basierend auf der Rolle eines Benutzers im Unternehmen.
Schwellenbewertung	Erforderliche Trefferanzahl eines regulären Ausdrucks, damit eine Übereinstimmung mit der Content Control List vorliegt.

Schwellenwert	Wert, der den Sicherheitszustand eines Objekts in „Warnung“ oder „kritisch“ ändert.
Server-Stammknoten	Der oberste Knoten einer Gruppenstruktur im Fenster Gruppen (einschl. der Gruppe Nicht zugewiesen).
Software-Abonnement	Ausgewählte Softwareversionen für unterschiedliche Systeme, die vom Update Manager heruntergeladen und auf dem neuesten Stand gehalten werden. Für jedes System können ausgesuchte Versionen abonniert werden (z.B. „Neueste“ für „Windows 2000 und höher“).
Sophos Enterprise Console	Software zur Installation und Verwaltung von Sophos Produkten auf Netzwerkcomputern.
Sophos Live-Schutz	Mit dieser Funktion lässt sich über ein "In-the-Cloud"-Verfahren sofort feststellen, ob eine Datei eine Bedrohung darstellt. Bei Bedarf werden umgehend die in der Schutzkonfiguration von Sophos Anti-Virus festgelegten Maßnahmen ergriffen.
SophosLabs Content Control List	Von Sophos bereitgestellte und verwaltete Content Control List. Sophos aktualisiert SophosLabs Content Control Lists und erstellt neue Content Control Lists, die in Enterprise Console verfügbar gemacht werden. SophosLabs Content Control Lists können inhaltlich nicht bearbeitet werden. Die Menge dieser Content Control Lists ist jedoch variabel.
Sophos Update Manager (SUM)	Programm zum Download von Sophos Sicherheitssoftware und Updates von Sophos oder einem anderen Update-Server in freigegebene Update-Verzeichnisse.
Standardteilverwaltungseinheit	Teilverwaltungseinheit, deren Stamm der Server-Stammknoten der Gruppenstruktur und der Gruppe Nicht zugewiesen ist. Sie wird beim ersten Start von Enterprise Console automatisch angezeigt.
Statusanzeige	Oberbegriff für Symbole, die den Sicherheitszustand eines Dashboards-Objekts oder der Netzwerkintegrität darstellen.
Synchronisierte Gruppe	Eine Gruppe unterhalb des Synchronisierungspunkts.

Synchronisierung mit Active Directory	Einweg-Synchronisierung von Gruppen in Sophos Enterprise Console mit Organisationseinheiten oder Containern von Active Directory.
Synchronisierungsintervall	Zeitraum, nach dessen Ablauf ein Synchronisierungspunkt in Enterprise Console mit dem ausgewählten Active Directory-Container synchronisiert wird.
Synchronisierungspunkt (in Active Directory-Struktur)	Gruppe in Sophos Enterprise Console, in die der Inhalt eines ausgewählten Active Directory-Containers (Gruppen und Computer oder nur Gruppen) zur Synchronisierung verschoben wird, wobei die Struktur unversehrt bleibt.
Systemadministrator	<p>Eine vorkonfigurierte Rolle für die Verwaltung von Sophos Sicherheitssoftware im Netzwerk und Rollen in Enterprise Console.</p> <p>Die Rolle „Systemadministrator“ kann nicht gelöscht, mit neuen Rechten versehen oder umbenannt werden. Die Windows-Gruppe „Sophos Full Administrators“ muss Bestandteil der Rolle sein. Andere Benutzer und Gruppen können jedoch hinzugefügt bzw. gelöscht werden.</p>
Teilverwaltungseinheit	Ein benannter Teil der IT-Verwaltungseinheit, der eine Untermenge der Computer und Gruppen ausmacht.
Teilverwaltungseinheitsadministration	Funktion zur Einschränkung der Computer und Gruppen, auf denen Vorgänge ausgeführt werden können.
Typ	Kriterien zur Kategorisierung von SophosLabs Content Control Lists. So wird etwa eine Content Control List, die Ausweisdaten, Postanschrift oder E-Mail-Adressen umfasst, dem Typ „Personally Identifiable Information“ (personenbezogene Daten) zugeordnet.
Update Manager	Siehe unter „Sophos Update Manager“.
Veralteter Computer	Computer mit Sophos Software, die nicht mehr auf dem neuesten Stand ist.
Verwalteter Computer	Computer mit Remote Management System (RMS), auf dem über Sophos Enterprise Console Software installiert und aktualisiert werden kann und Berichte erstellt werden können.
Verwaltungseinheit	Siehe unter „IT-Verwaltungseinheit“.

Warnstufe

Wert, der die Sicherheitsstufe eines Objekts in „Warnung“ ändert.

34 Technischer Support

Technischen Support zu Sophos Produkten können Sie wie folgt abrufen:

- Rufen Sie das SophosTalk-Forum unter <http://community.sophos.com/> auf und suchen Sie nach Benutzern mit dem gleichen Problem.
- Durchsuchen Sie die Support-Knowledgebase unter <http://www.sophos.de/support/>.
- Laden Sie Dokumentation zu den Produkten unter <http://www.sophos.de/support/docs/> herunter.
- Senden Sie eine E-Mail an den technischen Support support@sophos.de und geben Sie die Versionsnummer(n), Betriebssystem(e) und Patch Level Ihrer Sophos Software sowie ggf. den genauen Wortlaut von Fehlermeldungen an.

35 Rechtlicher Hinweis

Copyright © 2010 Sophos Group. Alle Rechte vorbehalten. Kein Teil dieser Publikation darf in jeglicher Form, weder elektronisch oder mechanisch, reproduziert, elektronisch gespeichert oder übertragen werden, noch fotokopiert oder aufgenommen werden, es sei denn, Sie haben entweder eine gültige Lizenz, gemäß der die Dokumentation in Übereinstimmung mit den Lizenzvereinbarungen reproduziert werden darf oder Sie haben eine schriftliche Genehmigung des Copyright-Inhabers.

Sophos und Sophos Anti-Virus sind eingetragene Warenzeichen der Sophos Plc und Sophos Group. Alle anderen erwähnten Produkt- und Unternehmensnamen sind Warenzeichen oder eingetragene Warenzeichen der jeweiligen Inhaber.

ACE™, TAO™, CIAO™, and CoSMIC™

ACE¹, TAO², CIAO³, and CoSMIC⁴ (henceforth referred to as “DOC software”) are copyrighted by Douglas C. Schmidt⁵ and his research group⁶ at Washington University⁷, University of California⁸, Irvine, and Vanderbilt University⁹, Copyright © 1993–2005, all rights reserved.

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

You can use DOC software in commercial and/or binary software releases and are under no obligation to redistribute any of your source code that is built using DOC software. Note, however, that you may not do anything to the DOC software code, such as copyrighting it yourself or claiming authorship of the DOC software code, that will prevent DOC software from being distributed freely using an open-source development model. You needn't inform anyone that you're using DOC software in your software, though we encourage you to let us¹¹ know so we can promote your project in the DOC software success stories¹².

DOC software is provided as is with no warranties of any kind, including the warranties of design, merchantability, and fitness for a particular purpose, noninfringement, or arising from a course of dealing, usage or trade practice. Moreover, DOC software is provided with no support and without any obligation on the part of Washington University, UC Irvine, Vanderbilt University, their employees, or students to assist in its use, correction, modification, or enhancement. A number of companies¹³ around the world provide commercial support for DOC software, however. DOC software is Y2K-compliant, as long as the underlying OS platform is Y2K-compliant.

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

The ACE¹⁴, TAO¹⁵, CIAO¹⁶, and CoSMIC¹⁷ web sites are maintained by the DOC Group¹⁸ at the Institute for Software Integrated Systems (ISIS)¹⁹ and the Center for Distributed Object Computing of Washington University, St. Louis²⁰ for the development of open-source software as part of the open-source software community²¹. By submitting comments, suggestions, code, code snippets, techniques (including that of usage), and algorithms, submitters acknowledge

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

The names ACE, TAO, CIAO, CoSMIC, 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 me²² know.

Douglas C. Schmidt²³

Quellen

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

Apache

The Sophos software that is described in this document may include some software programs that are licensed (or sublicensed) to the user under the Apache License. A copy of the license

agreement for any such included software can be found at
<http://www.apache.org/licenses/LICENSE-2.0>.

Common Public License

The Sophos software that is described in this document includes or may include some software programs that are licensed (or sublicensed) to the user under the Common Public License (CPL), which, among other rights, permits the user to have access to the source code. The CPL requires for any software licensed under the terms of the CPL, which is distributed in object code form, that the source code for such software also be made available to the users of the object code form. For any such software covered under the CPL, the source code is available via mail order by submitting a request to Sophos; via email to support@sophos.com or via the web at <http://www.sophos.com/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>

iMatix SFL

This product uses parts of the iMatix SFL, Copyright © 1991-2000 iMatix Corporation
<http://www.imatix.com>.

OpenSSL cryptographic toolkit

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

OpenSSL license

Copyright © 1998–2006 The OpenSSL Project. Alle Rechte vorbehalten.

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

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

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

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

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

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

Original SSLeay license

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

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

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

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

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

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

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

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

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

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

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED

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

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

Index

A

- Abonnement-Alerts 163
- Abonnements 70
 - Auswahl 103
 - Hinzufügen 71
- Abonnieren von Software 71
- Active Directory
 - Importieren aus 32
 - Synchronisierung 38
 - Synchronisierungs-Benachrichtigungen 171
- Adware 89
- Adware/PUA
 - Zulassen 90
- Aktivieren
 - Web-Schutz 95
- Alert-Symbole 54
- Alerts 54, 163
 - Abonnements 163
 - Application Control 167
 - Beheben 55
 - Desktop 166
 - E-Mail 164
 - Informationen zu erkannten Objekten 56
 - Löschen 56
 - Netzwerkstatus 170
 - SNMP 165
 - Synchronisierung mit Active Directory 171
 - Umgang mit 55
 - Update Manager 57
- alte Update-Richtlinien 110
 - alternative Update-Quelle 113
 - automatisch 110
 - Bandbreite 117
 - bei Internetverbindung 115
 - Erstinstallationsquelle 117
 - erweiterte Einstellungen 117
 - primäre Update-Quelle 112
 - Primärserver 112
 - Protokollierung 118
 - Proxyserver 116
 - sekundäre Update-Quelle 113
 - Sekundärserver 113
 - Standardverzeichnisse 119
 - über Proxyserver 116
 - Zeitpläne 114

- alternative Update-Quelle 108
- Ändern von Richtlinien 30
- Ändern von Rollen 16
- Anti-Virus 83
- Antivirus- und HIPS-Richtlinie 83
- Application Control 130, 131
 - Alerts 167
 - Ereignisse 62
- Application Control-Richtlinie 130
- Archivdateien 94
- Assistent zum Schützen von Computern
 - Funktionsauswahl 45
 - Zugangsdaten 45
- Ausschlüsse 101
 - geplante Scans 100
 - On-Access-Scans 92
- Auswahl der Software 75
- Auswahl von Abonnements 103
- automatische Bereinigung 59
- automatische Desinfektion 59
- Automatische Updates 103
- Automatischer Schutz
 - bei Synchronisierung mit Active Directory 40

B

- Bandbreite
 - Verringern 104
- Beheben von Alerts
 - Bereinigungsstatus 55
 - Informationen zu erkannten Objekten 56
 - zu ergreifende Maßnahmen 55, 56
- Benachrichtigung 163
- Benutzeroberfläche
 - Endpoint-Ansicht 5
 - Update Manager-Ansicht 5
- Benutzeroberfläche von Enterprise Console
 - Endpoint-Ansicht 5
 - Update Manager-Ansicht 5
- Benutzerrollen
 - Anzeigen 18
- Berechtigungen 18
 - Hinzufügen 16
 - Zuweisen 16
- Bereinigung 55, 58
 - automatisch 59
 - fehlgeschlagen 194
 - manuell 58
- Bereinigungsstatus 55
- Bereitstellung von Software 76

Bootstrap-Verzeichnisse 46

C

Computer mit aktuellem Schutz

Überprüfen 52

Computer mit Problemen 52

Computer-Details

Drucken 186

Kopieren 185

Computerliste

Drucken von Daten 185

Kopieren von Daten 185

Computersuche 32

Active Directory 32

Content Control Lists

Ändern 145

Ändern mit dem Advanced Editor 146

Erstellen 145

Erstellen mit dem Advanced Editor 146

Content Control-Inhaltsregeln

Erstellen 140

Controlled Applications

Scannen auf 131

sperrern 131

Controlled Applications, Deinstallieren 132

D

Dashboard

Konfigurieren 51

Übersicht 48

Data Control

Advanced Content Control List Editor 146

Aktivieren 138

Aktivieren von Data Control 138

Aktivieren/Deaktivieren 138

Alerts 167

Ändern von Content Control Lists 145

Ausschließen von Dateien 143

CCL 136

Content Control Lists 136

Dateiregeln 138

Entfernen von Regeln aus einer Richtlinie 143

Ereignisse 63, 137

Erstellen von Content Control Lists 145

Exportieren von Content Control Lists 148

Exportieren von Regeln 144

Hinzufügen von Regeln zu einer Richtlinie 142

Importieren von Content Control Lists 148

Data Control (*Fortsetzung*)

Importieren von Regeln 144

Inhaltsregeln 140

Maßnahmen 133

Regelbedingungen 133

Regeln 136

Übersicht 133

Data Control-Regeln

Hinzufügen zu einer Richtlinie 142

Datei- und Druckerfreigabe

Zulassen 123

Dateiregeln für Data Control

Erstellen 138

Deinstallieren von Controlled Applications 132

Desinfektion

automatisch 59

manuell 58

Desinfektion/Beseitigung 58

Desktop-Benachrichtigungen 166

Device Control

Alerts 169

Ausschließen eines Geräts von allen Richtlinien 153

Ausschließen von Geräten von einer Richtlinie 154

Auswahl der Gerätearten 151

Controlled Devices 150

Ereignisse 63, 149

Erkennen und Sperren von Geräten 152

Erkennen und Zulassen von Geräten 152

Liste der ausgeschlossenen Geräte 155

Sperren von Geräten 152

Sperren von Netzwerkbrücken 150

Übersicht 149

Drucken

Computer-Details 186

Computerlistendaten 185

Drucken von Reports 183

E

E-Mail-Benachrichtigungen

Antivirus und HIPS 164

Netzwerkstatus 170

Synchronisierung mit Active Directory 171

Endpoint-Ansicht 5

Drucken von Daten 185

Kopieren von Daten 185

Enterprise Console

Drucken von Daten 185

Enterprise Console (*Fortsetzung*)
Kopieren von Daten 185
Enterprise Console Zugriff 187
Entfernen von Computern aus Gruppen 24
Ereignisprotokoll 172
Ereignisse 62
 Application Control 62
 Data Control 63
 Device Control 63
 Exportieren in eine Datei 66
 Firewall 64
 Manipulationsschutz 65
Erstellen von Gruppen 23
Erstellen von Reports 173, 182
Erstellen von Richtlinien 29
Erstellen von Rollen 15
Erstellen von Teilverwaltungseinheiten 16
Erstinstallationsquelle 106
Erweiterungen 91
Exportieren von Reports 183

F

Fehler
 Löschen 56
Fehlersuche
 ausstehende Alerts 190
 Bereinigung 194
 Data Control, integrierte Browser 196
 deinstallierter Update Manager 196
 Firewall deaktiviert 189
 Firewall nicht installiert 189
 Gruppe „Nicht zugewiesen“ 190
 Linux 192
 Mac 191
 Nicht aktuelle Computer 191
 Nicht verwaltete Computer 190
 Objekt zum Teil erkannt 193
 On-Access-Scans 189
 PUA, Folgeerscheinungen 195
 PUA, Hohe Alert-Anzahl 194
 PUA, nicht erkannt 193
 Sophos Endpoint Security and Control: Installationsproblem 191
 UNIX 192
 Verbindungsprobleme 192
 Virus, Folgeerscheinung 194
 Windows 2000 und aufwärts 192
 Windows NT/95/98 192
 Zeitüberschreitung 192

fehlgeschlagene Bereinigung 194
feste Updates 70
Firewall
 Aktivieren 126
 Deaktivieren 126
 Einrichten 120
 Ereignisse 64
 Erstellen einer Regel 125, 128
 erweiterte Konfiguration 127
 Erweiterte Optionen 127, 129
 Hinzufügen von Prüfsummen 129
 Interaktiver Modus 124
 Lernmodus 124
 Zulassen der Datei- und Druckerfreigabe 123
 Zulassen von Anwendungen 122, 124
Freigeben von Sicherheitssoftware in einem Webserver 82

G

geplante Scans 98, 99
 Ausschließen von Objekten 100
geschützte Computer 48, 51
geschütztes Netzwerk 48
Glossar 197
Gruppe „Nicht zugewiesen“ 7, 190
Gruppen 7, 23
 Entfernen von Computern 24
 Erstellen 23
 Gruppe „Nicht zugewiesen“ 7
 Hinzufügen von Computern 24
 Importieren aus Active Directory 32
 Löschen 25
 Synchronisierung mit Active Directory 38
 Übertragen von Richtlinien 25
 Umbenennen 25
 Verschieben 24
 verwendete Richtlinien 25
 Zuweisen von Richtlinien 25

H

Hinzufügen von Berechtigungen 16
Hinzufügen von Computern 32
Hinzufügen von Computern zu Gruppen 24
HIPS 83, 84
HIPS-Benachrichtigungen
 Desktop 166
 E-Mail 164
 SNMP 165

Host Intrusion Prevention System 84

I

Importieren von Computern
 aus einer Datei 34
In-the-Cloud-Verfahren 87
Installationsproblem
 Sophos Endpoint Security and Control 191

J

Jetzt scannen 67

K

kategorisierte Updates 70
Konfigurieren
 Richtlinien 28
Konfigurieren des Dashboards 51
Konfigurieren des Update Managers 73
Kopieren
 Computer-Details 185
 Computerlistendaten 185

L

Laufzeitverhaltensanalyse 84
Löschen einer Gruppe 25
Löschen von Alerts 56
Löschen von Fehlern 56
Löschen von Richtlinien 30
Löschen von Rollen 15

M

Mac-Viren 94
Macintosh-Dateien
 Scannen 94
Macintosh-Viren 94
Manipulationsschutz
 Aktivieren 161
 Ausschalten 161
 Deaktivieren 161
 Einschalten 161
 Ereignisse 65, 160
 Kennwortänderung 161
 Übersicht 160
Manuelle Bereinigung 58
Manuelle Desinfektion 58

manuelle Updates 68, 115

N

NAC 157, 158, 159
NAC Manager 158
NAC-Richtlinie 158, 159
NAC-Server-URL 157
NAC-URL 157
NAC-Voreinstellungen 158
Network Access Control 157, 158, 159
Netzwerkfreigaben
 unterstützt 77
Netzwerkstatus-Benachrichtigungen 170
neuer Anwender 187
Nicht aktuelle Computer 191
 Auffinden 52
 Update 68
Nicht verwaltete Computer 190
Nutzungsstatistik 72

O

Objekt zum Teil erkannt 193
On-Access-Scans
 Aktivieren 97
 Ausschließen von Objekten 92
 Beim Lesen 98
 Beim Schreiben 98
 Beim Umbenennen 98
 Bereinigung 59
 Deaktivieren 97
 Einschalten 97
 Windows NT/95/98 192

P

potenziell unerwünschte Anwendungen 89
Primärserver 104
 Ändern der Zugangsdaten 107
Prüfsummen 129
PUA 89
 Folgeerscheinungen 195
 Hohe Alert-Anzahl 194
 nicht erkannt 193
Pufferüberlauf 84

R

- Removal Tool
 - Fremdsoftware 44
- Removal-Tool (zur Entfernung von Fremdsoftware) 44
- Report-Zeitpläne erstellen 182
- Reports
 - Alert- und Ereignisverlauf 174
 - Alert-Übersicht 175
 - Alerts und Ereignisse nach Objektname 176
 - Alerts und Ereignisse nach Ort 178
 - Alerts und Ereignisse nach Zeit 177
 - Ausführen 182
 - Darstellung als Tabelle 183
 - Drucken 183
 - Endpoint-Richtlinienabweichung 179
 - Endpoint-Schutz nach Zeit 181
 - Ereignisse nach Benutzer 180
 - Erstellen 173
 - Exportieren 183
 - Layout 184
 - Richtlinienabweichung nach Uhrzeit 179
 - Schutz verwalteter Endpoints 181
 - Übersicht 173
 - Update-Hierarchie 182
 - Zeitpläne 182
- Reports an Sophos 188
- Richtlinien 7
 - Ändern 30
 - Antivirus und HIPS 83
 - Durchsetzen 31
 - Erstellen 29
 - Konfigurieren 28
 - Löschen 30
 - Standard 26
 - Überblick 26
 - Überprüfen 31
 - Übertragen 25, 29
 - Umbenennen 30
 - zugehörige Gruppen 31
 - Zuweisen 25, 29
- Rollen 13
 - Ändern 16
 - Bearbeiten 16
 - Erstellen 15
 - Löschen 15
 - Umbenennen 16
 - vordefiniert 14

Rollen (Fortsetzung)

- Zuweisen von Berechtigungen 16

Rootkits

- Scannen auf 93

S

- Scan-Objekte 91
- Scannen von Computern 67
 - sofort 67
- Scans
 - Ausschlüsse 101
 - geplant 99
- Schutz, Überprüfen 48
- Schützen von Computern
 - Assistent zum Schützen von Computern 45
 - Funktionsauswahl 45
 - Voraussetzungen 43
 - Vorbereiten der Installation 43
 - Zugangsdaten 45
- Sekundärserver 104, 108
- Setup 10
- SNMP-Benachrichtigungen 165
- Sofort-Scan 67
- Sofort-Updates 68, 115
- Software
 - Abonnieren von Sicherheitssoftware 71
 - Auswahl 75
- Sophos Endpoint Security and Control
 - Installationsproblem 191
- Sophos Enterprise Console 4, 5
- Sophos Live-Schutz
 - Aktivieren 88
 - Ausschalten 88
 - Deaktivieren 88
 - Einschalten 88
 - In-the-Cloud-Verfahren 87
 - Überblick 87
- Sophos Update Manager 73
- Sortieren der Computer-Liste
 - Computer mit Problemen 52
 - Ungeschützte Computer 52
- sperren
 - Controlled Applications 131
- Spyware 83
- Starten von NAC Manager 158
- Suchen nach Computern
 - im Netzwerk 33
 - Importieren aus einer Datei 34
 - in einem IP-Bereich 34

Suchen nach Computern (*Fortsetzung*)
 mit Active Directory 33
 Symbole 8
 Synchronisierte Gruppe 38
 Synchronisierung mit Active Directory 36, 38
 Aktivieren 42
 Automatischer Schutz 40
 Deaktivieren 42
 Eigenschaften, ändern 41
 Synchronisierungspunkt 37

T

Teilverwaltungseinheiten 13
 aktiv 17
 Ändern 17
 Auswahl 17
 Bearbeiten 17
 Erstellen 16
 Kopieren 17
 Löschen 18
 Umbenennen 17
 Teilverwaltungseinheiten von Benutzern
 Anzeigen 18
 Trojaner 83

U

Übertragen von Richtlinien 29
 Überwachungsmodus 122
 Umbenennen von Gruppen 25
 Umbenennen von Richtlinien 30
 Umgang mit Alerts 55
 Ungeschützte Computer 52
 unterstützte Netzwerkfreigaben 77
 Update
 manuell 68
 Nicht aktuelle Computer 68
 sofort 68
 Update Manager 73
 Alerts 57
 Anzeige der Konfiguration 73
 Auswahl einer Update-Quelle 74
 Bereitstellung von Software 76
 Hinzufügen 80
 Konfigurieren 73
 Protokollierung 78
 Selbst-Updates 78
 Übernahme der Konfigurationseinstellungen
 80

Update Manager (*Fortsetzung*)
 Übersicht 79
 unterstützte Netzwerkfreigaben 77
 updating 79
 Zeitpläne 77
 zusätzlich 80
 Update Manager-Ansicht 5
 Update-Arten 70
 Update-Quelle 74
 alternativ 108
 primär 104
 sekundär 104, 108
 Web-Server 82
 Update-Server 73
 Update-Zeitplan 77
 Updates
 alt 110
 Arten 70
 automatisch 103
 feste Updates 70
 Freigeben von Sicherheitssoftware in einem
 Webserver 82
 kategorisierte Updates 70
 Zeitpläne 105
 updating
 alternative Update-Quelle 108
 Bandbreite verringern 104
 Erstinstallationsquelle 106
 manuell 115
 primäre Update-Quelle 104
 Primärserver 104
 Protokollierung 107
 Proxy-Details 104
 sekundäre Update-Quelle 104, 108
 Sekundärserver 104, 108
 sofort 115

V

Verbindungsprobleme 192
 verdächtige Dateien 85
 verdächtige Objekte
 vorzeitig zulassen 86
 Zulassen 86
 verdächtiges Verhalten
 Erkennen 84
 Sperren 84
 verwaltete Computer 8
 Viren 83

Viren-Alerts

Desktop 166

E-Mail 164

SNMP 165

Virus

Folgeerscheinungen 194

Vollständige Systemüberprüfung 67

vom Netzwerk getrennte Computer 8

Vorbereitung 10

vordefinierte Rollen 14

vorzeitig zulassen

verdächtige Objekte 86

Website 96

W

Warnsymbole 8

Web-Schutz 95

Website

vorzeitig zulassen 96

Zulassen 96

Würmer 83

Z

Zeitplan für Updates 105

Zeitüberschreitung 192

Zugriff auf Enterprise Console 187

Zulassen

Adware/PUA 90

Verdächtige Objekte 86

Website 96

Zulassen der Datei- und Druckerfreigabe 123

Zuweisen von Berechtigungen 16

Zuweisen von Richtlinien 29