

SOPHOS

simple + secure

Sophos Enterprise Manager Hilfe

Produktversion: 4.7
Stand: Juli 2011



Inhalt

1 Sophos Enterprise Manager.....	3
2 Übersicht über die Oberfläche von Enterprise Manager.....	4
3 Vorbereitung.....	13
4 Einrichtung von Enterprise Manager.....	15
5 Schützen von Computern.....	32
6 Updates.....	48
7 Konfigurieren von Richtlinien.....	64
8 Einrichten von Alerts und Benachrichtigungen.....	122
9 Erstellen von Reports.....	132
10 Kopieren und Drucken von Daten mit Enterprise Manager.....	144
11 Fehlersuche.....	146
12 Glossar.....	153
13 Technischer Support.....	156
14 Rechtlicher Hinweis.....	157

1 Sophos Enterprise Manager

Bei Sophos Enterprise Manager, Version 4.7, handelt es sich um eine eigenständige, automatisierte Konsole, mit der Sophos Sicherheitssoftware unter Windows, Mac und Linux verwaltet und upgedatet wird. Enterprise Manager bietet folgende Funktionen:

- Schutz des Netzwerks vor Viren, Trojanern, Würmern, Spyware, schädlichen Websites, unbekanntem Threats, Adware und sonstigen potenziell unerwünschten Anwendungen.
- Verwalten des Client Firewall-Schutzes auf Endpoints.
- Verhindern, dass Benutzer nicht zugelassene externe Speichermedien und Wireless-Geräte auf Endpoints einsetzen.
- Verhindern, dass Benutzer Sophos Sicherheitssoftware umkonfigurieren, deaktivieren oder deinstallieren.

Der Sophos Support-Artikel 113711

(<http://www.sophos.de/support/knowledgebase/article/113711.html>) bietet eine Übersicht über die im Lizenzumfang von Enterprise Manager und anderer Sicherheitssoftware von Sophos enthaltenen Funktionen.

2 Übersicht über die Oberfläche von Enterprise Manager

2.1 Komponenten der Benutzeroberfläche

Die Benutzeroberfläche von Enterprise Manager setzt sich aus folgenden Bereichen zusammen:

Symbolleiste

Die Symbolleiste umfasst Verknüpfungen zu den häufigsten Befehlen zur Verwendung und Konfiguration von Sophos Sicherheitssoftware.

Mehr dazu erfahren Sie unter [Schaltflächen der Symbolleiste](#) (Seite 5).

Dashboard

Das **Dashboard** zeigt den Sicherheitsstatus des Netzwerks auf einen Blick an.

Weitere Informationen finden Sie unter [Dashboard-Bereiche](#) (Seite 6).

Computerliste

Die Computerliste befindet sich oben rechts. Sie bietet zwei Ansichten:

- In der **Ansicht „Endpoints“** werden die Endpoints der Gruppe angezeigt, die im Feld **Gruppen** unten links ausgewählt ist. Weitere Informationen finden Sie unter [Navigation in der Ansicht „Endpoints“](#) (Seite 9).
- Auf der Registerkarte **Update Manager** wird der Computer angezeigt, auf dem Sophos Update Manager installiert ist. Weitere Informationen finden Sie unter [Navigation in der Ansicht „Update Manager“](#) (Seite 11).

Der Screenshot unten zeigt die Computerliste in der Ansicht **Endpoints**.

The screenshot displays the Sophos Enterprise Manager interface. At the top, there's a navigation bar with options like 'Datei', 'Bearbeiten', 'Ansicht', 'Maßnahmen', 'Gruppen', 'Richtlinien', 'Abonnements', 'Extras', and 'Hilfe'. Below this is a 'Dashboard' section with several summary cards: 'Computer' (302 total, 302 managed), 'Computer mit Alerts' (100 Virus/Spyware, 80 Verdächtige(s) Verhalten/Dateien, 50 Adware und PUA), 'Richtlinien' (9% non-compliant), 'Updates' (last update: Montag, 4. Juli 2011 09:06), 'Computer über Ereignis-Grenzwert' (1 Device Control, 1 Firewall), and 'Fehler' (18% computers with errors). The main area shows a table of computer details with columns for 'Computername', 'Richtlinienkonformität', 'Auf dem neuesten Stand', 'Alerts und Fehler', 'On-Access', 'Firewall aktiviert', and 'Status der...'. The table lists various computers and their compliance status, such as 'AIBDLVRLCOXHQJT' (compliant) and 'AVOAF' (non-compliant due to Adware/PUA).

2.2 Schaltflächen der Symbolleiste

Die folgende Tabelle bietet eine Übersicht über die Schaltflächen der Symbolleiste. Manche Schaltflächen sind nur unter bestimmten Umständen verfügbar. Die Schaltfläche **Schützen** zur Installation von Virenschutz- und Firewallsoftware ist etwa nur dann verfügbar, wenn eine Computergruppe im Feld **Gruppen** in der Ansicht **Endpoints** ausgewählt wurde.

Schaltflächen der Symbolleiste	Beschreibung
Computer suchen	Suche nach Computern im Netzwerk und Hinzufügen der Computer zur Konsole. Nähere Informationen entnehmen Sie bitte dem Abschnitt Auffinden von Computern (Seite 28) und anderen Themen im Bereich „ <i>Einrichtung von Enterprise Manager > Computersuche im Netzwerk</i> “.
Gruppen erstellen	Erstellen einer neuen Gruppe für Computer. Weitere Informationen finden Sie unter Erstellen einer Gruppe (Seite 20).
Richtlinie öffnen/ändern	Öffnen der im Feld Richtlinie ausgewählten Richtlinie zum Ändern. Weitere Informationen finden Sie unter Ändern einer Richtlinie (Seite 26).

Schaltflächen der Symbolleiste	Beschreibung
Schützen	Installieren der Virenschutz- und Firewallsoftware auf den in der Computerliste ausgewählten Computern. Mehr dazu erfahren Sie unter Schützen von Computern (Seite 34).
Endpoints	Wechsel in die Ansicht Endpoints in der Computerliste. Die Ansicht Endpoints zeigt die Computer der im Feld Gruppe ausgewählten Gruppe an. Weitere Informationen finden Sie unter Navigation in der Ansicht „Endpoints“ (Seite 9).
Update Manager	Wechsel in die Ansicht Update Manager in der Computerliste. In der Ansicht Update Manager wird der Computer angezeigt, auf dem Sophos Update Manager installiert ist. Weitere Informationen finden Sie unter Navigation in der Ansicht „Update Manager“ (Seite 11).
Dashboard	Anzeigen/Ausblenden des Dashboards . Das Dashboard zeigt den Sicherheitsstatus des Netzwerks auf einen Blick an. Weitere Informationen finden Sie unter Dashboard-Bereiche (Seite 6).
Reports	Starten des Report-Managers zur Report-Erstellung zu Meldungen und Ereignissen im Netzwerk. Nähere Informationen finden Sie im Abschnitt Reports (Seite 132) und anderen Themen im Bereich „Erstellen von Reports“.

2.3 Dashboard-Bereiche






Das **Dashboard** umfasst folgende Bereiche:

Dashboard-Bereich	Beschreibung
Computer	<p>Anzeige der Gesamtanzahl der Computer im Netzwerk sowie der Anzahl verbundener, verwalteter und nicht verwalteter Computer.</p> <p>Klicken Sie zum Anzeigen einer Liste verwalteter, nicht verwalteter, verbundener oder aller Computer auf einen der Links im Bereich Computer.</p>
Updates	Anzeige des Status des Update Managers.
Computer mit Alerts	<p>Anzeige der Anzahl und des prozentualen Anteils verwalteter Computer mit Alerts über Folgendes:</p> <ul style="list-style-type: none"> ■ Bekannte und unbekannte Viren und Spyware ■ Verdächtiges Verhalten und verdächtige Dateien ■ Adware und andere potenziell unerwünschte Anwendungen <p>Klicken Sie zum Aufrufen einer Liste verwalteter Computer mit ausstehenden Alerts auf den Bereichstitel Computer mit Alerts.</p>
Computer über Ereignis-Grenzwert	<p>Anzeige der Anzahl der Computer, auf denen die Summe der Ereignisse in den vergangenen 7 Tagen den angegebenen Höchstwert überschritten hat.</p> <p>Klicken Sie auf den jeweiligen Link im Abschnitt Computer über Ereignis-Grenzwert, um eine Liste der Computer mit Device Control-, oder Firewall-Ereignissen aufzurufen.</p>
Richtlinien	<p>Anzeige der Anzahl und des prozentualen Anteils verwalteter Computer mit Verstößen gegen Gruppenrichtlinien oder Richtlinienabgleichsfehlern. Dazu gehören auch Computer, die noch nicht auf die geänderte Richtlinie reagiert haben, die ihnen von der Konsole gesendet wurde.</p> <p>Klicken Sie zur Anzeige einer Liste verwalteter Computer, die von der Richtlinie abweichen, auf Richtlinien.</p>
Schutz	<p>Anzeige der Anzahl und des prozentualen Anteils verwalteter und verbundener Computer, auf denen Sophos Endpoint Security and Control oder Sophos Anti-Virus nicht aktuell sind oder die unbekannte Erkennungsdaten verwenden.</p> <p>Klicken Sie zur Anzeige einer Liste verwalteter Computer, die sich nicht auf dem neuesten Stand befinden, auf Schutz.</p>
Fehler	<p>Anzeige der Anzahl und des prozentualen Anteils verwalteter Computer mit ausstehenden Scans, Updates oder Firewall-Fehlern.</p> <p>Klicken Sie zur Anzeige einer Liste verwalteter Computer mit ausstehenden Sophos Produktfehlern auf Fehler.</p>

2.4 Sicherheitsstatussymbole

Die folgende Tabelle bietet eine Übersicht über die Sicherheitsstatussymbole im **Dashboard** sowie der Statusleiste von Enterprise Manager.

Sicherheitsstatussymbol	Beschreibung
	Normal Die Anzahl betroffener Computer liegt unter der Warnstufe.
	Hinweis Der Warnschwellenwert wurde überschritten.
	Kritisch Der kritische Schwellenwert wurde überschritten.

Systemintegritätssymbole im Dashboard

Systemintegritätssymbole im **Dashboard** befinden sich jeweils in der rechten oberen Ecke eines Dashboard-Felds. Die Symbole zeigen den Status des jeweiligen Sicherheitsbereichs des Felds an.

Eine Statussymbol zur Systemintegrität im **Dashboard** zeigt den Status des Bereichs mit dem schwerwiegendsten Status an, d.h.:

- Eine Statussymbol des Bereichs ändert sich von „**Normal**“ in „**Warnung**“, wenn ein Warnschwellenwert für mindestens ein Symbol 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.

Symbol der Netzwerkintegrität

Das Symbol der Netzwerkintegrität wird auf der rechten Seite der Statusleiste von Enterprise Manager angezeigt. Das Symbol gibt Aufschluss über den allgemeinen Sicherheitsstatus des Netzwerks.

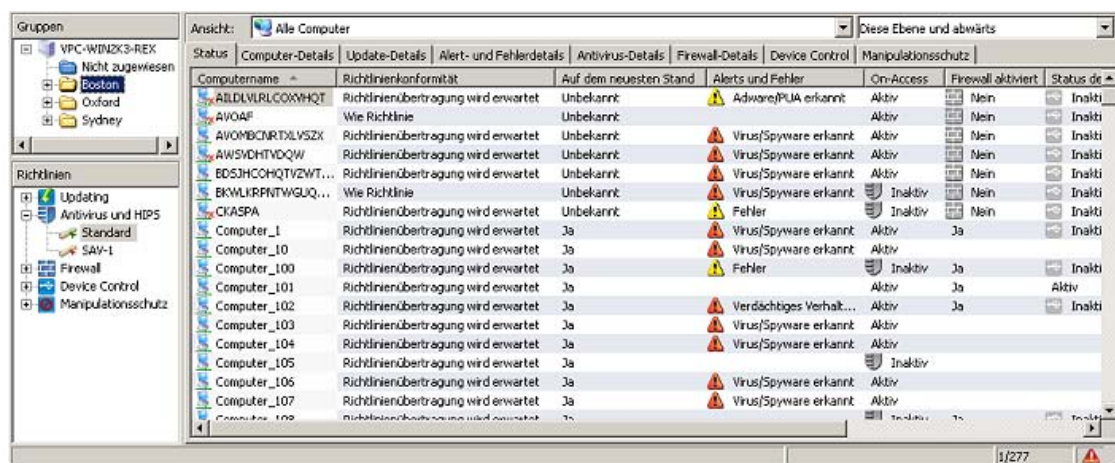
Das Statussymbol zur Netzwerkintegrität zeigt den Status des **Dashboard**-Bereichs mit dem schwerwiegendsten Status an, d.h.:

- Das Statussymbol zur Netzwerkintegrität ändert sich von „**Normal**“ in „**Warnung**“, wenn ein Warnschwellenwert für mindestens eine Anzeige im Dashboard überschritten wird.
- Das Statussymbol zur Netzwerkintegrität ändert sich von „**Warnung**“ in „**Kritisch**“, wenn ein kritischer Schwellenwert für mindestens eine Anzeige im **Dashboard** überschritten wird.

Bei der Erstinstallation von Enterprise Manager übernimmt das **Dashboard** die Standardwarnstufen und kritischen Stufen. Anweisungen zum Festlegen Ihrer eigenen Warnstufen und kritischen Stufen finden Sie im Feld [Konfigurieren des Dashboards](#) (Seite 36).

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 126).

2.5 Navigation in der Ansicht „Endpoints“



Computerliste


In der **Ansicht „Endpoints“** werden in der Computerliste die Endpoints der Gruppe angezeigt, die im Feld **Gruppen** ausgewählt ist.

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.


Eine Erklärung der in der Computerliste angezeigten Symbole wird unter [Computerlistensymbole](#) (Seite 10) aufgeführt.

Sie können die Informationen der Computerliste in der Ansicht „Endpoints“ kopieren oder ausdrucken. Mehr dazu erfahren Sie unter [Kopieren von Daten aus der Computerliste](#) (Seite 144) und anderen Bereichen im Abschnitt „*Kopieren und Drucken von Daten mit Enterprise Manager*“.

Der Fensterbereich „Gruppen“

Im Fensterbereich **Gruppen** können Sie Gruppen erstellen  und Netzwerkcomputer in die Gruppen stellen. Sie können selbst Gruppen erstellen oder Active Directory-Container mit oder ohne Computer importieren und als Enterprise Manager-Computergruppen einsetzen.

Nähere Informationen finden Sie im Abschnitt [Wofür gibt es Gruppen?](#) (Seite 20) und anderen Bereichen im Abschnitt „*Einrichtung von Enterprise Manager*“ > „*Erstellen und Verwenden von Gruppen*“.

In der Gruppe **Nicht zugewiesen**  befinden sich Computer, die noch keiner von Ihnen erstellten Gruppe zugeordnet wurden.



Fensterbereich „Richtlinien“

Im Fensterbereich **Richtlinien** erstellen und konfigurieren Sie die Richtlinien, die auf Computergruppen übertragen werden. Weitere Informationen finden Sie unter:

- [Informationen zu Richtlinien](#) (Seite 23) und anderen Bereichen im Abschnitt „*Einrichtung von Enterprise Manager*“ > „*Erstellen und Verwenden von Gruppen*“
- Abschnitt „*Konfigurieren von Richtlinien*“

2.6 Computerlistensymbole


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.

Symbol	Erklärung
	Ein graues Firewall-Symbol bedeutet, dass die Firewall deaktiviert ist.
	Ein Uhrensymbol bedeutet, dass die Software nicht aktuell ist.

Computerstatus

Symbol	Erklärung
	Ein blaues Computer-Symbol bedeutet, dass der Computer von Enterprise Manager 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 Manager verwaltet wird.
	Ein Computersymbol, neben dem sich ein rotes Kreuz befindet, weist darauf hin, dass ein Computer, der von Enterprise Manager verwaltet wird, nicht mit dem Netzwerk verbunden ist. (Nicht verwaltete Computer, die nicht mit dem Netzwerk verbunden sind, werden nicht angezeigt.)

2.7 Navigation in der Ansicht „Update Manager“



Computername	Alerts	Fehler	Letztes Update	Download-Status	Konfiguration	Version
VPC-WINZK3-REX		Update der Threat-Erkennung...	04.07.2011 09:06:31	Letzte Prüfung: 06.07.2011 ...	Treffer	1.2.1.160

Computerliste

In der Ansicht **Update Manager** können Sie automatische Updates für Sophos Sicherheitssoftware von der Sophos Website einrichten und den Status sowie weitere Informationen zum Update Manager aufrufen.

In der Computerliste wird der Computer angezeigt, auf dem Sophos Update Manager installiert ist.

Software-Abonnements

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.

3 Vorbereitung

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

Praxistipps zum Einsatz und zur Verwaltung von Sophos Sicherheitssoftware finden Sie in der Sophos Enterprise Manager *Richtlinienanleitung*. Begleitmaterial zu Sophos Software finden Sie hier: <http://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 56).

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 Manager Computer-Gruppen einsetzen.

Anweisungen zum Importieren von Active Directory-Containern finden Sie unter *Importieren von Containern und Computern aus Active Directory* (Seite 28). Es empfiehlt sich, Active Directory-Container zunächst ohne Computer zu importieren, den Gruppen dann Gruppenrichtlinien zuzuweisen und Computer in die Gruppen aufzunehmen.

Nähere Informationen zur manuellen Erstellung von Gruppen finden Sie unter *Wofür gibt es Gruppen?* (Seite 20) sowie an anderen Stellen im Unterabschnitt „Erstellen und Einsatz von Gruppen“ des Kapitels „Einrichten von Enterprise Manager“.

2. Erstellen/Konfigurieren Sie Richtlinien.

Enterprise Manager bietet diverse Standardrichtlinien, die für den Netzwerkschutz unerlässlich sind. Die Standard-**Update-** und **Antivirus- und HIPS-**Richtlinie können Sie ohne Vornahme weiterer Einstellungen übernehmen. Führen Sie zum Konfigurieren der Firewall mit den **Firewall-Richtlinienassistenten** aus. Mehr dazu erfahren Sie unter *Einrichten einer Firewall-Richtlinie* (Seite 81).

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 nicht, ziehen Sie *Auffinden von Computern* (Seite 28) und andere Stellen im Unterabschnitt „Computersuche im Netzwerk“ des Kapitels „Einrichten von Enterprise Manager“.

4. Schützen der 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. Nähere Informationen finden Sie unter *Schützen von Computern* (Seite 34) und anderen Bereichen des Abschnitts „Schützen von Computern“.

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 das Wort „Aktiv“ zu sehen sein, was darauf hinweist, dass der Computer durch On-Access-Scans geschützt ist und nun durch Enterprise Manager gesteuert wird. Weitere Informationen finden Sie unter [So überprüfen Sie, ob Ihr Netzwerk geschützt ist](#) (Seite 36).

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 [Sofortiges Bereinigen von Computern](#) (Seite 44).

Weitere Schutz- und Verwaltungsoptionen

Standardmäßig erkennt Sophos Endpoint Security and Control Viren, Trojaner, Würmer und Spyware und analysiert 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. Weitere Informationen finden Sie in den folgenden Abschnitten:

- [Scannen auf verdächtige Dateien](#) (Seite 66)
- [Scannen auf Adware und PUA](#) (Seite 69)
- [Device Control](#) (Seite 112)
- [Allgemeine Informationen](#) (Seite 119)

Sie können rollenbasierten Zugriff auf Enterprise Manager einrichten, indem Sie Windows-Benutzer und -Gruppen auf die vier vorkonfigurierten Rollen aufteilen – „Systemadministrator“, Administrator“, „Helpdesk“ und „Gast“. Die Rolle „Systemadministrator“, zu der auch die Windows-Gruppe „Sophos Full Administrators“ zählt, besitzt uneingeschränkte Zugriffsrechte und muss nicht eigens eingerichtet werden. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

4 Einrichtung von Enterprise Manager

4.1 Verwalten von Rollen

4.1.1 Informationen zu Rollen

Wichtig: Wenn Sie bereits mit rollenbasierter Verwaltung arbeiten, müssen Sie zum Einrichten von Rollen 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 15) und [Aufgabenbereich der Berechtigungen](#) (Seite 16).

Sie können rollenbasierten Zugriff auf die Konsole einrichten, indem Sie Windows-Benutzern und -Gruppen vordefinierte Konsolenrollen zuweisen. 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 Manager muss ein Benutzer der Gruppe „Sophos Console Administrators“ angehören und mindestens einer Enterprise Manager-Rolle zugewiesen worden sein. Mitglieder der Gruppe „Sophos Full Administrators“ besitzen uneingeschränkten Zugriff auf Enterprise Manager.

Hinweis: Nähere Informationen zum Gewähren des Zugriffs auf eine Remote- oder weitere Instanz von Enterprise Manager finden Sie unter [Wie kann ein anderer Anwender Enterprise Manager nutzen?](#) (Seite 19).

Sie können vorkonfigurierte Rollen bearbeiten und nutzen, jedoch keine eigenen Rollen erstellen.

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, kann er dennoch die entsprechenden Konfigurationseinstellungen aufrufen. Benutzer, denen keine Rollen zugewiesen wurden, können Enterprise Manager nicht öffnen.

4.1.2 Vordefinierte Rollen

Enterprise Manager bietet vier vorkonfigurierte Rollen. Sie können diese Rollen zwar bearbeiten, jedoch nicht umbenennen oder löschen.

Rolle	Beschreibung
Systemadministrator	Eine vorkonfigurierte Rolle für die Verwaltung von Sophos Sicherheitssoftware im Netzwerk und Rollen in Enterprise Manager.

Rolle	Beschreibung
Administrator	Eine vorkonfigurierte Berechtigungsklasse für die Verwaltung von Sophos Sicherheitssoftware im Netzwerk, jedoch nicht zur Verwaltung von Berechtigungsklassen in Enterprise Manager.
Helpdesk	Eine vorkonfigurierte Berechtigungsklasse, die nur über Korrekturrechte verfügt, z.B. zum Bereinigen oder Aktualisieren von Computern.
Gast	Eine vorkonfigurierte Berechtigungsklasse mit Lesezugriff auf Enterprise Manager.

4.1.3 Ändern einer Rolle

Bei rollenbasierter Verwaltung müssen Sie hierzu über die Berechtigung **Rollenbasierte Verwaltung** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

1. Wählen Sie aus dem Menü **Extras** die Option **Rollen verwalten**.
2. Wählen Sie im Dialogfeld **Rollen verwalten** auf der Registerkarte **Rollen verwalten** die gewünschte Rolle aus und klicken Sie auf **Ändern**.

Das Dialogfeld **Rolle ändern** wird angezeigt.

3. Fügen Sie im Fenster **Benutzer und Gruppen** Windows-Benutzer und -Gruppen zu der Rolle hinzu oder löschen Sie vorhandene Benutzer oder Gruppen.

4.1.4 Anzeigen der Rollen von Benutzern oder Gruppen

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

1. Wählen Sie aus dem Menü **Extras** die Option **Rollen verwalten**.
2. Rufen Sie im Dialogfeld **Rollen 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 angezeigt werden sollen und klicken Sie auf **OK**.

4.1.5 Aufgabenbereich der Berechtigungen

Berechtigung	Tasks
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

Berechtigung	Tasks
	Importieren von Computern aus einer Datei
	Löschen eines Computers
	Schützen eines Computers
	Verschieben eines Computers
	Erstellen einer Gruppe
	Umbenennen einer Gruppe
	Verschieben einer Gruppe
	Löschen einer Gruppe
	Übertragen einer Richtlinie auf eine Gruppe
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 – 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

Berechtigung	Tasks
	Wiederherstellen der Standardeinstellungen der Firewall
	Löschen einer Firewall-Richtlinie
Richtlinieneinstellung – Manipulationsschutz	Erstellen einer Manipulationsschutz-Richtlinie
	Duplizieren einer Manipulationsschutz-Richtlinie
	Umbenennen einer Manipulationsschutz-Richtlinie
	Bearbeiten einer Manipulationsschutz-Richtlinie
	Wiederherstellen der Standardeinstellungen des Manipulationsschutzes
	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 des Update Managers
Korrektur – Bereinigung	Bereinigung erkannter Objekte
	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

Berechtigung	Tasks
Rollenbasierte Verwaltung	Hinzufügen von Benutzern/Gruppen zur Rolle
	Entfernen eines Benutzers/einer Gruppe von einer Funktion
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

4.1.6 Wie kann ein anderer Anwender Enterprise Manager nutzen?

Mitglieder der Gruppe „Sophos Full Administrators“ besitzen uneingeschränkten Zugriff auf Enterprise Manager.

Sie können anderen Benutzern Zugriff auf Enterprise Manager gewähren. Benutzer müssen zum Öffnen von Enterprise Manager folgende Voraussetzungen erfüllen:

- Mitglied der Gruppe „Sophos Console Administrators“ sein.
- Mindestens eine Rolle in Enterprise Manager wahrnehmen.

Fügen Sie Benutzer mit Windows-Tools zu einer „Sophos Console Administrators“-Gruppe hinzu.

Klicken Sie zum Zuweisen eines Benutzers zu Rollen in Enterprise Manager im Menü **Extras** auf **Rollen verwalten**. Nähere Informationen zu Rollen finden Sie im Abschnitt [Informationen zu Rollen](#) (Seite 15).

Benutzer müssen zum Zugriff auf eine Remote- oder eine zusätzliche Instanz von Enterprise Manager folgende Voraussetzungen erfüllen:

- Mitglied der Gruppe „Sophos Console Administrators“ auf dem Server sein, auf dem der Enterprise Manager--Management-Server installiert ist.
- Mitglied der Gruppe „Distributed COM-Benutzer“ auf dem Server sein, auf dem der Enterprise Manager-Management-Server installiert ist. (Die Gruppe „Distributed COM-Benutzer“ befindet sich im vordefinierten Container des Active Directory-Benutzer und -Computer-Tools.)
- Mindestens eine Rolle in Enterprise Manager wahrnehmen.

4.2 Erstellen und Einsatz von Gruppen

4.2.1 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:

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

Tipp: Sie können Gruppen innerhalb von Gruppen erstellen und bestimmte Richtlinien auf jede Gruppe und Untergruppe übertragen.

4.2.2 Was ist eine Gruppe?

Eine Gruppe  ist ein Ordner, der mehrere Computer enthält.

Sie können selbst Gruppen erstellen oder Active Directory-Container mit oder ohne Computer importieren und als Enterprise Manager-Computergruppen einsetzen.

Jede Gruppe hat eigene Einstellungen für Updates, Viren- und HIPS-Schutz, Firewall-Schutz usw. Alle Computer einer Gruppe sollten normalerweise diese Einstellungen („Richtlinie“) verwenden.

Eine Gruppe kann Untergruppen enthalten.

4.2.3 Wozu dient die Gruppe „Nicht zugewiesen“?

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

Sie können nicht:

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

4.2.4 Erstellen einer Gruppe

Bei rollenbasierter Verwaltung ist hierzu die Berechtigung **Computersuche, -schutz und -gruppen** erforderlich. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

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-, Antivirus- und HIPS-, und Firewall-, Device Control- und Manipulationsschutz-Richtlinien werden automatisch auf die neue Gruppe übertragen. Sie können diese Richtlinien ändern oder andere Richtlinien anwenden. Nähere Informationen [Ändern einer Richtlinie](#) (Seite 26) und [Übertragen einer Richtlinie auf eine Gruppe](#) (Seite 26).

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.

4.2.5 Zuweisen von Computern zu einer Gruppe

Bei rollenbasierter Verwaltung ist hierzu die Berechtigung **Computersuche, -schutz und -gruppen** erforderlich. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

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.

4.2.6 Löschen von Computern aus einer Gruppe

Bei rollenbasierter Verwaltung ist hierzu die Berechtigung **Computersuche, -schutz und -gruppen** erforderlich. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

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.

4.2.7 Verschieben einer Gruppe

Bei rollenbasierter Verwaltung ist hierzu die Berechtigung **Computersuche, -schutz und -gruppen** erforderlich. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

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**.

4.2.8 Löschen einer Gruppe

Bei rollenbasierter Verwaltung ist hierzu die Berechtigung **Computersuche, -schutz und -gruppen** erforderlich. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

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.

4.2.9 Umbenennen einer Gruppe

Bei rollenbasierter Verwaltung ist hierzu die Berechtigung **Computersuche, -schutz und -gruppen** erforderlich. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

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

4.2.10 Übertragen einer Richtlinie auf eine Gruppe

Bei rollenbasierter Verwaltung ist hierzu die Berechtigung **Computersuche, -schutz und -gruppen** erforderlich. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

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.

4.2.11 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.

4.3 Erstellen und Einsatz von Richtlinien

4.3.1 Informationen zu Richtlinien

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

Bei der Installation von Enterprise Manager werden Standardrichtlinien erstellt, die für einen Basisschutz sorgen. Diese Richtlinien werden auf neu erstellte Gruppen übertragen. Sie können Standardrichtlinien bearbeiten.

Sie können bis zu vier Richtlinien von jedem Typ erstellen. Wenn Sie die Höchstanzahl erreicht haben, sind die Optionen **Richtlinie erstellen** und **Richtlinie kopieren** deaktiviert.

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

Enterprise Manager umfasst die vier folgenden Richtlinienarten:

- Die **Update**-Richtlinie gibt an, wie Computer mit neuer Sicherheitssoftware upgedatet werden.
- 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.
- Die **Firewall**-Richtlinie gibt an, wie die Firewall Computer schützt.
- In der **Device Control**-Richtlinie werden die Speichermedien und Netzwerkgeräte festgelegt, die nicht auf Arbeitsplatzrechnern verwendet werden dürfen.
- Die **Manipulationsschutz**-Richtlinie umfasst das Kennwort, über das autorisierte Endpoint-Benutzer Sophos Sicherheitssoftware konfigurieren, deaktivieren oder deinstallieren können.

4.3.2 Standardrichtlinien

Bei der Installation von Enterprise Manager werden Standardrichtlinien erstellt.

Update-Richtlinie

Die Standard-Update-Richtlinie bietet Folgendes:

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

Antivirus- und HIPS-Richtlinie

Die Standard-Antiviren- 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.

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 dazu erfahren Sie unter [Einrichten einer Firewall-Richtlinie](#) (Seite 81).

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

Device Control-Richtlinie

Device Control ist standardmäßig deaktiviert und alle Geräte sind zugelassen.

Manipulationsschutz-Richtlinie

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

4.3.3 Muss ich meine eigenen Richtlinien erstellen?

Bei der Installation von Enterprise Manager werden Standardrichtlinien erstellt. Diese Richtlinien werden auf neu erstellte Gruppen übertragen.

Die Standardrichtlinien bieten Ihnen grundlegenden Schutz. Wenn Sie jedoch Funktionen wie Device 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 [Informationen zu Rollen](#) (Seite 15).

Update-Richtlinie

In der Standard-Update-Richtlinie ist festgelegt, dass alle zehn Minuten auf Updates des empfohlenen Abonnements von der Standard-UNC-Freigabe zur Softwareverteilung geprüft werden soll. Wenn Sie Abonnements, Update-Standorte oder sonstige Einstellungen ändern möchten, konfigurieren Sie Update-Richtlinien anhand der Anweisungen im Abschnitt [Update-Richtlinie](#) (Seite 57).

Antivirus und HIPS

Die Antivirus- und HIPS-Standardrichtlinie schützt Computer vor Viren und sonstiger Malware. Sie können aber auch neue Richtlinien erstellen oder die Standardrichtlinie ändern, um die Erkennung anderer unerwünschte/verdächtiger Anwendungen oder Verhaltensmuster zu ermöglichen. Mehr dazu erfahren Sie unter [Die Antivirus- und HIPS-Richtlinie](#) (Seite 64).

Firewall-Richtlinie

Konfigurieren Sie Firewall-Richtlinien, um vertrauenswürdigen Anwendungen Netzwerkzugang zu gewähren. Anweisungen hierzu finden Sie unter [Einrichten einer Firewall-Richtlinie](#) (Seite 81).

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 112).

Manipulationsschutz

Der Manipulationsschutz ist standardmäßig deaktiviert. Konfigurieren Sie zum Aktivieren des Manipulationsschutzes Manipulationsschutz-Richtlinien. Anweisungen hierzu finden Sie unter [Allgemeine Informationen](#) (Seite 119).

4.3.4 Erstellen einer Richtlinie

Bei rollenbasierter Verwaltung müssen Sie hierzu über die Berechtigung **Richtlinieneinstellung** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

Sie können bis zu vier Richtlinien von jedem Typ erstellen. Wenn Sie die Höchstanzahl erreicht haben, sind die Optionen **Richtlinie erstellen** und **Richtlinie kopieren** deaktiviert.

So können Sie eine Richtlinie erstellen:

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**.

Es wird eine „Neue Richtlinie“ zur Liste hinzugefügt und ihr Name markiert.

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.

Die erstellte Richtlinie kann nun auf Gruppen übertragen werden.

4.3.5 Übertragen einer Richtlinie auf eine Gruppe

Bei rollenbasierter Verwaltung ist hierzu die Berechtigung **Computersuche, -schutz und -gruppen** erforderlich. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

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.

4.3.6 Ändern einer Richtlinie

Bei rollenbasierter Verwaltung müssen Sie hierzu über die Berechtigung **Richtlinieneinstellung** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

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.

4.3.7 Umbenennen einer Richtlinie

Bei rollenbasierter Verwaltung müssen Sie hierzu über die Berechtigung **Richtlinieneinstellung** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

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

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**.

4.3.8 Löschen einer Richtlinie

Bei rollenbasierter Verwaltung müssen Sie hierzu über die Berechtigung **Richtlinieneinstellung** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

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 zurückgesetzt.

4.3.9 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.

4.3.10 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 27).

4.3.11 Durchsetzen von Gruppenrichtlinien

Bei rollenbasierter Verwaltung müssen Sie hierzu über die Berechtigung **Korrektur – Updates und Scans** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

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**.

4.4 Computersuche im Netzwerk

4.4.1 Auffinden von Computern

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

- [Importieren von Containern und Computern aus Active Directory](#) (Seite 28)
- [Suchen nach Computern mit Active Directory](#) (Seite 29)
- [Computersuche im Netzwerk](#) (Seite 29)
- [Suchen nach Computern in einem IP-Bereich](#) (Seite 30)
- [Importieren von Computern aus einer Datei](#) (Seite 30)

Bei rollenbasierter Verwaltung ist die Berechtigung **Computersuche, -schutz und -gruppen** erforderlich, um Computer zur Konsole hinzuzufügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

4.4.2 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 [Informationen zu Rollen](#) (Seite 15).

Beim Importieren von Gruppen aus Active Directory wird die Active Directory-Containerstruktur abgerufen und in Enterprise Manager 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 sowohl „normale“ Gruppen haben, die Sie selbst erstellen und verwalten, als auch Gruppen, die von Active Directory importiert wurden.

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. Mehr dazu erfahren Sie unter [Informationen zu Richtlinien](#) (Seite 23).

4.4.3 Suchen nach Computern mit Active Directory

Bei rollenbasierter Verwaltung ist hierzu die Berechtigung **Computersuche, -schutz und -gruppen** erforderlich. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

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.

4.4.4 Computersuche im Netzwerk

Bei rollenbasierter Verwaltung ist hierzu die Berechtigung **Computersuche, -schutz und -gruppen** erforderlich. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

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 zur **Computersuche**.
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.

4.4.5 Suchen nach Computern in einem IP-Bereich

Bei rollenbasierter Verwaltung ist hierzu die Berechtigung **Computersuche, -schutz und -gruppen** erforderlich. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

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.

4.4.6 Importieren von Computern aus einer Datei

Bei rollenbasierter Verwaltung ist hierzu die Berechtigung **Computersuche, -schutz und -gruppen** erforderlich. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

Damit Enterprise Manager 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 | Windows7 | ComputerName1
Domain1 | WindowsServer2008R2 | 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: Windows2000, Windows2000Server, WindowsXP, Windows2003, WindowsVista, Windows7, WindowsServer2008, WindowsServer2008R2, MACOSX und Linux.

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.

5 Schützen von Computern

5.1 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 7/Vista:

- a) Öffnen Sie in Windows 7 in der Systemsteuerung das Netzwerk- und Freigabe-Center. Stellen Sie sicher, dass Sie für den Standort des **Firmennetzwerks** die folgenden Einstellungen vornehmen.

Netzwerkerkennung: Ein

Datei- und Druckerfreigabe: Ein

Dateifreigabeverbindungen: Aktivieren Sie die Dateifreigabe für Geräte mit 40- oder 56-bit-Verschlüsselung

Kennwortgeschütztes Freigeben: Aus

- b) Öffnen Sie in Windows Vista in der Systemsteuerung das Netzwerk- und Freigabe-Center. Nehmen Sie die folgenden Einstellungen vor:

Netzwerkerkennung: Ein

Dateifreigabe: Ein

Druckerfreigabe: Ein

Kennwortgeschütztes Freigeben: Aus

- c) Der Remote-Registrierungsdienst muss gestartet werden und der Starttyp „Automatisch“ lauten. Dieser Dienst ist unter Windows 7/Vista standardmäßig nicht aktiv.

- d) Wählen Sie in Windows 7 für die Benutzerkontensteuerung die Option **Nie benachrichtigen** aus. Nach der Installation sollten Sie den **Standard** wiederherstellen.

- e) Schalten Sie in Windows Vista die Benutzerkontensteuerung ab. Nach der Installation sollten Sie sie wieder aktivieren.

- f) Deaktivieren Sie den Freigabeassistenten.

- g) Öffnen Sie die Windows-Firewall mit erweiterter Sicherheit. Öffnen Sie in der Systemsteuerung die **Verwaltung**. Stellen Sie sicher, dass **Eingehende Verbindungen** zugelassen werden.

- h) Lassen Sie unter **Eingehende Regeln** die folgenden Prozesse zu. Deaktivieren Sie nach der Installation die folgenden 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:
 - 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 und höher:
 - 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.

5.2 Entfernen von Fremdsoftware

Wenn Sie installierte Sicherheitssoftware entfernen möchten, sollten Sie zunächst wie folgt verfahren, 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: Computer, auf denen die Software anderer Hersteller entfernt wurde, müssen anschließend 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 gleichen Verzeichnis wie „data.zip“. Legen Sie „crt.cfg“ nicht wieder in „data.zip“ ab, weil die Datei sonst beim nächsten Update 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.

5.3 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 "Einfache Dateifreigabe" ausgeschaltet ist.
- Bei rollenbasierter Verwaltung ist hierzu die Berechtigung **Computersuche, -schutz und -gruppen** erforderlich. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

Die automatische Installation mit Enterprise Manager wird von Mac- und Linux-Computern nicht unterstützt. Anweisungen zum Schutz dieser Betriebssysteme finden Sie in der *Startup-Anleitung* zu Sophos Enterprise Manager. Begleitmaterial zu Sophos Software finden Sie hier: <http://www.sophos.de/support/docs/>.

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:

■ **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 148) oder führen Sie auf diesen Computern die Installation manuell durch (mehr Informationen hierzu können Sie der Startup-Anleitung zu Sophos Enterprise Manager entnehmen). Klicken Sie auf **Weiter**.
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. Nähere Informationen finden Sie unter *Update-Server-Standorte* (Seite 58) und anderen Abschnitten zum *Konfigurieren der Update-Server-Standorte*.

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.

5.4 Anzeigen der Bootstrap-Verzeichnisse

Wenn Enterprise Manager auf bestimmten Computern die Virenschutz- oder Firewall-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-Software auf Windows 2000- oder neueren Computern installieren.

Anweisungen zur manuellen Installation von Sicherheitssoftware auf unterschiedlichen Betriebssystemen finden Sie in der *Erweiterten Startup-Anleitung* zu Sophos Enterprise Manager.

5.5 Ermitteln des Netzwerkschutzes

5.5.1 So überprüfen Sie, ob Ihr Netzwerk geschützt ist

Das Dashboard bietet Ihnen einen Überblick über den Sicherheitsstatus des Netzwerks. Mehr dazu erfahren Sie unter [Dashboard-Bereiche](#) (Seite 6) und [Konfigurieren des Dashboards](#) (Seite 36).

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 37), [Überprüfen, ob sich die Computer auf dem neuesten Stand befinden](#) (Seite 38) und [Auffinden von Computern mit Problemen](#) (Seite 38).

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 27).

5.5.2 Konfigurieren des Dashboards

Bei rollenbasierter Verwaltung müssen Sie zur Konfiguration des Dashboards über die Berechtigung **Systemkonfiguration** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

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 126).

5.5.3 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**.
3. 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.

4. 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.
5. Den Status anderer Funktionen (z.B. Application Control oder Device 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 38).

Weitere Informationen zum Auffinden von Computern mit Problemen über Computerlistenfilter finden Sie unter [Auffinden von Computern mit Problemen](#) (Seite 38).

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

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

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

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 Drop-Down-Liste **Auf dieser Stufe und darunter**.
3. 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.

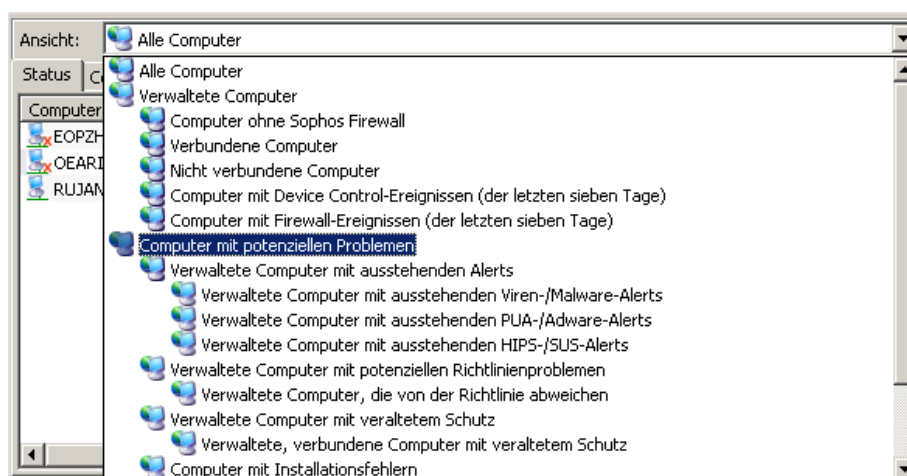
Informationen zum Updaten solcher Computer finden Sie im Abschnitt [Updaten nicht aktueller Computer](#) (Seite 62).

5.5.5 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:

1. 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.

Anweisungen zum Beheben von Schutzproblemen finden Sie im Abschnitt [Keine Durchführung von On-Access-Scans](#) (Seite 146) und anderen Themen zur *Fehlersuche*.

5.6 Benachrichtigungen, Alerts und Fehlermeldungen



5.6.1 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 36).

Alert-Symbole

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

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**.

5.6.2 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 [Informationen zu Rollen](#) (Seite 15).

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 42).
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 42).
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 43).
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 Manager 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 45).
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 70) und [Zulassen verdächtiger Objekte](#) (Seite 67).

5.6.3 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 auch die **Sicherheitsanalysen** auf der Sophos Website aufrufen (<http://www.sophos.de/security/analyses/>). 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.

5.6.4 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 [Informationen zu Rollen](#) (Seite 15).

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 42).

5.6.5 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 [Informationen zu Rollen](#) (Seite 15).

So löschen Sie Update Manager-Alerts aus der Konsole:

1. Wählen Sie in der Ansicht **Update Manager** den Update Manager. 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.

5.7 Scannen von Computern

5.7.1 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 66).
- Scannen auf Adware und potenziell unerwünschte Anwendungen. Mehr dazu erfahren Sie unter [Scannen auf Adware und PUA](#) (Seite 69).
- Scannen von Computern zu festen Zeiten. Mehr dazu erfahren Sie unter [Scannen von Computern zu bestimmten Zeiten](#) (Seite 74).

Weitere Informationen zur Konfiguration von Scans entnehmen Sie bitte dem Abschnitt [Die Antivirus- und HIPS-Richtlinie](#) (Seite 64).

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

5.7.2 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 [Informationen zu Rollen](#) (Seite 15).

Hinweis: Sofortige vollständige Systemüberprüfungen über die Konsole sind nur unter Windows 2000 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.

Hinweis: Wenn beim Scan Threat-Komponenten im Speicher erkannt werden, wird der Scan angehalten und ein Alert wird an Enterprise Manager gesendet. Wenn der Scan fortgesetzt wird, könnte sich der Threat ausbreiten. Sie müssen den Threat zunächst bereinigen, bevor Sie den Scan erneut ausführen können.

5.8 Bereinigen von Computern

5.8.1 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 [Informationen zu Rollen](#) (Seite 15).

Hinweis: Zur Bereinigung von Macintosh-, oder Linux-Systemen können Sie entweder anhand der Anweisungen im Abschnitt [Einrichten der automatischen Bereinigung](#) (Seite 45) eine automatische Bereinigung von der Konsole aus einrichten oder die Computer einzeln bereinigen, wie unter [Bearbeiten erkannter Objekte, falls die Bereinigung fehlschlägt](#) (Seite 45) 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 150).

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 45).

Hinweis: Bei der Bereinigung wird unter Umständen eine vollständige Systemüberprüfung auf den betroffenen Computern eingeleitet, um *alle* Viren zu bereinigen. Dieser Vorgang kann viel Zeit in Anspruch nehmen. Die Alerts werden nach Abschluss des Scan-Vorgangs aktualisiert.

5.8.2 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.

5.8.3 Einrichten der automatischen Bereinigung

Bei rollenbasierter Verwaltung müssen Sie hierzu über die Berechtigung **Richtlinieneinstellung – Antivirus und HIPS** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

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 44) 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 23).
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. Richten Sie die automatische Bereinigung für *On-Access-Scans* ein.
 - a) Klicken Sie im Fensterbereich **Antivirus- und HIPS-Konfiguration** auf die Schaltfläche **On-Access-Scans**.
 - b) Klicken Sie im Dialogfeld **Einstellungen für On-Access-Scans** auf die Registerkarte **Bereinigung**.
 - c) Nehmen Sie die folgenden Einstellungen vor:

Viren/Spyware

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

- **Zugriff verweigern**
- **Löschen**
- **Zugriff verweigern und in das Standardverzeichnis verschieben**
- **Zugriff verweigern und in <UNC>-Pfad verschieben**

Hinweise

- 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-Computern ignoriert.

Verdächtige Dateien

Hinweis: Diese Einstellungen gelten nur für Systeme unter Windows 2000 und aufwärts.

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

- **Zugriff verweigern**
- **Löschen**
- **Zugriff verweigern und in das Standardverzeichnis verschieben**
- **Zugriff verweigern und in <UNC>-Pfad verschieben**

4. Richten Sie die automatische Bereinigung für *geplante Scans* ein.
 - a) Markieren Sie im Dialogfeld **Antivirus- und HIPS-Richtlinie** im Fensterbereich **Geplante Scans** den Scan und klicken Sie auf **Ändern**.
 - b) Klicken Sie dann im Dialogfeld **Einstellungen zu geplanten Scans** auf **Konfigurieren**.
 - c) Klicken Sie im Dialogfeld **Scan- und Bereinigungs-Einstellungen** auf die Registerkarte **Bereinigung**.
 - d) Nehmen Sie die folgenden Einstellungen vor:

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 protokollieren**
- **Löschen**
- **In Standardspeicherort verschieben** oder **In <UNC-Pfad> verschieben**

Hinweise

- Das Verschieben einer ausführbaren Datei senkt das Risiko, dass diese Datei gestartet wird.
- Eine Infektion mit mehreren Komponenten kann nicht automatisch verschoben werden.

Adware und PUA

Hinweis: Diese Einstellung ist nur für Windows 2000 und höher relevant.

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

Verdächtige Dateien

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

- **Nur protokollieren**
- **Löschen**
- **In Standardspeicherort verschieben** oder **In <UNC-Pfad> verschieben**

Hinweise

- Diese Einstellungen gelten nur für Systeme unter Windows 2000 und aufwärts.
- Das Verschieben einer ausführbaren Datei senkt das Risiko, dass diese Datei gestartet wird.
- Eine Infektion mit mehreren Komponenten kann nicht automatisch verschoben werden.

6 Updates

6.1 Konfigurieren des Update Managers

6.1.1 Wozu dient der Update Manager?

Mit dem Update Manager können Sie automatische Updates von Sophos Sicherheitssoftware über die Sophos Website konfigurieren.

Enterprise Manager unterstützt nur einen Update Manager. Der Update Manager wird mit Enterprise Manager installiert und verwaltet.

Der Update Manager wird beim Ausführen des **Assistenten zum Download von Sicherheitssoftware** installiert. Der Assistent wird beim ersten Öffnen von Enterprise Manager nach der Installation automatisch gestartet.

Sie können die Konfiguration des Update Managers zu einem späteren Zeitpunkt ändern. Dies kann sich etwa anbieten, wenn Sie heruntergeladene Sophos Software auf weitere Freigaben im Netzwerk verteilen möchten.

6.1.2 Funktionsweise des 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 Netzwerkfreigaben ab.

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

6.1.3 Anzeigen oder Ändern der Update Manager-Konfiguration

Bei rollenbasierter Verwaltung müssen Sie zum Konfigurieren des Update Managers über die Berechtigung **Richtlinieneinstellung – Updates** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

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 in der Computerliste aus. Rechtsklicken Sie und wählen Sie aus dem Kontextmenü die Option **Konfiguration öffnen/ändern**.

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 den Update Manager](#) (Seite 49).
 - [Softwareauswahl](#) (Seite 50).
 - [Festlegen des Download-Verzeichnisses](#) (Seite 50).
 - [Erstellen/Ändern eines Update-Zeitplans](#) (Seite 52).
 - [Konfigurieren des Update Manager-Protokolls](#) (Seite 53).
 - [Konfigurieren der Selbst-Update-Funktion des Update Managers](#) (Seite 53).

Weitere Informationen zum Löschen von Update Manager-Alerts aus der Konsole finden Sie unter [Löschen von Update Manager-Alerts aus der Konsole](#) (Seite 42).

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

6.1.4 Auswahl einer Update-Quelle für den Update Manager

Bei rollenbasierter Verwaltung müssen Sie zum Konfigurieren des Update Managers über die Berechtigung **Richtlinieneinstellung – Updates** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

Es muss eine Quelle angegeben werden, von der der Update Manager Sicherheitssoftware und Updates herunterlädt, die dann im Netzwerk bereitgestellt 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 den Update Manager in der Computerliste aus. Rechtsklicken Sie und wählen Sie aus dem Kontextmenü die Option **Konfiguration öffnen/ändern**.
3. Klicken Sie im Fenster **Update Manager konfigurieren** auf der Registerkarte **Quellen** auf die Option **Hinzufügen**.
4. Wählen Sie im Dialogfeld **Quellenangaben** im Feld **Adresse Sophos** aus, um Updates direkt von Sophos zu beziehen.
5. Geben Sie in die Felder **Benutzername** und **Kennwort** die Zugangsdaten für den Download ein, die Sie von Sophos erhalten haben.

6. Wenn Sie über einen Proxyserver auf das Internet 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.

6.1.5 Softwareauswahl

Bei rollenbasierter Verwaltung müssen Sie zum Konfigurieren des Update Managers über die Berechtigung **Richtlinieneinstellung – Updates** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

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 Update Manager in der Computerliste aus. Rechtsklicken Sie und wählen Sie aus dem Kontextmenü die Option **Konfiguration öffnen/ändern**.
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 auf „Alle hinzufügen“, wenn Sie alle Abonnements in die Liste „Abonniert für“ verschieben möchten.



Nähere Informationen zu Abonnements finden Sie unter [Software-Abonnements](#) (Seite 55).

6.1.6 Festlegen des Download-Verzeichnisses

Bei rollenbasierter Verwaltung müssen Sie zum Konfigurieren des Update Managers über die Berechtigung **Richtlinieneinstellung – Updates** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

Wenn Sie angegeben haben, welche Software heruntergeladen werden soll, können Sie nun das Download-Verzeichnis im Netzwerk angeben. Standardmäßig wird Software in einer

UNC-Freigabe abgelegt: \\<Computername>\SophosUpdate. ComputerName steht dabei für den Namen des Computers, auf dem der Update Manager installiert wurde.

Sie können heruntergeladene Software in weiteren Freigaben im Netzwerk bereitstellen. 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 51) 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 Update Manager in der Computerliste aus. Rechtsklicken Sie und wählen Sie aus dem Kontextmenü die Option **Konfiguration öffnen/ändern**.
3. Wählen Sie im Dialogfeld **Update Manager konfigurieren** auf der Registerkarte **Verteilung** 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.

In der Liste mit den verfügbaren Freigaben werden sämtliche Freigaben angezeigt, auf die Enterprise Manager zugreifen kann.

Über die Schaltfläche „Hinzufügen“ (>) bzw. „Entfernen“ (<) können Sie Freigaben in die Liste der verfügbaren Freigaben 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.

6.1.7 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.

6.1.8 Erstellen/Ändern eines Update-Zeitplans

Bei rollenbasierter Verwaltung müssen Sie zum Konfigurieren des Update Managers über die Berechtigung **Richtlinieneinstellung – Updates** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

Standardmäßig sucht der Update Manager alle 10 Minuten in der Sophos Datenbank nach Updates für **Threat-Erkennungsdaten**.

Sie können das Update-Intervall ändern. Das Intervall muss mindestens 5 und höchstens 1440 Minuten (24 Stunden) betragen. Es empfiehlt sich ein Update-Intervall von 10 Minuten für Threat-Erkennungsdaten, um sicherzustellen, dass Sie umgehend vor neu erkannten Threats geschützt sind.

Standardmäßig sucht der Update Manager alle 60 Minuten in der Sophos Datenbank nach **Software-Updates**.

Sie können das Update-Intervall ändern. Das Intervall muss mindestens 10 und höchstens 1440 Minuten (24 Stunden) betragen.

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 Tage 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 den Update Manager in der Computerliste aus. Rechtsklicken Sie und wählen Sie aus dem Kontextmenü die Option **Konfiguration öffnen/ändern**.
3. Rufen Sie im Dialogfeld **Update Manager konfigurieren** die Registerkarte **Zeitplan** auf und legen Sie ein Intervall für Threat-Erkennungsdaten 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.

6.1.9 Konfigurieren des Update Manager-Protokolls

Bei rollenbasierter Verwaltung müssen Sie zum Konfigurieren des Update Managers über die Berechtigung **Richtlinieneinstellung – Updates** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

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 in der Computerliste aus. Rechtsklicken Sie und wählen Sie aus dem Kontextmenü die Option **Konfiguration öffnen/ändern**.
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.

6.1.10 Konfigurieren der Selbst-Update-Funktion des Update Managers

Bei rollenbasierter Verwaltung müssen Sie zum Konfigurieren des Update Managers über die Berechtigung **Richtlinieneinstellung – Updates** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

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 in der Computerliste aus. Rechtsklicken Sie und wählen Sie aus dem Kontextmenü die Option **Konfiguration öffnen/ändern**.
3. Wählen Sie im Dialogfeld **Update Manager konfigurieren** auf der Registerkarte **Erweitert** die gewünschte Update Manager-Version aus.

Enterprise Manager unterstützt nur die „empfohlene“ Version des Update Managers. Der Update Manager wird stets an die Version mit der entsprechenden Bezeichnung angepasst. Die Version des Update Managers ändert sich dabei.

6.1.11 Sofort-Update-Suche

Bei rollenbasierter Verwaltung müssen Sie hierzu über die Berechtigung **Korrektur – Updates und Scans** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

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 den Update Manager in der Ansicht „Update Manager“ aus, rechtsklicken Sie darauf und klicken Sie auf **Jetzt updaten**.

6.1.12 Überwachen des Update Managers

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 Computerliste in den Spalten **Alerts** und **Fehler** nach möglichen Problemen.
3. Wenn neben dem 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 **Update Manager-Details** werden der Zeitpunkt der letzten Software- und Threaterkennungsdaten-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: Im Abschnitt **Updates** des Dashboards wird kein Alert oder Fehler angezeigt, wenn der Update Manager vorübergehend keine Updates beziehen kann. Es werden lediglich dann Alerts oder Fehler angezeigt, wenn die seit dem letzten Update verstrichene Zeit über dem in [Konfigurieren des Dashboards](#) (Seite 36) festgelegten Warnschwellenwert bzw. kritischen Schwellenwert liegt.

6.1.13 Übernahme der Konfigurationseinstellungen

Bei rollenbasierter Verwaltung müssen Sie hierzu über die Berechtigung **Korrektur – Updates und Scans** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

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 in der Ansicht „Update Manager“ aus, rechtsklicken Sie darauf und klicken Sie auf **Konformität mit Konfiguration**.

6.1.14 Freigeben von Sicherheitssoftware in einem Webserver

Bisweilen empfiehlt sich, Sophos Sicherheitssoftware in einem Webserver freizugeben, damit Computer über HTTP darauf zugreifen können.

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 Manager 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 Webserver. Wenden Sie sich bei weiteren Fragen bitte an Ihren Webserver-Betreiber.

6.2 Konfigurieren von Software-Abonnements

6.2.1 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 ausgewählten Software. So wird sichergestellt, dass Ihre Software automatisch auf dem aktuellen Stand gehalten wird.

Wenn Sie bereits im Assistenten alle zu schützenden Plattformen angegeben haben, müssen Sie keine Software-Abonnements konfigurieren. Wenn Sie eine weitere Plattform schützen möchten, konfigurieren Sie anhand der Anweisungen unter [Abonnieren von Sicherheitssoftware](#) (Seite 55) ein Abonnement.

Wenn Sie den Assistenten nach der Installation von Enterprise Manager nicht ausgeführt haben, finden Sie im Abschnitt [Ausführen des Download-Assistenten für Sicherheitssoftware](#) (Seite 56) nähere Informationen.

6.2.2 Abonnieren von Sicherheitssoftware

Bei rollenbasierter Verwaltung müssen Sie zum Bearbeiten einer eines Abonnements über die Berechtigung **Richtlinieneinstellung – Updates** verfügen. Nähere Informationen zur rollenbasierten Verwaltung können Sie dem Abschnitt [Informationen zu Rollen](#) (Seite 15) 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.
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 empfohlene Version aus, z.B. *9.7 Empfohlen*.

Wichtig: Wählen Sie nur auf Anraten des technischen Support von Sophos eine feste Version (z.B. *9.7.1*) aus.

Konfigurieren Sie den Update Manager nach dem Erstellen des neuen Software-Abonnements, damit er wie unter [Anzeigen oder Ändern der Update Manager-Konfiguration](#) (Seite 48) erläutert verwaltet wird.

Sie können auch E-Mail-Benachrichtigungen für Software-Abonnements einrichten. Nähere Informationen zu Abonnement-E-Mail-Alerts können Sie dem Abschnitt [Einrichten von Softwareabonnement-Alerts](#) (Seite 122) entnehmen.

6.2.3 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 [Informationen zu Rollen](#) (Seite 15).

Wenn Sie den **Download-Assistenten für Sicherheitssoftware** nach der Installation von Enterprise Manager 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.

6.2.4 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 **Abonnement-Statistik anzeigen**.

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

6.3 Konfigurieren der Update-Richtlinie

6.3.1 Update-Richtlinie

Update-Richtlinien halten die Sicherheitssoftware auf Ihren Computer auf dem neuesten Stand. Enterprise Manager sucht nach Updates und aktualisiert Computer in festgelegten Zeitabständen bei Bedarf.

Die Standard-Update-Richtlinie ermöglicht Installation und Updates der Software, die im „empfohlenen“ Abonnement angegeben sind.

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

- [Auswahl eines Abonnements](#) (Seite 57)
- [Update-Server-Standorte](#) (Seite 58)
- [Update-Zeitpläne](#) (Seite 60)
- [Ändern der Erstinstallationsquelle](#) (Seite 61)
- [Update-Protokoll](#) (Seite 61)

Hinweis: Bei rollenbasierter Verwaltung müssen Sie zum Konfigurieren einer Update-Richtlinie über die Berechtigung **Richtlinieneinstellung – Updates** verfügen. Nähere Informationen zur rollenbasierten Verwaltung können Sie dem Abschnitt [Informationen zu Rollen](#) (Seite 15) entnehmen.

6.3.2 Auswahl eines Abonnements

Bei rollenbasierter Verwaltung müssen Sie zum Konfigurieren einer Update-Richtlinie über die Berechtigung **Richtlinieneinstellung – Updates** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

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 23).
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.

6.3.3 Konfigurieren der Update-Server-Standorte

6.3.3.1 Update-Server-Standorte

Die Standard-Update-Quelle ist eine einzelne primäre UNC-Freigabe, \\<ComputerName>\SophosUpdate. <ComputerName> ist dabei der Name des Computers mit dem Update Manager. Auf Wunsch können Sie auch eine alternative sekundäre Update-Quelle angeben und Standort-Roaming aktivieren. Wenn Endpoints keine Verbindung zur primären Quelle herstellen können, versuchen sie, Updates von der sekundären Quelle (falls vorhanden) zu beziehen. Es empfiehlt sich, stets eine sekundäre Quelle anzugeben.

Bei dem primären und sekundären Update-Server-Verzeichnis handelt es sich um eine UNC-Freigabe oder HTTP-URL von dem Update Manager im Netzwerk. Für die sekundäre Update-Quelle kann auch angegeben werden, dass Updates per HTTP über das Internet direkt von Sophos bezogen werden.

Hinweis: Je nach Konfiguration stehen dem Update Manager mitunter mehrere Verteilungsfreigaben zur Verfügung.

6.3.3.2 Laptop-Roaming

Unter Umständen roamen Mitarbeiter mit Laptops sehr viel, auch international. Bei aktiviertem Standort-Roaming (in der Update-Richtlinie für Roaming-Laptops) suchen Roaming-Laptops nach dem nächsten Update-Server und versuchen, von diesem Updates zu beziehen. Hierzu senden sie eine Anfrage an andere (feste) Endpoints im lokalen Netzwerk, mit dem sie verbunden sind, um Update-Zeit und Bandbreite einzusparen.

Roaming-Laptops beziehen Update-Server-Standorte und Zugangsdaten, indem sie eine Anfrage an feste Computer im gleichen lokalen Netzwerk beziehen. Wenn mehrere Standorte gefunden werden, sucht das Laptop nach dem nächsten und greift auf diesen zu. Wenn dies nicht möglich ist, greift das Laptop auf den in der Update-Richtlinie festgelegten primären (und anschließend den sekundären) Standort zu.

Hinweis: Wenn feste Computer Update-Standorte und Zugangsdaten an das Laptop senden, sind die Kennwörter bei der Übertragung und Speicherung verschleiert. Konten zum Lesen der Update-Server-Standorte sollten nur mit Lesezugriff ausgestattet werden. Mehr dazu erfahren Sie unter *Festlegen des Download-Verzeichnisses* (Seite 50).

Standort-Roaming ist nur in folgenden Fällen möglich:

- Roaming-Endpoints und feste Endpoints greifen auf die gleiche Enterprise Manager zu.
- Das Software-Abonnement von festen Endpoints und Roaming-Laptops ist identisch.
- Enterprise Manager ist Version 4.7 oder höher und Endpoint Security and Control ist Version 9.7 oder höher auf festen und Roaming-Endpoints.
- In Firewalls von anderen Anbietern sind Update-Standort-Anfragen und -Antworten zugelassen. Der Standortport lautet „51235“, ist jedoch konfigurierbar. Details finden Sie hier: <http://www.sophos.de/support/knowledgebase/article/110371.html>.

Sie können Standort-Roaming bei der Angabe von Update-Quellen aktivieren. Anweisungen hierzu entnehmen Sie bitte dem Abschnitt *Ändern der Zugangsdaten zum Primärserver* (Seite 59).

6.3.3.3 Ändern der Zugangsdaten zum Primärserver

Bei rollenbasierter Verwaltung müssen Sie zum Konfigurieren einer Update-Richtlinie über die Berechtigung **Richtlinieneinstellung – Updates** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

So ändern Sie die Zugangsdaten des Primärservers:

1. Doppelklicken Sie im Fensterbereich **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.

6.3.3.4 Festlegen des sekundären Update-Server-Standorts

Bei rollenbasierter Verwaltung müssen Sie zum Konfigurieren einer Update-Richtlinie über die Berechtigung **Richtlinieneinstellung – Updates** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

So legen Sie den sekundären Update-Server-Standort fest:

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 23).
2. Doppelklicken Sie im Feld **Richtlinien** auf **Updates** und doppelklicken Sie anschließend auf die Richtlinie, die Sie ändern möchten.
3. Klicken Sie im Dialogfeld **Update-Richtlinie** auf die Registerkarte **Sekundärserver** und aktivieren Sie das Kontrollkästchen **Sekundärserver festlegen**.
4. Das Feld **Adresse** bietet folgende Optionen:
 - Eingabe der HTTP-URL bzw. des UNC-Netzwerkpfads der Update-Server-Freigabe.
 - Auswahl von **Sophos**.

Wichtig: Wenn Sie eine HTTP-URL oder eine Freigabe auswählen, die nicht von einem verwalteten Update Manager verwaltet wird, kann Enterprise Manager nicht überprüfen, ob das angegebene Software-Abonnement verfügbar ist. Stellen Sie sicher, dass die Freigabe das angegebene Abonnement enthält, da Computer andernfalls keine Updates beziehen.

5. Wenn die Richtlinie Mac-Endpoints umfasst und Sie im **Adressfeld** unter **Wählen Sie ein File Sharing-Protokoll für Mac OS X** einen UNC-Pfad angegeben haben, wählen Sie ein Protokoll für den Zugriff der Macs auf die Update-Freigabe aus.

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. Bei Sophos HTTP handelt es sich um die Zugangsdaten des Abonnements.
Das Konto muss Lesezugriff (Navigationsszugriff) auf die Freigabe besitzen, die Sie oben in das Adressfeld eingegeben haben.
Hinweis: Falls der Benutzername auch eine Domäne erfordert, geben Sie ihn im Format Domäne\Benutzername ein. Nähere Informationen zum Überprüfen eines Windows-Benutzerkontos finden Sie im Sophos Support-Artikel 11637 (<http://www.sophos.de/support/knowledgebase/article/11637.html>).
7. Klicken Sie zum Verringern der Bandbreite auf **Erweitert**. Aktivieren Sie im Dialogfeld **Erweiterte Einstellungen** die Option **Bandbreite verringern** und geben Sie mit Hilfe des Schiebereglers die Bandbreite in KBit/s an.
8. Wenn Sie über einen Proxyserver auf die Update-Quelle zugreifen, klicken Sie auf **Proxyserver-Details**. Aktivieren Sie im Dialogfeld **Proxy-Details** die Option **Internetverbindung über Proxyserver herstellen** und geben Sie dann **Adresse** und **Portzahl** des Proxyservers ein. Geben Sie die **Zugangsdaten** des Proxyservers ein. Falls der Benutzername auch eine Domäne erfordert, geben Sie ihn im Format Domäne\Benutzername ein.
Hinweis: Bei einigen Internet Service Providern werden HTTP-Anfragen an einen Proxyserver gesendet.
9. Klicken Sie auf **OK**, um das Fenster **Updating-Richtlinie** zu schließen.
10. Rechtsklicken Sie im Fenster **Gruppen** auf eine Gruppe, die die soeben geänderte Update-Richtlinie nutzt und klicken Sie anschließend auf **Konformität mit > Update-Gruppenrichtlinie**.
Wiederholen Sie diesen Schritt für alle Gruppen in der Richtlinie.

6.3.4 Update-Zeitpläne

Bei rollenbasierter Verwaltung müssen Sie zum Konfigurieren einer Update-Richtlinie über die Berechtigung **Richtlinieneinstellung – Updates** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

Standardmäßig suchen Endpoints alle 5 Minuten nach Updates in den Netzwerkfreigaben.

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 23).
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 **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 Verbindungsherstellung ein Update durchzuführen.

6.3.5 Ändern der Erstinstallationsquelle

Bei rollenbasierter Verwaltung müssen Sie zum Konfigurieren einer Update-Richtlinie über die Berechtigung **Richtlinieneinstellung – Updates** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

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 23).
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.

6.3.6 Update-Protokoll

Bei rollenbasierter Verwaltung müssen Sie zum Konfigurieren einer Update-Richtlinie über die Berechtigung **Richtlinieneinstellung – Updates** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

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 23).
2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Update**. 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 Problembeseitigung benötigen.

6.4 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 [Informationen zu Rollen](#) (Seite 15).

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 Uhrensymbol 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**.

7 Konfigurieren von Richtlinien

7.1 Konfigurieren der Antivirus- und HIPS-Richtlinie

7.1.1 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 66)
- [Scannen auf Adware und PUA](#) (Seite 69)
- [Scannen von Computern zu bestimmten Zeiten](#) (Seite 74)

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 45).

Hinweis: Bei rollenbasierter Verwaltung müssen Sie zum Bearbeiten der Antivirus- und HIPS-Richtlinie über die Berechtigung **Richtlinieneinstellung – Antivirus und HIPS** verfügen. Nähere Informationen zur rollenbasierten Verwaltung können Sie dem Abschnitt [Informationen zu Rollen](#) (Seite 15) entnehmen.

Hinweis: Enterprise Manager 4.7 kann keine geplanten Scans auf Macs durchführen. Wählen Sie eine andere Scan-Variante aus. Weitere Informationen zu Scan-Optionen können Sie der [Hilfe zu Sophos Anti-Virus für Mac OS X](#) entnehmen.

7.1.2 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.

7.1.3 Erkennung verdächtigen Verhaltens und verdächtiger Dateien (HIPS)

7.1.3.1 Was ist HIPS?

Host Intrusion Prevention System (HIPS) schützt Computer vor verdächtigen Dateien, unbekanntem Viren und verdächtigem Verhalten. HIPS basiert auf zwei 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 65).

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 66).

7.1.3.2 Erkennen und Sperren verdächtigen Verhaltens

Bei rollenbasierter Verwaltung müssen Sie hierzu über die Berechtigung **Richtlinieneinstellung – Antivirus und HIPS** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

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 44) und [Zulassen verdächtiger](#)

Objekte (Seite 67). 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 dazu erfahren Sie unter *Welche Richtlinien sind einer Gruppe zugewiesen?* (Seite 23).
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**.

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**.

7.1.3.3 Scannen auf verdächtige Dateien

Bei rollenbasierter Verwaltung müssen Sie hierzu über die Berechtigung **Richtlinieneinstellung – Antivirus und HIPS** verfügen. Weitere Informationen finden Sie unter *Informationen zu Rollen* (Seite 15).

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 dazu erfahren Sie unter *Welche Richtlinien sind einer Gruppe zugewiesen?* (Seite 23).
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-Überprüfung

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**. 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 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 44) und [Zulassen verdächtiger Objekte](#) (Seite 67).

7.1.3.4 Zulassen verdächtiger Objekte

Bei rollenbasierter Verwaltung müssen Sie hierzu über die Berechtigung **Richtlinieneinstellung – Antivirus und HIPS** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

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 23).
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.

7.1.4 Sophos Live-Schutz

7.1.4.1 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.

7.1.4.2 Aktivieren/Deaktivieren von Sophos Live-Schutz

Bei rollenbasierter Verwaltung müssen Sie hierzu über die Berechtigung **Richtlinieneinstellung – Antivirus und Hips** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

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 23).
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.

7.1.5 Adware und PUA

7.1.5.1 Scannen auf Adware und PUA

Bei rollenbasierter Verwaltung müssen Sie hierzu über die Berechtigung **Richtlinieneinstellung – Antivirus und HIPS** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

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 dazu erfahren Sie unter [Welche Richtlinien sind einer Gruppe zugewiesen?](#) (Seite 23).
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 70)). Andernfalls entfernen Sie die Anwendungen (mehr dazu erfahren Sie im Abschnitt [Sofortiges Bereinigen von Computern](#) (Seite 44)).
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 dazu erfahren Sie unter [Hohe Alert-Anzahl aufgrund potenziell unerwünschter Anwendungen](#) (Seite 150).

7.1.5.2 Zulassen von Adware und PUA

Bei rollenbasierter Verwaltung müssen Sie hierzu über die Berechtigung **Richtlinieneinstellung – Antivirus und HIPS** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

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 23).
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. 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 Manager 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.
8. 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**.

7.1.6 Web-Schutz

7.1.6.1 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.

Web-Schutz:

- 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 71) entnehmen.

7.1.6.2 Aktivieren des Web-Schutzes

Bei rollenbasierter Verwaltung müssen Sie hierzu über die Berechtigung **Richtlinieneinstellung – Antivirus und HIPS** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

So aktivieren Sie den Web-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 23).
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 72).

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.

7.1.6.3 Zulassen von Websites

Bei rollenbasierter Verwaltung müssen Sie hierzu über die Berechtigung **Richtlinieneinstellung – Antivirus und HIPS** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).



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 23).
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 130) wird erläutert, wie Sie eine Liste der in letzter Zeit gesperrten Websites auf einem Endpoint aufrufen können.

7.1.7 On-Access-Scans

7.1.7.1 Ändern der Bedingungen für On-Access-Scans

Bei rollenbasierter Verwaltung müssen Sie hierzu über die Berechtigung **Richtlinieneinstellung – Antivirus und HIPS** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

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 dazu erfahren Sie unter [Welche Richtlinien sind einer Gruppe zugewiesen?](#) (Seite 23).
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 **Dateien prüfen beim** die gewünschten Optionen.

7.1.7.2 Ausschließen von Objekten von On-Access-Scans

Bei rollenbasierter Verwaltung müssen Sie hierzu über die Berechtigung **Richtlinieneinstellung – Antivirus und HIPS** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

Sie können Objekte von On-Access-Scans ausschließen.

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 23).
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-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 80).

7.1.7.3 Aktivieren/Deaktivieren der On-Access-Scans

Bei rollenbasierter Verwaltung müssen Sie hierzu über die Berechtigung **Richtlinieneinstellung – Antivirus und HIPS** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

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 Antivirus- 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 23).
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 neu starten möchten, aktivieren Sie das Kästchen **On-Access-Scans aktivieren** wieder.

7.1.8 Geplante Scans

7.1.8.1 Scannen von Computern zu bestimmten Zeiten

Bei rollenbasierter Verwaltung müssen Sie hierzu über die Berechtigung **Richtlinieneinstellung – Antivirus und HIPS** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

Computer können zu festgesetzten Zeiten gescannt werden.

Hinweis: Geplante Scans bzw. Zeitgesteuerte Überprüfungen können nur auf Windows- und Linux-Computern ausgeführt werden.

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 23).
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 Scanzeitpunkt (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 75).

Hinweis: Wenn beim Scan Threat-Komponenten im Speicher erkannt werden und Sie keine automatische Bereinigung für den Scan eingerichtet haben, wird der Scan angehalten und ein Alert wird an Enterprise Manager gesendet. Wenn der Scan fortgesetzt wird, könnte sich der Threat ausbreiten. Sie müssen den Threat zunächst bereinigen, bevor Sie den Scan erneut ausführen können.

7.1.8.2 Ändern der Einstellungen für geplante Scans

Bei rollenbasierter Verwaltung müssen Sie hierzu über die Berechtigung **Richtlinieneinstellung – Antivirus und HIPS** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

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 23).
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 66), [Scannen auf Adware und PUA](#) (Seite 69) und [Scannen von Archivdateien](#) (Seite 78). Bereinigungs-Optionen werden unter [Einrichten der automatischen Bereinigung](#) (Seite 45) näher erläutert.

7.1.8.3 Ausschließen von Objekten von geplanten Scans

Bei rollenbasierter Verwaltung müssen Sie hierzu über die Berechtigung **Richtlinieneinstellung – Antivirus und HIPS** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

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 43).

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 23).
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 geöffnet. Klicken Sie im Fensterbereich **Geplante Scans** auf **Erweiterungen und Ausschlüsse**.
4. Klicken Sie auf die Registerkarte **Windows-Ausschlüsse** oder **Linux-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 80).

7.1.9 Scan-Optionen

7.1.9.1 Ändern der Scan-Objekte

Bei rollenbasierter Verwaltung müssen Sie hierzu über die Berechtigung **Richtlinieneinstellung – Antivirus und HIPS** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

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.

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. Um den Sophos Update Manager auf einem Mac OS X-Computer zu öffnen, suchen Sie in einem **Finder**-Fenster nach dem Ordner Sophos Anti-Virus:ESOSX. Doppelklicken Sie auf **Sophos Update Manager**. Weitere Details werden in der Hilfe zu Sophos Update Manager 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.

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 dazu erfahren Sie unter [Welche Richtlinien sind einer Gruppe zugewiesen?](#) (Seite 23).
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.

7.1.9.2 Scannen von Macintosh-Dateien

Bei rollenbasierter Verwaltung müssen Sie hierzu über die Berechtigung **Richtlinieneinstellung – Antivirus und HIPS** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

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 dazu erfahren Sie unter [Welche Richtlinien sind einer Gruppe zugewiesen?](#) (Seite 23).
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**.

Markieren Sie auf der Registerkarte **Scans** im Bereich **Scannen auf** das Kontrollkästchen **Macintosh-Viren**.

- **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** im Bereich **Scannen auf** das Kontrollkästchen **Macintosh-Viren**.

7.1.9.3 Scannen auf Rootkits

Bei rollenbasierter Verwaltung müssen Sie hierzu über die Berechtigung **Richtlinieneinstellung – Antivirus und HIPS** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

Beim Durchführen einer vollständigen Systemüberprüfung wird auch auf Rootkits gescannt. (Mehr dazu erfahren Sie unter [Sofort-Scans](#) (Seite 43)). 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 23).
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 **Scans** im Bereich **Scannen auf** das Kontrollkästchen **Rootkits**. Klicken Sie auf **OK**.

7.1.9.4 Scannen von Archivdateien

Bei rollenbasierter Verwaltung müssen Sie hierzu über die Berechtigung **Richtlinieneinstellung – Antivirus und HIPS** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

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 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 23).
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 **Scan- und Bereinigungs-Einstellungen** auf der Registerkarte **Scans** unter *Sonstige Scan-Einstellungen* die Option **Archivdateien scannen**. Klicken Sie auf **OK**.

7.1.9.5 Scannen des Systemspeichers

Bei rollenbasierter Verwaltung müssen Sie hierzu über die Berechtigung **Richtlinieneinstellung – Antivirus und HIPS** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

Endpoint Security and Control für Windows kann den Systemspeicher auf Threats scannen. Der *Systemspeicher* wird vom Betriebssystem genutzt. Der Systemspeicher kann in Endpoint Security and Control in regelmäßigen Abständen im Hintergrund bei aktivierten On-Access-Scans oder im Rahmen eines geplanten Scans gescannt werden.

So können Sie den Systemspeicher scannen:

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 23).
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 **Sonstige Scan-Optionen** das Kontrollkästchen **Systemspeicher scannen**.

■ 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 **Sonstige Scanoptionen** das Kontrollkästchen **Systemspeicher scannen**.

Hinweis: Wenn Sie die automatische Bereinigung von von On-Access-Scans erkannten Viren aktiviert haben, wird unter Umständen eine vollständige Systemüberprüfung eingeleitet, um *alle* Viren vom Computer zu bereinigen. Dieser Vorgang kann viel Zeit in Anspruch nehmen.

7.1.9.6 Scannen mit niedriger Priorität

Bei rollenbasierter Verwaltung müssen Sie hierzu über die Berechtigung **Richtlinieneinstellung – Antivirus und HIPS** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

Sie können einen benutzerdefinierten Scan mit niedriger Priorität ausführen, um die Auswirkungen auf Anwendungen zu minimieren.

Hinweis: Die Option beschränkt sich auf Sophos Endpoint Security and Control für Windows Vista 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 23).
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. Aktivieren Sie im Dialogfeld **Scan- und Bereinigungs-Einstellungen** auf der Registerkarte **Scans** im Bereich *Sonstige Scanoptionen* das Kontrollkästchen **Scan mit niedriger Priorität ausführen**. Klicken Sie auf **OK**.

7.1.9.7 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 9,7 beschrieben.

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

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

Hinweis: Enterprise Manager unterstützt nur Pfad-basierte Linux-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 werden im *Benutzerhandbuch für Sophos Anti-Virus für Linux* aufgeführt.

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

7.2 Konfigurieren der Firewall-Richtlinie

7.2.1 Basiskonfiguration der Firewall

7.2.1.1 Einrichten einer Firewall-Richtlinie

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 Enterprise Manager – 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 112).

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 müssen Sie zum Konfigurieren einer Firewall-Richtlinie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen. Nähere Informationen zur rollenbasierten Verwaltung können Sie dem Abschnitt [Informationen zu Rollen](#) (Seite 15) entnehmen.

So richten Sie eine Firewall-Richtlinie ein:

1. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Firewall**.
2. Doppelklicken Sie auf die **Standardrichtlinie**, um sie zu bearbeiten.

Der **Firewall-Richtlinienassistent** wird geöffnet. Befolgen Sie die Anweisungen auf dem Bildschirm. Diverse Optionen werden unten näher erläutert.

3. 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 (nicht im Firmennetzwerk). Für Laptops empfiehlt sich die Auswahl mehrerer Standorte.

4. 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 89).
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 83).

5. 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.

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 129).

Im Dashboard wird die Anzahl der Computer angezeigt, deren Ereignisanzahl in den vergangenen 7 Tagen einen festgelegten Höchstwert überschritten hat.

7.2.1.2 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-Ereignisregel](#) (Seite 87) 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**.

Wenn unbekannter Datenfluss nicht standardmäßig zugelassen werden soll, betreiben Sie die Firewall im *interaktiven Modus*.

Im interaktiven Modus gibt der Benutzer an, ob Datenfluss und Anwendungen, denen keine Regel zugewiesen wurde, zugelassen oder gesperrt werden sollen. Details entnehmen Sie bitte [Allgemeine Informationen](#) (Seite 88) und anderen Abschnitten im Kapitel „Arbeiten im interaktiven Modus“.

7.2.1.3 Hinzufügen und Zulassen einer Anwendung

Hinweis: Bei rollenbasierter Verwaltung müssen Sie zum Konfigurieren einer Firewall-Richtlinie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

Vertrauenswürdige Anwendungen erhalten uneingeschränkten Vollzugriff auf das Netzwerk und das Internet.

So können Sie eine Anwendung in die Firewall-Richtlinie aufnehmen und zulassen:

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 23).
2. Doppelklicken Sie im Feld **Richtlinien** auf **Firewall** und doppelklicken Sie anschließend auf die Richtlinie, die Sie ändern möchten.
3. Klicken Sie auf der Seite **Arbeitsmodus** des **Firewall-Richtlinienassistenten** auf **Vertrauen**.
Das Dialogfenster **Firewall-Richtlinie** wird angezeigt.
4. Klicken Sie auf **Hinzufügen**.
Das Dialogfenster **Firewall-Richtlinie – Zuverlässige Anwendung hinzufügen** wird angezeigt.
5. Wählen Sie im Dropdown-Menü **Suchperiode** den Zeitraum aus, für den Anwendungsereignisse 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.
6. Wenn Sie Anwendungsereignisse eines bestimmten Typs aufrufen möchten, wählen Sie den gewünschten Typ im Dropdown-Menü **Ereignistyp** aus.

7. Wenn Sie Anwendungsereignisse für eine bestimmte Datei aufrufen möchten, geben Sie in das Feld **Dateiname** den entsprechenden Namen ein.
Wenn Sie keine spezifischen Angaben machen, werden Anwendungsereignisse für alle Dateien angezeigt.
Die Eingabe folgender Platzhalter ist erlaubt: ? für ein einzelnes Zeichen und * für eine Zeichenfolge.
8. Klicken Sie zur Anzeige einer Anwendungsereignisliste auf **Suche**.
9. Wählen Sie ein Anwendungsereignis aus der Liste und klicken Sie auf **OK**.

Die Anwendung wird in die Firewall-Richtlinie aufgenommen und als **vertrauenswürdig** gekennzeichnet.

7.2.1.4 Zulassen des gesamten Dateiflusses in einem lokalen Netzwerk

Hinweis: Bei rollenbasierter Verwaltung müssen Sie zum Konfigurieren einer Firewall-Richtlinie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

So lassen Sie den gesamten Datenfluss zwischen Computern in einem lokalen Netzwerk (Local Area Network) 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 23).
2. Doppelklicken Sie im Feld **Richtlinien** auf **Firewall** und doppelklicken Sie anschließend auf die Richtlinie, die Sie ändern möchten.
3. Wählen Sie in der **Datei- und Druckerfreigabe** auf der Seite des **Firewall-Richtlinien-Assistenten** die Option **Benutzerdefinierte Einstellungen verwenden** und klicken Sie anschließend auf **Benutzerdefiniert**.
4. Aktivieren Sie für ein Netzwerk in der Liste **LAN-Einstellungen** die Option **Zuverlässig**.

Hinweise

- Wenn Sie den gesamten Datenverkehr zwischen den Computern in einem LAN zulassen, werden automatisch auch Dateien und Drucker zur gemeinsamen Nutzung freigegeben.

7.2.1.5 Zulassen der Datei- und Druckerfreigabe

Hinweis: Bei rollenbasierter Verwaltung müssen Sie zum Konfigurieren einer Firewall-Richtlinie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

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 23).
2. Doppelklicken Sie im Feld **Richtlinien** auf **Firewall** und doppelklicken Sie anschließend auf die Richtlinie, die Sie ändern möchten.

3. Wählen Sie auf der Seite **Datei- und Druckerfreigabe** des **Firewall-Richtlinien-Assistenten** die Option **Datei- und Druckerfreigabe zulassen**.

7.2.1.6 Zulassen der flexiblen Steuerung der Datei- und Druckerfreigabe

Hinweis: Bei rollenbasierter Verwaltung müssen Sie zum Konfigurieren einer Firewall-Richtlinie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

Wenn Sie die Datei- und Druckerfreigabe in den Unternehmensnetzwerken flexibler steuern können möchten (z.B. unidirektionalen NetBIOS-Traffic), können Sie wie folgt vorgehen:

1. Lassen Sie die Datei- und Druckerfreigabe auf den LANs (Local Area Networks) zu, die nicht in der Liste mit den **LAN-Einstellungen** aufgeführt sind. So wird der NetBIOS-Traffic auf diesen LANs von den Firewall-Regeln erfasst.
2. Erstellen Sie globale Regeln hoher Priorität, die die Kommunikation zu und von den Hosts mit den passenden NetBIOS-Ports und Protokollen ermöglichen. Es empfiehlt sich, globale Regeln zu erstellen und unerwünschten Traffic der Datei- und Druckerfreigabe zu sperren, anstatt ihn von der Standardregel steuern zu lassen.

So lassen Sie die Datei- und Druckerfreigabe auf den LANs (Local Area Networks) zu, die nicht in der Liste mit den **LAN-Einstellungen** aufgeführt sind:

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 23).
2. Doppelklicken Sie im Feld **Richtlinien** auf **Firewall** und doppelklicken Sie anschließend auf die Richtlinie, die Sie ändern möchten.
3. Wählen Sie in der **Datei- und Druckerfreigabe** auf der Seite des **Firewall-Richtlinien-Assistenten** die Option **Benutzerdefinierte Einstellungen verwenden** und klicken Sie anschließend auf **Benutzerdefiniert**.
4. Deaktivieren Sie die Option **Datei- und Druckerfreigabe für andere Netzwerke sperren**.

7.2.1.7 Sperren unerwünschter Datei- und Druckerfreigabe

Hinweis: Bei rollenbasierter Verwaltung müssen Sie zum Konfigurieren einer Firewall-Richtlinie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

So sperren Sie die Datei- und Druckerfreigabe auf den LANs (Local Area Networks), die nicht in der Liste mit den **LAN-Einstellungen** auf der Registerkarte **LAN** aufgeführt sind:

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 23).
2. Doppelklicken Sie im Feld **Richtlinien** auf **Firewall** und doppelklicken Sie anschließend auf die Richtlinie, die Sie ändern möchten.
3. Wählen Sie in der **Datei- und Druckerfreigabe** auf der Seite des **Firewall-Richtlinien-Assistenten** die Option **Benutzerdefinierte Einstellungen verwenden** und klicken Sie anschließend auf **Benutzerdefiniert**.
4. Aktivieren Sie die Option **Datei- und Druckerfreigabe für andere Netzwerke sperren**.

7.2.1.8 Erstellen einer Firewall-Ereignisregel

Hinweis: Bei rollenbasierter Verwaltung müssen Sie zum Konfigurieren einer Firewall-Richtlinie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

Sie können Regeln für alle Firewall-Ereignisse erstellen. Eine Ausnahme bilden Ereignisse vom Typ „Modifizierter Speicher“.

So können Sie eine Firewall-Ereignisregel 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: 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 104).

7.2.1.9 Vorübergehende Deaktivierung der Firewall

Hinweis: Bei rollenbasierter Verwaltung müssen Sie zum Konfigurieren einer Firewall-Richtlinie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

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 23).
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**.

7.2.2 Erweiterte Konfiguration der Firewall

7.2.2.1 Öffnen der erweiterten Konfiguration

Hinweis: Bei rollenbasierter Verwaltung müssen Sie zum Konfigurieren einer Firewall-Richtlinie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

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**.
3. Klicken Sie im Bereich **Konfigurationen** neben dem Standort, für den Sie die Firewall konfigurieren möchten, auf **Konfigurieren**.

7.2.2.2 Arbeiten im interaktiven Modus

7.2.2.2.1 Allgemeine Informationen

Im interaktiven Modus 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.

7.2.2.2.2 Aktivieren des interaktiven Modus

Hinweis: Bei rollenbasierter Verwaltung müssen Sie zum Konfigurieren einer Firewall-Richtlinie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

Sie können die Firewall im interaktiven Modus betreiben. Der Benutzer wird dabei gefragt, wie mit dem erkannten Datenverkehr umgegangen werden soll. Weitere Informationen finden Sie unter [Allgemeine Informationen](#) (Seite 88).

So können Sie auf Computergruppen den interaktiven Modus 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 23).
2. Doppelklicken Sie im Feld **Richtlinien** auf **Firewall** und doppelklicken Sie anschließend auf die Richtlinie, die Sie ändern möchten.
3. Klicken Sie auf der **Startseite** des **Firewall-Richtlinienassistenten** auf **Erweiterte Einstellungen**.
4. Klicken Sie im Bereich **Konfigurationen** neben dem zu konfigurierenden Standort auf **Konfigurieren**.
5. Klicken Sie auf der Registerkarte **Allgemein** unter **Arbeitsmodus** auf **Interaktiv**.

7.2.2.2.3 Auswählen eines nicht interaktiven Modus

Hinweis: Bei rollenbasierter Verwaltung müssen Sie zum Konfigurieren einer Firewall-Richtlinie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

Es gibt zwei nicht interaktive Modi:

- Standardmäßig zulassen
- Standardmäßig sperren

In den nicht interaktiven Modi regelt die Firewall den Datenfluss automatisch anhand festgelegter Regeln. (Ausgehender) Netzwerk-Datenfluss ohne passende Regeln wird entweder zugelassen oder gesperrt.

So können Sie auf Computergruppen in einen nicht interaktiven Modus der Firewall wechseln:

1. Doppelklicken Sie im Feld **Richtlinien** auf **Firewall** und doppelklicken Sie anschließend auf die Richtlinie, die Sie ändern möchten.
2. Klicken Sie auf der **Startseite** des **Firewall-Richtlinienassistenten** auf **Erweiterte Einstellungen**.
3. Klicken Sie im Bereich **Konfigurationen** neben dem zu konfigurierenden Standort auf **Konfigurieren**.
4. Klicken Sie auf die Registerkarte **Allgemein**.
5. Klicken Sie im Bereich **Arbeitsmodus** auf **Standardmäßig zulassen** bzw. **Standardmäßig sperren**.

7.2.2.3 Konfigurieren der Firewall

7.2.2.3.1 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 finden Sie im Abschnitt [Erstellen einer Anwendungsregel](#) (Seite 104) und anderen Themen zu [Anwendungsregeln](#).

7.2.2.3.2 Aufnahme einer Anwendung in eine Firewall-Richtlinie

Hinweis: Bei rollenbasierter Verwaltung müssen Sie zum Konfigurieren einer Firewall-Richtlinie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

So können Sie eine Anwendung in eine Firewall-Richtlinie aufnehmen:

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 23).
2. Doppelklicken Sie im Feld **Richtlinien** auf **Firewall** und doppelklicken Sie anschließend auf die Richtlinie, die Sie ändern möchten.
3. Klicken Sie auf der **Startseite** des **Firewall-Richtlinienassistenten** auf **Erweiterte Einstellungen**.
4. Klicken Sie im Bereich **Konfigurationen** neben dem zu konfigurierenden Standort auf **Konfigurieren**.
5. Klicken Sie auf die Registerkarte **Anwendungen**.
6. Klicken Sie auf **Hinzufügen**.

Das Dialogfenster **Firewall-Richtlinie – Anwendung hinzufügen** wird angezeigt.

7. Wählen Sie im Dropdown-Menü **Suchperiode** den Zeitraum aus, für den Anwendungsereignisse 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.
8. Wenn Sie Anwendungsereignisse eines bestimmten Typs aufrufen möchten, wählen Sie den gewünschten Typ im Dropdown-Menü **Ereignistyp** aus.
9. Wenn Sie Anwendungsereignisse für eine bestimmte Datei aufrufen möchten, geben Sie in das Feld **Dateiname** den entsprechenden Namen ein.
Wenn Sie keine spezifischen Angaben machen, werden Anwendungsereignisse für alle Dateien angezeigt.
Die Eingabe folgender Platzhalter ist erlaubt: ? für ein einzelnes Zeichen und * für eine Zeichenfolge.
10. Klicken Sie zur Anzeige einer Anwendungsereignisliste auf **Suche**.
11. Wählen Sie ein Anwendungsereignis aus der Liste und klicken Sie auf **OK**.
 - Die Anwendung wird in die Firewall-Richtlinie aufgenommen und als **vertrauenswürdig** gekennzeichnet.
 - Die Prüfsumme der Anwendung wird in die Liste der zulässigen Prüfsummen aufgenommen.

7.2.2.3.3 Entfernen einer Anwendung aus der Firewall-Richtlinie

Hinweis: Bei rollenbasierter Verwaltung müssen Sie zum Konfigurieren einer Firewall-Richtlinie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

So können Sie eine Anwendung aus der Firewall-Richtlinie entfernen:

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 23).
2. Doppelklicken Sie im Feld **Richtlinien** auf **Firewall** und doppelklicken Sie anschließend auf die Richtlinie, die Sie ändern möchten.
3. Klicken Sie auf der **Startseite** des **Firewall-Richtlinienassistenten** auf **Erweiterte Einstellungen**.
4. Klicken Sie im Bereich **Konfigurationen** neben dem zu konfigurierenden Standort auf **Konfigurieren**.
5. Klicken Sie auf die Registerkarte **Anwendungen**.
6. Wählen Sie die Anwendung aus der Liste aus und klicken Sie anschließend auf **Entfernen**.

7.2.2.3.4 Zulassen einer Anwendung

Hinweis: Bei rollenbasierter Verwaltung müssen Sie zum Konfigurieren einer Firewall-Richtlinie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

So lassen Sie eine Anwendung auf einer Computergruppe 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 23).
2. Doppelklicken Sie im Feld **Richtlinien** auf **Firewall** und doppelklicken Sie anschließend auf die Richtlinie, die Sie ändern möchten.
3. Klicken Sie auf der **Startseite** des **Firewall-Richtlinienassistenten** auf **Erweiterte Einstellungen**.
4. Klicken Sie im Bereich **Konfigurationen** neben dem zu konfigurierenden Standort auf **Konfigurieren**.
5. Klicken Sie auf die Registerkarte **Anwendungen**.
Wenn sich die Anwendung nicht in der Liste befindet, befolgen Sie die Anweisungen unter [Aufnahme einer Anwendung in eine Firewall-Richtlinie](#) (Seite 90), um sie hinzuzufügen.
6. Wählen Sie die Anwendung aus der Liste aus und klicken Sie anschließend auf **Vertrauen**.
 - Die Anwendung wird in die Firewall-Richtlinie aufgenommen und als **vertrauenswürdig** gekennzeichnet.
 - Die Prüfsumme der Anwendung wird in die Liste der zulässigen Prüfsummen aufgenommen.

Vertrauenswürdige Anwendungen erhalten uneingeschränkten Vollzugriff auf das Netzwerk und das Internet. Über *Anwendungsregeln* können Sie Bedingungen für die Ausführung der Anwendung festlegen und somit die Sicherheit erhöhen.

- [Erstellen einer Anwendungsregel](#) (Seite 104)
- [Übernahme vordefinierter Anwendungsregeln](#) (Seite 106)

7.2.2.3.5 Zulassen von Anwendungen über die Ereignisanzeige der Firewall

Hinweis: Bei rollenbasierter Verwaltung müssen Sie zum Konfigurieren einer Firewall-Richtlinie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

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 als vertrauenswürdig eingestuft bzw. für die eine Regel erstellt werden soll, und 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**.
- Wenn Sie Prüfsummen verwenden, müssen Sie die Prüfsumme der Anwendung unter Umständen in die Liste der erlaubten Prüfsummen aufnehmen. Mehr dazu erfahren Sie unter [Hinzufügen einer Anwendungsprüfsumme](#) (Seite 95).
 - 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 104).

7.2.2.3.6 Sperren einer Anwendung

Hinweis: Bei rollenbasierter Verwaltung müssen Sie zum Konfigurieren einer Firewall-Richtlinie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

So sperren Sie eine Anwendung auf einer 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 23).
2. Doppelklicken Sie im Feld **Richtlinien** auf **Firewall** und doppelklicken Sie anschließend auf die Richtlinie, die Sie ändern möchten.

3. Klicken Sie auf der **Startseite** des **Firewall-Richtlinienassistenten** auf **Erweiterte Einstellungen**.
4. Klicken Sie im Bereich **Konfigurationen** neben dem zu konfigurierenden Standort auf **Konfigurieren**.
5. Klicken Sie auf die Registerkarte **Anwendungen**.
Wenn sich die Anwendung nicht in der Liste befindet, befolgen Sie die Anweisungen unter [Aufnahme einer Anwendung in eine Firewall-Richtlinie](#) (Seite 90), um sie hinzuzufügen.
6. Wählen Sie die Anwendung aus der Liste aus und klicken Sie anschließend auf **Sperren**.

7.2.2.3.7 Zulassen versteckter Prozesse

Hinweis: Bei rollenbasierter Verwaltung müssen Sie zum Konfigurieren einer Firewall-Richtlinie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

Eine Anwendung kann im Hintergrund einen anderen Prozess starten, der für sie auf das Netzwerk zugreift.

Malware kann auf diese Weise Firewalls umgehen: Zum Zugriff auf das Netzwerk wird eine vertrauenswürdige Anwendung und nicht die Malware selbst gestartet.

So erlauben Sie Anwendungen den Start versteckter Prozesse:

1. Doppelklicken Sie auf die zu ändernde Firewall-Richtlinie.
2. Klicken Sie auf der **Startseite** des **Firewall-Richtlinienassistenten** auf **Erweiterte Einstellungen**.
3. Klicken Sie im Bereich **Konfigurationen** neben dem Standort, für den Sie die Firewall konfigurieren möchten, auf **Konfigurieren**.
4. Klicken Sie auf die Registerkarte **Prozesse**.
5. Klicken Sie im oberen Bereich auf **Hinzufügen**.

Das Dialogfenster **Firewall-Richtlinie – Anwendung hinzufügen** wird angezeigt.

6. Wählen Sie im Dropdown-Menü **Suchperiode** den Zeitraum aus, für den Anwendungsereignisse 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.
7. Wenn Sie Anwendungsereignisse eines bestimmten Typs aufrufen möchten, wählen Sie den gewünschten Typ im Dropdown-Menü **Ereignistyp** aus.
8. Wenn Sie Anwendungsereignisse für eine bestimmte Datei aufrufen möchten, geben Sie in das Feld **Dateiname** den entsprechenden Namen ein.
Wenn Sie keine spezifischen Angaben machen, werden Anwendungsereignisse für alle Dateien angezeigt.
Die Eingabe folgender Platzhalter ist erlaubt: ? für ein einzelnes Zeichen und * für eine Zeichenfolge.
9. Klicken Sie zur Anzeige einer Anwendungsereignisliste auf **Suche**.
10. Wählen Sie ein Anwendungsereignis aus der Liste und klicken Sie auf **OK**.

Im interaktiven Modus kann die Firewall Lerndialoge auf dem Endpoint anzeigen, wenn neue Startprogramme erkannt werden. Mehr dazu erfahren Sie unter [Aktivieren des interaktiven Modus](#) (Seite 88).

7.2.2.3.8 Zulassen von Raw-Sockets

Hinweis: Bei rollenbasierter Verwaltung müssen Sie zum Konfigurieren einer Firewall-Richtlinie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

Einige Anwendungen können den Netzwerkzugriff über Raw-Sockets herstellen, wodurch sie die im Netzwerk gesendeten Daten beeinflussen können.

Schadprogramme können Raw-Sockets ausnutzen, indem sie deren IP-Adressen duplizieren oder korruptierte Meldungen senden.

So lassen Sie den Zugriff über Raw-Sockets zu:

1. Doppelklicken Sie auf die zu ändernde Firewall-Richtlinie.
2. Klicken Sie auf der **Startseite** des **Firewall-Richtlinienassistenten** auf **Erweiterte Einstellungen**.
3. Klicken Sie im Bereich **Konfigurationen** neben dem Standort, für den Sie die Firewall konfigurieren möchten, auf **Konfigurieren**.
4. Klicken Sie auf die Registerkarte **Prozesse**.
5. Klicken Sie im oberen Bereich auf **Hinzufügen**.

Das Dialogfenster **Firewall-Richtlinie – Anwendung hinzufügen** wird angezeigt.

6. Wählen Sie im Dropdown-Menü **Suchperiode** den Zeitraum aus, für den Anwendungsereignisse 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.
7. Wenn Sie Anwendungsereignisse eines bestimmten Typs aufrufen möchten, wählen Sie den gewünschten Typ im Dropdown-Menü **Ereignistyp** aus.
8. Wenn Sie Anwendungsereignisse für eine bestimmte Datei aufrufen möchten, geben Sie in das Feld **Dateiname** den entsprechenden Namen ein.
Wenn Sie keine spezifischen Angaben machen, werden Anwendungsereignisse für alle Dateien angezeigt.
Die Eingabe folgender Platzhalter ist erlaubt: ? für ein einzelnes Zeichen und * für eine Zeichenfolge.
9. Klicken Sie zur Anzeige einer Anwendungsereignisliste auf **Suche**.
10. Wählen Sie ein Anwendungsereignis aus der Liste und klicken Sie auf **OK**.

Im interaktiven Modus kann die Firewall Lerndialoge auf dem Endpoint anzeigen, wenn neue Raw-Sockets erkannt werden. Mehr dazu erfahren Sie unter [Aktivieren des interaktiven Modus](#) (Seite 88).

7.2.2.3.9 Hinzufügen einer Anwendungsprüfsumme

Hinweis: Bei rollenbasierter Verwaltung müssen Sie zum Konfigurieren einer Firewall-Richtlinie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

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. Klicken Sie auf die Registerkarte **Prüfsummen**.
4. Klicken Sie auf **Hinzufügen**.

Das Dialogfenster **Firewall-Richtlinie – Anwendungsprüfsumme hinzufügen** wird angezeigt.

5. Wählen Sie im Dropdown-Menü **Suchperiode** den Zeitraum aus, für den Anwendungsereignisse 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.
6. Klicken Sie im Feld **Ereignistyp** auf den Dropdown-Pfeil und geben Sie an, ob eine Prüfsumme für geänderte oder neue Anwendungen hinzugefügt werden soll.
7. Wenn Sie Anwendungsereignisse für eine bestimmte Datei aufrufen möchten, geben Sie in das Feld **Dateiname** den entsprechenden Namen ein.
Wenn Sie keine spezifischen Angaben machen, werden Anwendungsereignisse für alle Dateien angezeigt.
Die Eingabe folgender Platzhalter ist erlaubt: ? für ein einzelnes Zeichen und * für eine Zeichenfolge.
8. Klicken Sie zur Anzeige einer Anwendungsereignisliste auf **Suche**.
9. Wählen Sie das Anwendungsereignis aus, für das Sie eine Prüfsumme hinzufügen möchten, und klicken Sie auf **OK**.

Die Anwendungsprüfsumme wird der Liste der zugelassenen Prüfsummen im Dialogfeld **Firewall-Richtlinie** hinzugefügt.

Im interaktiven Modus kann die Firewall Lerndialoge auf dem Endpoint anzeigen, wenn neue oder geänderte Anwendungen erkannt werden. Mehr dazu erfahren Sie unter [Aktivieren des interaktiven Modus](#) (Seite 88).

7.2.2.3.10 Aktivieren/Deaktivieren des Sperrens modifizierter Prozesse

Hinweis: Bei rollenbasierter Verwaltung müssen Sie zum Konfigurieren einer Firewall-Richtlinie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

Unter Umständen versuchen Malware-Autoren die Firewall zu umgehen, indem ein Prozess im Speicher modifiziert wird, der von einem vertrauenswürdigen Programm eingeleitet wurde. Anschließend wird versucht, über den modifizierten Prozess Zugriff zum Netzwerk zu erlangen.

Sie können die Firewall zum Erkennen und Sperren von modifizierten Prozessen im Speicher konfigurieren.

Verfahren Sie zum Aktivieren/Deaktivieren des Sperrens modifizierter Prozesse wie folgt:

1. Doppelklicken Sie auf die zu ändernde Firewall-Richtlinie.
2. Klicken Sie auf der **Startseite** des **Firewall-Richtlinienassistenten** auf **Erweiterte Einstellungen**.
3. Klicken Sie im Bereich **Konfigurationen** neben dem Standort, für den Sie die Firewall konfigurieren möchten, auf **Konfigurieren**.
4. Deaktivieren Sie auf der Registerkarte **Allgemein** im Bereich **Sperren** die Option **Prozesse sperren, wenn Speicher durch andere Anwendung geändert wird**, um das Sperren modifizierter Prozesse zu deaktivieren.

Wenn Sie das Sperren modifizierter Prozesse wieder aktivieren möchten, wählen Sie das Kontrollkästchen aus.

Wenn die Firewall erkennt, dass ein Prozess im Speicher geändert, werden Regeln hinzugefügt, die verhindern, dass der modifizierte Prozess auf das Netzwerk zugreift.

Hinweise

- Wir raten davon ab, das Sperren modifizierter Prozesse über einen längeren Zeitraum zu deaktivieren. Die Deaktivierung sollte sich auf den Bedarfsfall beschränken.
- Das Sperren modifizierter Prozesse wird auf 64-Bit-Versionen von Windows nicht unterstützt.
- Nur der modifizierte Prozess selbst kann gesperrt werden. Dem modifizierten Programm wird der Netzwerkzugriff jedoch nicht verweigert.

7.2.2.3.11 Filtern von ICMP-Meldungen

Hinweis: Bei rollenbasierter Verwaltung müssen Sie zum Konfigurieren einer Firewall-Richtlinie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

ICMP-Meldungen (Internet Control Message Protocol) ermöglichen Computern im Netzwerk die Freigabe von Fehler- und Statusinformationen. Sie können bestimmte Typen eingehender oder ausgehender ICMP-Meldungen zulassen oder sperren.

Die Filterung von ICMP-Meldungen empfiehlt sich lediglich, wenn Sie mit Netzwerkprotokollen vertraut sind. Im Abschnitt [Erläuterung der ICMP-Meldungen](#) (Seite 97) werden die ICMP-Meldungstypen beschrieben.

So filtern Sie ICMP-Meldungen:

1. Doppelklicken Sie auf die zu ändernde Firewall-Richtlinie.
2. Klicken Sie auf der **Startseite** des **Firewall-Richtlinienassistenten** auf **Erweiterte Einstellungen**.

3. Klicken Sie im Bereich **Konfigurationen** neben dem Standort, für den Sie die Firewall konfigurieren möchten, auf **Konfigurieren**.
4. Wählen Sie auf der Registerkarte **ICMP** die Option **Eingehend** oder **Ausgehend**, um eingehende bzw. ausgehende Meldungen des angegebenen Typs zuzulassen.

7.2.2.3.12 Erläuterung der ICMP-Meldungen

Echo-Anforderung, Echo-Antwort	Meldung zum Testen von Verfügbarkeit und Status des Ziels. Ein Host sendet eine Echo-Anfrage und wartet auf eine Echo-Antwort . Dies erfolgt in der Regel über den ping -Befehl.
Ziel nicht erreichbar, Echo-Antwort	Meldung eines Routers, der ein IP-Datagramm nicht abliefern kann. Ein Datagramm ist eine Dateneinheit oder ein Paket, die/das in einem TCP-/IP-Netzwerk übertragen wird.
Quelldrosselung	Meldung eines Hosts oder Routers, wenn Daten zu schnell eingehen und somit nicht verarbeitet werden können. Die Meldung ist als Aufforderung zur Verringerung der Datagramm-Übertragungsrate durch die Quelle zu verstehen.
Umleitung	Meldung eines Routers bei Empfang eines an einen anderen Router gerichteten Datagramms. Die Meldung umfasst die Adresse, an die Datagramme von der Quelle künftig gesendet werden sollen. Sie dient der Optimierung des Routings von Datenfluss im Netzwerk.
Router-Ankündigung, Router-Anfrage	Die Meldung macht Hosts auf Router aufmerksam. Router versenden regelmäßig ihre IP-Adressen über Router-Ankündigungsmeldungen . Mitunter fordern Hosts mittels Router-Anfragen Router-Adressen an. Die Antwort durch den Router erfolgt über Router-Ankündigungen .
Datagramm-Zeitüberschreitung	Meldung eines Routers, wenn ein Datagramm die maximale Routeranzahl erreicht hat.
Datagramm-Parameterproblem	Meldung eines Routers, wenn bei der Übertragung eines Datagramms ein Problem auftritt und die Verarbeitung nicht abgeschlossen werden kann. Solche Probleme werden beispielsweise durch ungültige Datagramm-Header verursacht.
Zeitstempel-Anforderung, Zeitstempel-Antwort	Dient der zeitlichen Synchronisierung von Hosts und der Schätzung der Transitzeit.
Informations-Anforderung, Informations-Antwort	Veraltet. Die Meldungen wurden zur Bestimmung der Internetwork-Adressen von Hosts eingesetzt, gelten jetzt aber als veraltet und sollten nicht mehr verwendet werden.

Adressmasken-Anforderung, Adressmasken-Antwort Meldung zur Ermittlung der Subnetz-Maske (d.h. der Adressabschnitte, die das Netzwerk definieren). Ein Host sendet eine **Adressmasken-Anforderung** an einen Router und empfängt eine **Adressmasken-Antwort**.

7.2.2.4 Firewall-Regeln

7.2.2.4.1 Allgemeine Informationen

Globale Regeln

Globale Regeln gelten für die gesamte Netzwerkkommunikation sowie für Anwendungen, für die Anwendungsregeln erstellt wurden.

Anwendungsregeln

Einer Anwendung kann eine oder mehrere Regeln zugewiesen werden. Sie können die vordefinierten Regeln von Sophos verwenden oder benutzerdefinierte Regeln erstellen und so den Zugriff auf eine Anwendung ganz an die Bedürfnisse in Ihrem Unternehmen anpassen.

7.2.2.4.2 Reihenfolge der Regeln

Für Raw-Socket-Verbindungen werden nur die globalen Regeln abgerufen.

In Abhängigkeit davon, ob die Verbindung zu einer Netzwerkadresse in der Registerkarte **LAN** besteht, werden bei Verbindungen *ohne* Raw-Sockets werden diverse Regeln geprüft.

Wenn die Netzwerkadresse nicht in der Registerkarte **LAN** aufgeführt wird, werden die folgenden Regeln geprüft:

- Wenn die Adresse als **Zuverlässig** ausgewiesen wird, wird der gesamte über diese Verbindung laufende Datenfluss ohne weitere Prüfungen zugelassen.
- Wenn die Adresse als **NetBIOS** ausgewiesen wurde, wird Datei- und Druckerfreigabe auf allen Verbindungen zugelassen, die die folgenden Voraussetzungen erfüllt:

Verbindung	Port	Reichweite
TCP	Remote	137-139 oder 445
TCP	Lokal	137-139 oder 445
UDP	Remote	137 oder 138
UDP	Lokal	137 oder 138

Wenn sich die Netzwerkadresse *nicht* in der Registerkarte **LAN** befindet, werden andere Firewall-Regeln in der folgenden Reihenfolge geprüft:

1. **NetBIOS-Datenfluss**, der nicht auf der Registerkarte **LAN** zugelassen wird, wird über die Option **Datei- und Druckerfreigabe für andere Netzwerke sperren** geregelt:
 - Wenn die Option aktiviert ist, wird der Datenfluss gesperrt.
 - Wenn die Option nicht aktiviert ist, regeln die restlichen Regeln den Datenfluss.

2. Die globalen Richtlinien hoher Priorität werden in der aufgelisteten Reihenfolge abgerufen.
3. Wenn der Verbindung noch keine Regel zugewiesen wurde, werden Anwendungsregeln abgerufen.
4. Wenn die Verbindung immer noch nicht erfasst wurde, werden die globalen Regeln normaler Priorität in der festgelegten Reihenfolge abgerufen.
5. Wenn keine Regeln für die Verbindung abgerufen werden konnten:
 - Im Modus **Datenfluss ohne passende Regel zulassen** wird der (ausgehende) Datenfluss zugelassen.
 - Im Modus **Datenfluss ohne passende Regel sperren** wird der Datenfluss gesperrt.
 - Im Modus **Interaktiv** wird der Benutzer gefragt, wie er mit der Verbindung verfahren möchte.

Hinweis: Wenn Sie den Arbeitsmodus nicht geändert haben, befindet sich die Firewall im Modus **Standardmäßig sperren**.

7.2.2.4.3 Lokale Netzwerkerkennung

Sie können den Firewall-Regeln für diesen Computer ein lokales Netzwerk zuweisen.

Die Firewall ermittelt das lokale Netzwerk des Computers beim Starten und stellt bei der Ausführung ggf. Änderungen fest. Bei Änderungen aktualisiert die Firewall die Regeln des lokalen Netzwerks mit dem neuen Adressbereich des lokalen Netzwerks.



Vorsicht: Bei lokalen Netzwerkregeln in sekundären Konfigurationen ist Vorsicht geboten. Laptops, die außerhalb des Unternehmens eingesetzt werden, stellen unter Umständen eine Verbindung zu einem unbekanntem lokalen Netzwerk her. Wenn dies der Fall ist, wird aufgrund der Firewallregeln der sekundären Konfiguration, bei denen die Adresse das lokale Netzwerk ist, unter Umständen der gesamte unbekannte Datenverkehr zugelassen.

7.2.2.4.4 Globale Regeln

7.2.2.4.4.1 Standardeinstellungen globaler Regeln

In diesem Abschnitt werden Bedingungen und Maßnahmen zu den standardmäßigen globalen Regeln erläutert. Es empfiehlt sich, diese Einstellungen beim Erstellen einer neuen standardmäßigen globalen Regel zu beachten.

DNS-Auflösung (TCP) zulassen

- Protokoll: TCP
- Richtung: Ausgehend
- Remote-Port: DOMÄNE
- Maßnahme: Zulassen

DNS-Auflösung (UDP) zulassen

- Protokoll: UDP
- Richtung: Ausgehend
- Remote-Port: DNS

- Maßnahme: Stateful Inspection zulassen

Ausgehendes DHCP zulassen

- Protokoll: UDP
- Lokaler Port: BOOTPS,BOOTPC,546,547
- Maßnahme: Zulassen

Eingehende Identifizierung zulassen

- Protokoll: TCP
- Richtung: Eingehend
- Lokaler Port: AUTH
- Maßnahme: Zulassen

Loopback zulassen

- Protokoll: TCP
- Richtung: Eingehend
- Lokaler Port: 127.0.0.0 (255.255.255.0)
- Maßnahme: Zulassen

GRE-Protokoll zulassen

- Protokoll: TCP
- Protokolltyp: Ausgehend
- Maßnahme: Zulassen

PPTP-Control-Verbindung zulassen

- Protokoll: TCP
- Richtung: Ausgehend
- Remote-Port: PPTP
- Lokaler Port: 1024-65535
- Maßnahme: Zulassen

RPC-Call (TCP) sperren

- Protokoll: TCP
- Richtung: Eingehend
- Lokaler Port: DCOM
- Maßnahme: Sperren

RPC-Call (UDP) sperren

- Protokoll: UDP
- Lokaler Port: 135

- Maßnahme: Sperren

Server Message Block-Protokoll (UDP) sperren

- Protokoll: TCP
- Richtung: Eingehend
- Lokaler Port: MICROSOFT_DS
- Maßnahme: Sperren

Server Message Protokoll (UDP) sperren

- Protokoll: TCP
- Lokaler Port: 445
- Maßnahme: Sperren

Localhost-Verbindung (UDP) zulassen

- Protokoll: UDP
- Remote-Host: 255.255.255.255 (0.0.0.0)
- Lokaler Host: 255.255.255.255 (0.0.0.0)
- Der lokale Port ist dem Remote-Port dabei gleich: True
- Maßnahme: Zulassen

7.2.2.4.4.2 Erstellen einer globalen Regel

Hinweis: Bei rollenbasierter Verwaltung müssen Sie zum Konfigurieren einer Firewall-Richtlinie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

Wichtig: Das Erstellen globaler Regeln empfiehlt sich lediglich, wenn Sie sich mit Netzwerkprotokollen auskennen.

Globale Regeln gelten für alle Datenbewegungen im Netzwerk und für Anwendungen, denen noch keine Regel zugewiesen wurde.

So erstellen Sie eine globale Regel:

1. Doppelklicken Sie auf die zu ändernde Firewall-Richtlinie.
2. Klicken Sie auf der **Startseite** des **Firewall-Richtlinienassistenten** auf **Erweiterte Einstellungen**.
3. Klicken Sie im Bereich **Konfigurationen** neben dem Standort, für den Sie die Firewall konfigurieren möchten, auf **Konfigurieren**.
4. Klicken Sie auf die Registerkarte **Globale Regel**.
5. Klicken Sie auf **Hinzufügen**.
6. Geben Sie unter **Regelname** den gewünschten Regelnamen ein.
Der Regelname darf in einer Regelliste nicht mehrfach verwendet werden. Alle globalen Regeln müssen einen eindeutigen Namen haben.

7. Wenn die Regel vor Anwendungsregeln oder anderen Regeln normaler Priorität greifen soll, wählen Sie die Option **Regel mit hoher Priorität**.
Weitere Informationen zur Regelpriorität finden Sie unter [Reihenfolge der Regeln](#) (Seite 98).
8. Wählen Sie im Bereich **Ereignisse, für die die Regel zutreffen soll** die Bedingungen aus, die eine Verbindung erfüllen muss, damit die Regel greift.
9. Wählen Sie im Bereich **Maßnahmen, die die Regel ergreifen soll Zulassen** oder **Sperren** aus.
10. Führen Sie einen der folgenden Schritte aus:
 - Wählen Sie die Option **Gleichzeitige Verbindungen** aus, damit weitere Verbindungen von und an die gleiche Remote-Adresse möglich sind, auch wenn die ursprüngliche Verbindung besteht.
Hinweis: Die Option beschränkt sich auf TCP-Regeln, die standardmäßig statusbehaftet sind.
 - Bei Auswahl der Option **Stateful Inspection** basieren die Antworten des Remote-Computers auf der ersten Verbindung.
11. Klicken Sie im Bereich **Regelbeschreibung** auf einen unterstrichenen Wert. Wenn Sie beispielsweise auf den Link **TCP** klicken, wird das Dialogfeld **Protokoll wählen** geöffnet.

7.2.2.4.4.3 Ändern einer globalen Regel

Hinweis: Bei rollenbasierter Verwaltung müssen Sie zum Konfigurieren einer Firewall-Richtlinie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

Wichtig: Das Ändern globaler Regeln empfiehlt sich lediglich, wenn Sie sich mit Netzwerkprotokollen auskennen.

So ändern Sie eine globale Regel:

1. Doppelklicken Sie auf die zu ändernde Firewall-Richtlinie.
2. Klicken Sie auf der **Startseite** des **Firewall-Richtlinienassistenten** auf **Erweiterte Einstellungen**.
3. Klicken Sie im Bereich **Konfigurationen** neben dem Standort, für den Sie die Firewall konfigurieren möchten, auf **Konfigurieren**.
4. Klicken Sie auf die Registerkarte **Globale Regel**.
5. Wählen Sie die gewünschte Regel aus der **Regelliste** aus.
6. Klicken Sie auf **Bearbeiten**.

Nähere Informationen zu den Einstellungen globaler Regeln können Sie dem Abschnitt [Standardeinstellungen globaler Regeln](#) (Seite 99) entnehmen.

7.2.2.4.4.4 Kopieren einer globalen Regel

Hinweis: Bei rollenbasierter Verwaltung müssen Sie zum Konfigurieren einer Firewall-Richtlinie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

So kopieren Sie eine globale Regel und nehmen sie in die Regelliste auf:

1. Doppelklicken Sie auf die zu ändernde Firewall-Richtlinie.
2. Klicken Sie auf der **Startseite** des **Firewall-Richtlinienassistenten** auf **Erweiterte Einstellungen**.
3. Klicken Sie im Bereich **Konfigurationen** neben dem Standort, für den Sie die Firewall konfigurieren möchten, auf **Konfigurieren**.
4. Klicken Sie auf die Registerkarte **Globale Regel**.
5. Wählen Sie die gewünschte Regel aus der **Regelliste** aus.
6. Klicken Sie auf **Kopieren**.

7.2.2.4.4.5 Löschen einer globalen Regel

Hinweis: Bei rollenbasierter Verwaltung müssen Sie zum Konfigurieren einer Firewall-Richtlinie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

1. Doppelklicken Sie auf die zu ändernde Firewall-Richtlinie.
2. Klicken Sie auf der **Startseite** des **Firewall-Richtlinienassistenten** auf **Erweiterte Einstellungen**.
3. Klicken Sie im Bereich **Konfigurationen** neben dem Standort, für den Sie die Firewall konfigurieren möchten, auf **Konfigurieren**.
4. Klicken Sie auf die Registerkarte **Globale Regel**.
5. Wählen Sie die gewünschte Regel aus der **Regelliste** aus.
6. Klicken Sie auf **Entfernen**.

7.2.2.4.4.6 Ändern der Priorität von globalen Regeln

Hinweis: Bei rollenbasierter Verwaltung müssen Sie zum Konfigurieren einer Firewall-Richtlinie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

Globale Regeln werden in der Reihenfolge angewandt, in der sie in der Regelliste aufgeführt werden (von oben nach unten).

So können Sie die Priorität von globalen Regeln ändern:

1. Doppelklicken Sie auf die zu ändernde Firewall-Richtlinie.
2. Klicken Sie auf der **Startseite** des **Firewall-Richtlinienassistenten** auf **Erweiterte Einstellungen**.
3. Klicken Sie im Bereich **Konfigurationen** neben dem Standort, für den Sie die Firewall konfigurieren möchten, auf **Konfigurieren**.
4. Klicken Sie auf die Registerkarte **Globale Regel**.
5. Klicken Sie in der **Regelliste** auf die Regel, die Sie nach oben oder unter verschieben möchten.
6. Klicken Sie auf **Nach oben** oder **Nach unten**.

7.2.2.4.5 Anwendungsregeln

7.2.2.4.5.1 Erstellen einer Anwendungsregel

Hinweis: Bei rollenbasierter Verwaltung müssen Sie zum Konfigurieren einer Firewall-Richtlinie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

So erstellen Sie eine Anwendungsregel, um den Zugriff auf eine bestimmte Anwendung an die Bedürfnisse in Ihrem Unternehmen anzupassen:

1. Doppelklicken Sie auf die zu ändernde Firewall-Richtlinie.
2. Klicken Sie auf der **Startseite** des **Firewall-Richtlinienassistenten** auf **Erweiterte Einstellungen**.
3. Klicken Sie im Bereich **Konfigurationen** neben dem Standort, für den Sie die Firewall konfigurieren möchten, auf **Konfigurieren**.
4. Klicken Sie auf die Registerkarte **Anwendungen**.
5. Wählen Sie die Anwendung aus der Liste aus und klicken Sie anschließend auf den Pfeil neben der Option **Regel**.
6. Klicken Sie im Dialogfeld **Anwendungsregeln** auf **Hinzufügen**.
7. Geben Sie unter **Regelname** den gewünschten Regelnamen ein.
Der Regelname darf in einer Regelliste nicht mehrfach verwendet werden. Jedoch können zwei Anwendungen gleichnamige Regeln zugewiesen werden.
8. Wählen Sie im Bereich **Ereignisse, für die die Regel zutreffen soll** die Bedingungen aus, die eine Verbindung erfüllen muss, damit die Regel greift.
9. Wählen Sie im Bereich **Maßnahmen, die die Regel ergreifen soll Zulassen** oder **Sperren** aus.
10. Bei Auswahl der Option **Stateful Inspection** basieren die Antworten des Remote-Computers auf der ersten Verbindung.
11. Klicken Sie im Bereich **Regelbeschreibung** auf einen unterstrichenen Wert. Wenn Sie beispielsweise auf den Link **TCP** klicken, wird das Dialogfeld **Protokoll wählen** geöffnet.

7.2.2.4.5.2 Erstellen einer Anwendungsregel aus einer Firewall-Richtlinie

Hinweis: Bei rollenbasierter Verwaltung müssen Sie zum Konfigurieren einer Firewall-Richtlinie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

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.

7.2.2.4.5.3 Bearbeiten einer Anwendungsregel

Hinweis: Bei rollenbasierter Verwaltung müssen Sie zum Konfigurieren einer Firewall-Richtlinie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

1. Doppelklicken Sie auf die zu ändernde Firewall-Richtlinie.
2. Klicken Sie auf der **Startseite** des **Firewall-Richtlinienassistenten** auf **Erweiterte Einstellungen**.
3. Klicken Sie im Bereich **Konfigurationen** neben dem Standort, für den Sie die Firewall konfigurieren möchten, auf **Konfigurieren**.
4. Klicken Sie auf die Registerkarte **Anwendungen**.
5. Wählen Sie die Anwendung aus der Liste aus und klicken Sie anschließend auf den Pfeil neben der Option **Regel**.
6. Klicken Sie im Dialogfeld **Anwendungsregeln** auf **Bearbeiten**.
7. Geben Sie unter **Regelname** den gewünschten Regelnamen ein.
Der Regelname darf in einer Regelliste nicht mehrfach verwendet werden. Jedoch können zwei Anwendungen gleichnamige Regeln zugewiesen werden.
8. Wählen Sie im Bereich **Ereignisse, für die die Regel zutreffen soll** die Bedingungen aus, die eine Verbindung erfüllen muss, damit die Regel greift.
9. Wählen Sie im Bereich **Maßnahmen, die die Regel ergreifen soll Zulassen** oder **Sperren** aus.
10. Bei Auswahl der Option **Stateful Inspection** basieren die Antworten des Remote-Computers auf der ersten Verbindung.

11. Klicken Sie im Bereich **Regelbeschreibung** auf einen unterstrichenen Wert. Wenn Sie beispielsweise auf den Link **TCP** klicken, wird das Dialogfeld **Protokoll wählen** geöffnet.

7.2.2.4.5.4 Übernahme vordefinierter Anwendungsregeln

Hinweis: Bei rollenbasierter Verwaltung müssen Sie zum Konfigurieren einer Firewall-Richtlinie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

Bei einer vordefinierten Regel handelt es sich um einen Satz von Anwendungsregeln, der von Sophos erstellt wurde. So fügen Sie einer Anwendung vordefinierte Regeln zur bestehenden Liste hinzu:

1. Doppelklicken Sie auf die zu ändernde Firewall-Richtlinie.
2. Klicken Sie auf der **Startseite** des **Firewall-Richtlinienassistenten** auf **Erweiterte Einstellungen**.
3. Klicken Sie im Bereich **Konfigurationen** neben dem Standort, für den Sie die Firewall konfigurieren möchten, auf **Konfigurieren**.
4. Klicken Sie auf die Registerkarte **Anwendungen**.
5. Wählen Sie die Anwendung aus der Liste aus und klicken Sie anschließend auf den Pfeil neben der Option **Regel**.
6. Richten Sie den Mauszeiger auf **Regeln aus Voreinstellungen hinzufügen** und klicken Sie auf eine vordefinierte Regel.

7.2.2.4.5.5 Kopieren einer Anwendungsregel

Hinweis: Bei rollenbasierter Verwaltung müssen Sie zum Konfigurieren einer Firewall-Richtlinie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

So kopieren Sie eine Anwendungsregel und nehmen sie in die Regelliste auf:

1. Doppelklicken Sie auf die zu ändernde Firewall-Richtlinie.
2. Klicken Sie auf der **Startseite** des **Firewall-Richtlinienassistenten** auf **Erweiterte Einstellungen**.
3. Klicken Sie im Bereich **Konfigurationen** neben dem Standort, für den Sie die Firewall konfigurieren möchten, auf **Konfigurieren**.
4. Klicken Sie auf die Registerkarte **Anwendungen**.
5. Wählen Sie die Anwendung aus der Liste aus und klicken Sie anschließend auf den Pfeil neben der Option **Regel**.
6. Klicken Sie im Dialogfeld **Anwendungsregeln** auf **Kopieren**.

7.2.2.4.5.6 Löschen einer Anwendungsregel

Hinweis: Bei rollenbasierter Verwaltung müssen Sie zum Konfigurieren einer Firewall-Richtlinie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

1. Doppelklicken Sie auf die zu ändernde Firewall-Richtlinie.

2. Klicken Sie auf der **Startseite** des **Firewall-Richtlinienassistenten** auf **Erweiterte Einstellungen**.
3. Klicken Sie im Bereich **Konfigurationen** neben dem Standort, für den Sie die Firewall konfigurieren möchten, auf **Konfigurieren**.
4. Klicken Sie auf die Registerkarte **Anwendungen**.
5. Wählen Sie die Anwendung aus der Liste aus und klicken Sie anschließend auf den Pfeil neben der Option **Regel**.
6. Klicken Sie im Dialogfeld **Anwendungsregeln** auf **Entfernen**.

7.2.2.4.5.7 Ändern der Priorität von Anwendungsregeln

Hinweis: Bei rollenbasierter Verwaltung müssen Sie zum Konfigurieren einer Firewall-Richtlinie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

Anwendungsregeln werden in der Reihenfolge angewandt, in der sie in der Regelliste aufgeführt werden (von oben nach unten).

Sie können die Priorität von Anwendungsregeln ändern:

1. Doppelklicken Sie auf die zu ändernde Firewall-Richtlinie.
2. Klicken Sie auf der **Startseite** des **Firewall-Richtlinienassistenten** auf **Erweiterte Einstellungen**.
3. Klicken Sie im Bereich **Konfigurationen** neben dem Standort, für den Sie die Firewall konfigurieren möchten, auf **Konfigurieren**.
4. Klicken Sie auf die Registerkarte **Anwendungen**.
5. Wählen Sie die Anwendung aus der Liste aus und klicken Sie anschließend auf den Pfeil neben der Option **Regel**.
6. Klicken Sie in der **Regelliste** auf die Regel, die Sie nach oben oder unter verschieben möchten.
7. Klicken Sie auf **Nach oben** oder **Nach unten**.

7.2.2.5 Standortspezifische Konfiguration

7.2.2.5.1 Allgemeine Informationen

Die standortspezifische Konfiguration ist eine Funktion von Sophos Client Firewall. Hierbei wird allen Netzwerkadpatern des Computers je nach aktuellem Standort des Netzwerkadapters eine Firewall-Konfiguration zugewiesen.

Die Funktion bietet sich an, wenn Sie ein Unternehmenslaptop besitzen und von zu Hause aus arbeiten. Sie verwenden zwei Netzwerkverbindungen gleichzeitig:

- Wenn Sie den Computer zu Unternehmenszwecken nutzen, stellen Sie eine Verbindung über einen VPN-Client und einen **virtuellen Netzwerkadpater** zum Unternehmensnetzwerk her.
- Für den Privatgebrauch stellen Sie über ein Netzworkkabel und einen **physischen Netzwerkadapter** eine Verbindung zum Internet her.

In diesem Beispiel müssen Sie die Unternehmenskonfiguration auf die virtuelle Unternehmensverbindung und die (in der Regel strengere) Konfiguration für unternehmensfremde Zwecke auf die physische Verbindung anwenden.

Hinweis: Die Konfiguration für unternehmensfremde Zwecke muss genügend Regeln umfassen, damit die virtuelle Unternehmenskonfiguration hergestellt werden kann.

7.2.2.5.2 Einrichtung der standortspezifischen Konfiguration

1. Erstellen Sie eine Liste von Gateway-MAC-Adressen oder Domännennamen Ihrer Primärstandorte. Hierbei handelt es sich in der Regel um Ihre Unternehmensnetzwerke.
2. Erstellen Sie die Firewallkonfiguration für Ihre Primärstandorte. Die Konfiguration ist in der Regel weniger restriktiv.
3. Erstellen Sie eine sekundäre Firewallkonfiguration. In der Regel ist diese Konfiguration restriktiver.
4. Wählen Sie die gewünschte Konfiguration aus.

Je nach verwendeter Erkennungsmethode bezieht die Firewall die DNS- oder Gateway-Adressen für alle Netzwerkadapter der Computer und stimmt diese im Anschluss mit der Adressliste ab.

- Wenn eine Adresse in der Liste mit der Adresse eines Netzwerkadapters übereinstimmt, wird dem Adapter die Konfiguration des **Primärstandorts** zugewiesen.
- Wenn keine Adresse in der Liste mit der Adresse eines Netzwerkadapters übereinstimmt, wird dem Adapter die Konfiguration des **Sekundärstandorts** zugewiesen.

Wichtig: Die sekundäre Konfiguration wechselt vom **interaktiven** Modus in den Modus **Standardmäßig sperren**, wenn die beiden folgenden Bedingungen erfüllt sind:

- Beide Standorte sind aktiv.
- Die primäre Konfiguration ist *nicht* interaktiv.

7.2.2.5.3 Festlegen der primären Standorte

1. Doppelklicken Sie auf die zu ändernde Firewall-Richtlinie.
2. Klicken Sie auf der **Startseite** des **Firewall-Richtlinienassistenten** auf **Erweiterte Einstellungen**.
3. Klicken Sie im Bereich **Konfigurationen** neben dem Standort, für den Sie die Firewall konfigurieren möchten, auf **Konfigurieren**.
4. Klicken Sie auf die Registerkarte **Standorterkenntung**.
5. Klicken Sie im Bereich **Erkennungsmethode** auf die Schaltfläche **Konfigurieren** neben der gewünschten Option:

Option	Beschreibung
DNS-Suche	Sie können eine Liste mit Domännennamen und erwarteten IP-Adressen erstellen, die Ihren primären Standorten entsprechen.
MAC-Adressenerkennung	Sie können eine Liste mit Gateway-MAC-Adressen erstellen, die Ihren primären Standorten entsprechen.

6. Befolgen Sie die Anweisungen auf dem Bildschirm.

7.2.2.5.4 Festlegen des sekundären Standorts

1. Doppelklicken Sie auf die zu ändernde Firewall-Richtlinie.
2. Klicken Sie auf der **Startseite** des **Firewall-Richtlinienassistenten** auf **Erweiterte Einstellungen**.
3. Klicken Sie im Bereich **Konfigurationen** neben dem Standort, für den Sie die Firewall konfigurieren möchten, auf **Konfigurieren**.
4. Aktivieren Sie das Kontrollkästchen **Konfiguration für einen sekundären Standort**.

Konfigurieren Sie den sekundären Standort. Anweisungen hierzu finden Sie im Abschnitt *Konfigurieren der Firewall*.



Vorsicht: Bei lokalen Netzwerkregeln in sekundären Konfigurationen ist Vorsicht geboten. Laptops, die außerhalb des Unternehmens eingesetzt werden, stellen unter Umständen eine Verbindung zu einem unbekanntem lokalen Netzwerk her. Wenn dies der Fall ist, wird aufgrund der Firewallregeln der sekundären Konfiguration, bei denen die Adresse das lokale Netzwerk ist, unter Umständen der gesamte unbekanntete Datenverkehr zugelassen.

7.2.2.5.5 Auswahl einer Konfiguration

1. Doppelklicken Sie auf die zu ändernde Firewall-Richtlinie.
2. Klicken Sie auf der **Startseite** des **Firewall-Richtlinienassistenten** auf **Erweiterte Einstellungen**.
3. Klicken Sie im Bereich **Konfigurationen** neben dem Standort, für den Sie die Firewall konfigurieren möchten, auf **Konfigurieren**.
4. Klicken Sie auf der Registerkarte **Allgemein** im Bereich **Standort** auf eine der folgenden Optionen:

Option	Beschreibung
Konfiguration des erkannten Standorts	Je nach Netzwerkverbindung weist die Firewall in Einklang mit den Erkennungseinstellungen der standortspezifischen Konfiguration immer die primäre oder die sekundäre Konfiguration zu (nähere Informationen hierzu finden Sie im Abschnitt <i>Einrichtung der standortspezifischen Konfiguration</i> (Seite 108)).
Konfiguration des primären Standorts	Die Firewall überträgt die primäre Konfiguration auf alle Netzwerkverbindungen.
Konfiguration des sekundären Standorts	Die Firewall überträgt die sekundäre Konfiguration auf alle Netzwerkverbindungen.

7.2.2.6 Firewall-Meldungen

7.2.2.6.1 Allgemeine Informationen

Standardmäßig meldet die Firewall auf dem Endpoint Änderungen, Ereignisse und Fehler an Enterprise Manager.

Firewall-Status-Änderungen

Als Statusänderungen gelten:

- Wechsel des Arbeitsmodus
- Änderungen an der Softwareversion
- Änderungen mit Bezug auf das Zulassen von Datenfluss in der Firewall
- Änderungen mit Bezug auf die Richtlinienkonformität der Firewall

Im interaktiven Modus kann die Firewall-Konfiguration von der Richtlinie für Enterprise Manager abweichen. Dies ist kein Zufall. In diesem Fall können Sie Alerts zu Abweichungen von der Richtlinie an Enterprise Manager bei Änderungen an der Firewall-Konfiguration **deaktivieren**.

Weitere Informationen finden Sie unter [Aktivieren/Deaktivieren der Meldungen über lokale Änderungen](#) (Seite 110).

Firewall-Ereignisse

Ein *Ereignis* findet statt, wenn das Betriebssystem oder eine unbekannt Anwendung auf dem Computer versucht, über eine Netzwerkverbindung mit einem anderen Computer zu kommunizieren.

Sie können Ereignismeldungen an Enterprise Manager deaktivieren.

Weitere Informationen finden Sie unter [Deaktivieren von Meldungen über unbekannt Datenbewegungen](#) (Seite 111).

7.2.2.6.2 Aktivieren/Deaktivieren der Meldungen über lokale Änderungen

Hinweis: Bei rollenbasierter Verwaltung müssen Sie zum Konfigurieren einer Firewall-Richtlinie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

Wenn die Firewall-Konfiguration von der Richtlinie abweicht, können Sie **Meldungen über lokale Änderungen deaktivieren**.

Wenn Sie die Meldungen über lokale Änderungen deaktivieren, sendet die Firewall nach Änderungen an globalen Regeln, Anwendungen, Prozessen oder Prüfsummen keine Alerts der Art „weicht von Richtlinie ab“ mehr an Enterprise Manager. Eine Deaktivierung empfiehlt sich z.B. für den interaktiven Modus, da sich diese Einstellungen durch Lernregeln jederzeit anpassen lassen.

Wenn die Firewall-Konfiguration richtlinienkonform sein soll, sollten Sie **Meldungen über lokale Änderungen aktivieren**.

So deaktivieren Sie Meldungen über lokale Änderungen:

1. Doppelklicken Sie auf die zu ändernde Firewall-Richtlinie.
2. Klicken Sie auf der **Startseite** des **Firewall-Richtlinienassistenten** auf **Erweiterte Einstellungen**.
3. Klicken Sie im Bereich **Konfigurationen** neben dem Standort, für den Sie die Firewall konfigurieren möchten, auf **Konfigurieren**.
4. Klicken Sie auf die Registerkarte **Allgemein**.

5. Wählen Sie im Bereich **Reports** eine der folgenden Funktionen aus:
 - Wenn lokale Änderungen gemeldet werden sollen, aktivieren Sie bitte das Kontrollkästchen **Lokal geänderte globale Regeln, Anwendungen, Prozesse und Prüfsummen an die Management-Konsole melden**.
 - Wenn lokale Änderungen nicht gemeldet werden sollen, deaktivieren Sie bitte das Kontrollkästchen **Lokal geänderte globale Regeln, Anwendungen, Prozesse und Prüfsummen an die Management-Konsole melden**.

7.2.2.6.3 Deaktivieren von Meldungen über unbekannte Datenbewegungen

Hinweis: Bei rollenbasierter Verwaltung müssen Sie zum Konfigurieren einer Firewall-Richtlinie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

Sie können festlegen, dass die Firewall auf den Endpoints unbekannte Datenbewegungen nicht an Enterprise Manager meldet. Datenbewegungen, die keinen Regeln entsprechen, werden von der Firewall als „unbekannt“ eingestuft.

So legen Sie fest, dass die Firewall auf den Endpoints unbekannte Datenbewegungen nicht an Enterprise Manager meldet.

1. Doppelklicken Sie auf die zu ändernde Firewall-Richtlinie.
2. Klicken Sie auf der **Startseite** des **Firewall-Richtlinienassistenten** auf **Erweiterte Einstellungen**.
3. Klicken Sie im Bereich **Konfigurationen** neben dem Standort, für den Sie die Firewall konfigurieren möchten, auf **Konfigurieren**.
4. Klicken Sie auf die Registerkarte **Allgemein**.
5. Aktivieren Sie im Bereich **Sperren** das Kontrollkästchen **Anwendungen anhand von Prüfsummen authentifizieren**.
6. Deaktivieren Sie unter **Reports** das Kontrollkästchen **Neue und geänderte Anwendungen an die Management-Konsole melden**.

7.2.2.6.4 Deaktivieren von Firewall-Fehlermeldungen

Wichtig: Wir raten davon ab, Firewall-Fehlermeldungen über einen längeren Zeitraum zu deaktivieren. Die Deaktivierung sollte sich auf den Bedarfsfall beschränken.

So verhindern Sie, dass die Firewall auf dem Endpoint Fehler an Enterprise Manager meldet:

1. Doppelklicken Sie auf die zu ändernde Firewall-Richtlinie.
2. Klicken Sie auf der **Startseite** des **Firewall-Richtlinienassistenten** auf **Erweiterte Einstellungen**.
3. Klicken Sie im Bereich **Konfigurationen** neben dem Standort, für den Sie die Firewall konfigurieren möchten, auf **Konfigurieren**.
4. Klicken Sie auf die Registerkarte **Allgemein**.
5. Deaktivieren Sie unter **Reports** das Kontrollkästchen **Fehler an die Management-Konsole melden**.

7.2.2.7 Importieren/Exportieren der Firewall-Konfiguration

Hinweis: Bei rollenbasierter Verwaltung müssen Sie zum Konfigurieren einer Firewall-Richtlinie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

Sie können allgemeine Firewall-Einstellungen und -Regeln als Konfigurationsdatei (*.conf) importieren oder exportieren. Diese Funktion umfasst folgende Optionen:

- Sichern und Wiederherstellen der Firewall-Konfiguration.
- Importieren von auf einem Computer erstellten Anwendungsregeln und Erstellen einer Richtlinie für andere Computer mit den gleichen Anwendungen auf der Basis der Anwendungsregeln.
- Kombination der Konfiguration unterschiedlicher Computer zur Erstellung einer für eine oder mehrere Computergruppen gültige Richtlinie.

Verfahren Sie zum Importieren/Exportieren der Firewall-Konfiguration wie folgt:

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 23).
2. Doppelklicken Sie im Feld **Richtlinien** auf **Firewall** und doppelklicken Sie anschließend auf die Richtlinie, die Sie importieren/exportieren möchten.
3. Klicken Sie auf der **Startseite** des **Firewall-Richtlinienassistenten** auf **Erweiterte Einstellungen**.
4. Klicken Sie im Dialogfeld **Firewall-Richtlinie** auf der Registerkarte **Allgemein** unter **Konfiguration verwalten** auf **Importieren** bzw. **Exportieren**.

7.3 Konfigurieren der Device Control-Richtlinie

7.3.1 Device Control

Wichtig: Es ist davon abzuraten, Sophos Device Control mit Gerätesteuersoftware 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 sich:

- 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 Enterprise Manager*.

Hinweis: Bei rollenbasierter Verwaltung müssen Sie zum Konfigurieren einer Device Control-Richtlinie über die Berechtigung **Richtlinieneinstellung – Device Control** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

7.3.2 Device Control-Ereignisse

Device Control-Ereignisse (z.B. Sperren eines Wechselsmediums) werden im Dialogfeld **Device Control – Ereignisanzeige** angezeigt und an Enterprise Manager gesendet.

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. Nähere Informationen hierzu finden Sie unter [Anzeige von Device Control-Ereignissen](#) (Seite 128) und [Exportieren der Ereignisliste in eine Datei](#) (Seite 131).

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 117) oder [Ausschließen eines Geräts von allen Richtlinien](#) (Seite 116) 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 36).

Zudem können Sie festlegen, dass die gewählten Empfänger über Device Control-Ereignisse benachrichtigt werden. Mehr dazu erfahren Sie unter [Einrichten von Device Control-Alerts und -Benachrichtigungen](#) (Seite 125).

7.3.3 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.

7.3.4 Auswählen von Geräten für Device Control

Bei rollenbasierter Verwaltung müssen Sie zum Bearbeiten einer Device Control-Richtlinie über die Berechtigung **Richtlinieneinstellung – Device Control** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

Wichtig: Sie sollten keine Drahtlosverbindungen auf Computern trennen, die auf diese Weise über Enterprise Manager 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 23).
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**.

7.3.5 Erkennen und Zulassen von Geräten

Bei rollenbasierter Verwaltung müssen Sie zum Bearbeiten einer Device Control-Richtlinie über die Berechtigung **Richtlinieneinstellung – Device Control** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

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 128).

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 23).
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 114).)
Klicken Sie auf **OK**.

7.3.6 Erkennen und Sperren von Geräten

Bei rollenbasierter Verwaltung müssen Sie zum Bearbeiten einer Device Control-Richtlinie über die Berechtigung **Richtlinieneinstellung – Device Control** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

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 23).
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 114).)
Klicken Sie auf **OK**.

7.3.7 Ausschließen eines Geräts von allen Richtlinien

Bei rollenbasierter Verwaltung müssen Sie zum Bearbeiten einer Device Control-Richtlinie über die Berechtigung **Richtlinieneinstellung – Device Control** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

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. Wählen Sie im Menü **Ansicht** die Option **Device Control-Ereignisse**.
Das Dialogfeld **Device Control – Ereignisanzeige** wird angezeigt.

2. Wenn nur ausgewählte Ereignisse angezeigt werden sollen, legen Sie im Feld **Suchkriterien** Filter fest und klicken Sie zur Anzeige der Ereignisse auf **Suchen**.
Weitere Informationen finden Sie unter [Anzeige von Device Control-Ereignissen](#) (Seite 128).
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**.

7.3.8 Ausschließen von Geräten von einer einzelnen Richtlinie

Bei rollenbasierter Verwaltung müssen Sie zum Bearbeiten einer Device Control-Richtlinie über die Berechtigung **Richtlinieneinstellung – Device Control** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

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 23).
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 128).
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**.

7.3.9 Anzeigen/Ändern der Liste der ausgeschlossenen Geräte

Bei rollenbasierter Verwaltung müssen Sie zum Bearbeiten einer Device Control-Richtlinie über die Berechtigung **Richtlinieneinstellung – Device Control** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

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 23).
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 117).

- 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.

7.4 Konfigurieren der Manipulationsschutz-Richtlinie

7.4.1 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. Weitere Informationen finden Sie unter [Die Antivirus- und HIPS-Richtlinie](#) (Seite 64).

Nach der Aktivierung des Manipulationsschutzes und der Erstellung eines Manipulationsschutz-Kennworts können Mitglieder der Gruppe SophosAdministrators folgende Aktionen nur unter Angabe des Kennworts vornehmen:

- Erneute Konfiguration der Einstellungen von On-Access-Scans bzw. der Erkennung verdächtigen Verhaltens in Sophos Endpoint Security and Control.
- 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 möchten, dass SophosAdministrators diese Aufgaben ausführen können, müssen Sie den Administratoren das Manipulationsschutz-Kennwort zur Authentifizierung geben.

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 müssen Sie zum Konfigurieren einer Manipulationsschutz-Richtlinie über die Berechtigung **Richtlinieneinstellung – Manipulationsschutz** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

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 Manager angezeigt werden. Mehr dazu erfahren Sie unter [Anzeige von Manipulationsschutz-Ereignissen](#) (Seite 130).

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).

7.4.2 Aktivieren/Deaktivieren des Manipulationsschutzes

Bei rollenbasierter Verwaltung müssen Sie zum Konfigurieren einer Manipulationsschutz-Richtlinie über die Berechtigung **Richtlinieneinstellung – Manipulationsschutz** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

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 23).
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.

7.4.3 Ändern des Manipulationsschutz-Kennworts

Bei rollenbasierter Verwaltung müssen Sie zum Konfigurieren einer Manipulationsschutz-Richtlinie über die Berechtigung **Richtlinieneinstellung – Manipulationsschutz** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

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 23).

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 in das Feld **Manipulationsschutz-Kennwort** ein Kennwort ein und bestätigen Sie es.

Tipp: Das Kennwort sollte mindestens 8 Zeichen umfassen und sich aus Buchstaben und Zahlen zusammensetzen.

8 Einrichten von Alerts und Benachrichtigungen

8.1 Was sind Alerts und Benachrichtigungen?

In Enterprise Manager 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 Manager. Der Alert wird in der Computerliste angezeigt. Nähere Informationen zum Umgang mit solchen Alerts können Sie dem Abschnitt [Umgang mit Alerts zu erkannten Objekten](#) (Seite 40) entnehmen.

Diese Alerts werden immer angezeigt. Sie müssen nicht eingerichtet werden.

■ In der Konsole angezeigte Ereignisse

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

■ Von der Konsole an die ausgewählten Empfänger gesendete Alerts und Benachrichtigungen

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 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.

8.2 Einrichten von Softwareabonnements-Alerts

Bei rollenbasierter Verwaltung müssen Sie hierzu über die Berechtigung **Systemkonfiguration** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

Update Manager-Alerts werden in Enterprise Manager in der Spalte **Alerts** in der Ansicht **Update Manager** angezeigt.

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** unter „Software-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.

8.3 Einrichten von Antivirus- und HIPS-E-Mail-Benachrichtigungen

Bei rollenbasierter Verwaltung müssen Sie hierzu über die Berechtigung **Richtlinieneinstellung – Antivirus und HIPS** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

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 in das 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-Computer ignorieren SMTP-Sender- und Antworten an-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.

8.4 Einrichten von Antivirus- und HIPS-SNMP-Benachrichtigungen

Bei rollenbasierter Verwaltung müssen Sie hierzu über die Berechtigung **Richtlinieneinstellung – Antivirus und HIPS** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

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.

8.5 Konfigurieren von Antivirus- und HIPS-Desktop-Benachrichtigungen

Bei rollenbasierter Verwaltung müssen Sie hierzu über die Berechtigung **Richtlinieneinstellung – Antivirus und HIPS** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

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.

8.6 Einrichten von Device Control-Alerts und -Benachrichtigungen

Bei rollenbasierter Verwaltung müssen Sie zum Bearbeiten einer Device Control-Richtlinie über die Berechtigung **Richtlinieneinstellung – Device Control** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

Enterprise Manager meldet erkannte bzw. gesperrte Geräte über Alarme und Benachrichtigungen.

Nähere Informationen zu Device Control-Richtlinien und -ereignissen finden Sie im Abschnitt [Device Control](#) (Seite 112).

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 Manager 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.

Sie können in Enterprise Manager auch folgende Benachrichtigungen konfigurieren:

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-Benachrichtigungen 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 23).
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.

Sie können maximal 100 Zeichen eingeben. Sie können auch einen HTML-Link in die Nachricht aufnehmen, z.B. `Über Sophos`.
 - *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.

8.7 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 [Informationen zu Rollen](#) (Seite 15).

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.

8.8 Konfigurieren des Windows-Ereignisprotokolls

Bei rollenbasierter Verwaltung müssen Sie hierzu über die Berechtigung **Richtlinieneinstellung – Antivirus und HIPS** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

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.

8.9 Ereignisanzeige

8.9.1 Allgemeine Informationen

Firewall-, Device Control- oder Manipulationsschutz-Ereignisse auf einem Endpoint (z.B. die Firewall hat eine Anwendung blockiert) werden an Enterprise Manager 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 Device 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 36).

Sie können einstellen, dass die von Ihnen ausgewählten Empfänger bei Ereignissen benachrichtigt werden. Weitere Informationen finden Sie unter [Was sind Alerts und Benachrichtigungen?](#) (Seite 122).

8.9.2 Anzeige von Device Control-Ereignissen

So können Sie sich Device Control-Ereignisse anzeigen lassen:

1. Wählen Sie im Menü **Ansicht** die Option **Device Control-Ereignisse**.
Das Dialogfeld **Device 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 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 116).

Sie können die Liste von Device Control-Ereignissen in eine Datei exportieren. Mehr dazu erfahren Sie unter [Exportieren der Ereignisliste in eine Datei](#) (Seite 131).

8.9.3 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-Ereignisregel](#) (Seite 87) 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 131).

8.9.4 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-Ereignisse 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 131).

8.9.5 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 139).

8.9.6 Exportieren der Ereignisliste in eine Datei

Sie können Firewall-, Device Control- oder Manipulationsschutz-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 [Anzeige von Device Control-Ereignissen](#) (Seite 128), [Anzeige von Firewall-Ereignissen](#) (Seite 129) und [Anzeige von Manipulationsschutz-Ereignissen](#) (Seite 130).

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

9 Erstellen von Reports

9.1 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 [Informationen zu Rollen](#) (Seite 15) entnehmen.

9.2 Erstellen eines neuen Reports

Bei rollenbasierter Administration müssen Sie hierzu über die Berechtigung **Report-Konfiguration** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

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.

9.3 Konfigurieren des Reports „Alert- und Ereignisverlauf“

Bei rollenbasierter Administration müssen Sie hierzu über die Berechtigung **Report-Konfiguration** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

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 **Einzubehaltende 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 **Anzeigeoptionen** 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.

9.4 Konfigurieren des Reports „Alert-Übersicht“

Bei rollenbasierter Administration müssen Sie hierzu über die Berechtigung **Report-Konfiguration** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

Der Report **Alert-Übersicht** liefert statistische Informationen über den allgemeinen Netzwerkzustand.

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 **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 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.

9.5 Konfigurieren des Reports „Alerts und Ereignisse nach Objektname“

Bei rollenbasierter Administration müssen Sie hierzu über die Berechtigung **Report-Konfiguration** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

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.

9.6 Konfigurieren des Reports „Alerts und Ereignisse nach Zeit“

Bei rollenbasierter Administration müssen Sie hierzu über die Berechtigung **Report-Konfiguration** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

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.

9.7 Konfigurieren des Reports „Alerts und Ereignisse nach Ort“

Bei rollenbasierter Administration müssen Sie hierzu über die Berechtigung **Report-Konfiguration** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

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.

9.8 Konfigurieren des Reports „Endpoint-Richtlinienabweichung“

Bei rollenbasierter Administration müssen Sie hierzu über die Berechtigung **Report-Konfiguration** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

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.

9.9 Konfigurieren des Reports „Ereignisse nach Benutzer“

Bei rollenbasierter Administration müssen Sie hierzu über die Berechtigung **Report-Konfiguration** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

Im Report **Ereignisse nach Benutzer** werden Firewall-, 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.

9.10 Konfigurieren des Reports „Schutz verwalteter Endpoints“

Bei rollenbasierter Administration müssen Sie hierzu über die Berechtigung **Report-Konfiguration** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

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.

9.11 Update-Hierarchie-Reports

Im **Update-Hierarchie**-Report werden der 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 141) durchführen.

9.12 Report-Zeitpläne

Bei rollenbasierter Administration müssen Sie hierzu über die Berechtigung **Report-Konfiguration** verfügen. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

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.

9.13 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.

9.14 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.

9.15 Drucken von Reports

Klicken Sie zum Drucken eines Reports auf das **Drucker**-Symbol in der Symbolleiste im oberen Bereich des Reports.



9.16 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 auf **OK**.

9.17 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 auf **OK**.

Der Report wird im gewählten Format angezeigt.

Das Format wird auch beim Drucken oder Exportieren von Reports übernommen.

10 Kopieren und Drucken von Daten mit Enterprise Manager

10.1 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.

10.2 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**.

10.3 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.

10.4 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**.

11 Fehlersuche

11.1 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 23).
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 73) und [Durchsetzen von Gruppenrichtlinien](#) (Seite 27).

11.2 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 23).
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 87) und [Durchsetzen von Gruppenrichtlinien](#) (Seite 27).

11.3 Firewall nicht installiert

Hinweis: Bei rollenbasierter Verwaltung ist zur Installation der Firewall die Berechtigung **Computersuche, -schutz und -gruppen** erforderlich. Weitere Informationen finden Sie unter [Informationen zu Rollen](#) (Seite 15).

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.

11.4 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 44).
- 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 70).
- Bei nicht aktuellen Computern finden Sie im Abschnitt [Updates nicht aktueller Computer](#) (Seite 62) Anweisungen zur Fehlersuche und Problembhebung.

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.

11.5 Computer werden nicht von der Konsole verwaltet

Computer sollten von Enterprise Manager verwaltet werden, damit sie upgedatet und überwacht werden können.

Hinweis: Neue Computer werden 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 Manager nicht automatisch installieren kann, eine manuelle Installation durch.

Nähere Anweisungen entnehmen Sie bitte der Erweiterten *Startup-Anleitung* zu *Sophos Enterprise Manager*.

11.6 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.

11.7 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 Manager konnte das Betriebssystem der Computer nicht ermitteln. Sie haben wahrscheinlich beim Suchen von Computern Ihren Benutzernamen nicht im Format „Domäne\Benutzer“ eingegeben.
- Auf dem Betriebssystem ist eine automatische Installation nicht möglich. Führen Sie eine manuelle Installation durch. Nähere Anweisungen entnehmen Sie bitte der *Erweiterten Startup-Anleitung* zu Sophos Enterprise Manager.
- 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>.

11.8 Computer werden nicht upgedatet

Im Abschnitt *Updaten nicht aktueller Computer* (Seite 62) finden Sie Hinweise zur Fehlersuche und Problembeseitigung.

11.9 Fehler beim Erstellen einer neuen Update-Richtlinie

Wenn die Optionen **Richtlinie erstellen** und **Richtlinie kopieren** deaktiviert sind, haben Sie bereits so viele Richtlinien wie möglich erstellt. Je Richtlinientyp können Sie jeweils maximal vier neue Richtlinien erstellen (vier neue Update-Richtlinien, vier neue Antivirus- und HIPS-Richtlinien usw.).

11.10 Virenschutzeinstellungen werden von Macintosh-Computern 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. Um den Sophos Update Manager auf einem Mac-Computer zu öffnen, suchen Sie in

einem **Finder**-Fenster nach dem Ordner „Sophos Anti-Virus:ESOSX“. Doppelklicken Sie auf **Sophos Update Manager**. Weitere Details werden in der Hilfe zu Sophos Update Manager aufgeführt.

11.11 Virenschutzeinstellungen werden von Linux nicht übernommen

Manche Virenschutzeinstellungen können von Linux-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.

11.12 Linux-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.

11.13 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.

11.14 Verbindungs- und Zeitüberschreitungsprobleme

Wenn die Kommunikation zwischen Enterprise Manager 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 Manager bietet. 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.

11.15 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 69).
- Anwendungen werden auf einem Computer unter Windows 2000 oder höher ausgeführt.

11.16 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 69).

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 73)). 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.

11.17 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 einen 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 70).
- Bereinigen Sie die Computer, indem Sie Anwendungen entfernen, die Sie nicht zugelassen haben. Mehr dazu erfahren Sie unter [Sofortiges Bereinigen von Computern](#) (Seite 44).

11.18 Bereinigung fehlgeschlagen

Wenn Endpoint Security and Control Objekte nicht bereinigen kann („Bereinigung fehlgeschlagen“), kann es dafür folgenden Grund geben:

- Das Programm 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 43).
- 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 73). Wenn sich Objekte in der Liste befinden, entfernen Sie diese.
- Sie haben keine ausreichenden Zugriffsrechte.
- Die Software kann diese Objektart nicht bereinigen.
- Sophos Anti-Virus hat ein Virenfragment anstelle einer genauen Virenübereinstimmung entdeckt.
- Das Objekt befindet sich auf einer schreibgeschützten Diskette oder CD.
- Das Objekt befindet sich auf einem schreibgeschützten NTFS-Volume (Windows 2000 oder höher).

11.19 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 **Sicherheitsinformationen**. 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 der Infektion keine Sicherungskopien hatten, 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 Problembeseitigung behilflich sein.

11.20 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 **Sicherheitsinformationen**. 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.

12 Glossar

Application Manager	In diesem Fenster lassen sich neue Regeln für von Sophos Client Firewall gesperrte Anwendungen erstellen.
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.
Datenbanken	Komponente von Sophos Enterprise Manager, 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.
Erkennung verdächtigen Verhaltens	Dynamische Analyse des Verhaltens aller auf einem System ausgeführten Programme. Bei Erkennung von Schadenspotenzial wird das jeweilige Programm an der Ausführung gehindert.
Geräte-Ausschluss	Ein von der Funktion „Device Control“ nicht zu berücksichtigendes Gerät.
Gruppe	Gruppe von Sophos Enterprise Manager verwalteter Computer.
Host Intrusion Prevention System (HIPS)	Sicherheitsverfahren, das Computer vor verdächtigen Dateien, unbekanntem Viren und verdächtigem Verhalten schützt.
Kritische Stufe	Dieser Wert ändert den Sicherheitsstatus eines Objekts in „kritisch“.
Management-Konsole	Die Komponente von Sophos Enterprise Manager zur Verwaltung und zum Schutz von Computern.
Management-Server	Die Komponente von Sophos Enterprise Manager 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.
Potenziell unerwünschte Anwendung (PUA)	Ein Programm, das an sich nicht schädlich ist, generell aber für die meisten Unternehmensnetzwerke als nicht geeignet angesehen wird.
Recht	Ein Satz von Berechtigungen zum Ausführen bestimmter Aufgaben über Enterprise Manager.
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 Manager.
Rollenbasierte Verwaltung	Verteilung von Zugriffsrechten auf bestimmte Computer und Prozesse basierend auf der Rolle eines Benutzers im Unternehmen.
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 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 Bereinigungskonfiguration von Sophos Anti-Virus festgelegten Maßnahmen ergriffen.
Sophos Update Manager (SUM)	Programm zum Download von Sophos Sicherheitssoftware und Updates von Sophos oder einem anderen Update-Server in freigegebene Update-Verzeichnisse.
Statusanzeige	Oberbegriff für Symbole, die den Sicherheitszustand eines Dashboards-Objekts oder der Netzwerkintegrität darstellen.
Systemadministrator	Eine vorkonfigurierte Rolle für die Verwaltung von Sophos Sicherheitssoftware im Netzwerk und Rollen in Enterprise Manager. 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.
Update Manager	Siehe unter „Sophos Update Manager“.

Veralteter Computer	Computer mit Sophos Software, die nicht mehr auf dem neuesten Stand ist.
Verdächtige Datei	Datei, die zwar für Viren typische Merkmale aufweist, jedoch nicht schädlich sein muss, da diese Merkmale auch in harmlosen Programmen auftreten können.
Verwalteter Computer	Computer mit Remote Management System (RMS), auf dem über Sophos Enterprise Manager Software installiert und aktualisiert werden kann und Berichte erstellt werden können.
Warnstufe	Wert, der die Sicherheitsstufe eines Objekts in „Warnung“ ändert.

13 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.

14 Rechtlicher Hinweis

Copyright © 2011 Sophos Limited. Alle Rechte vorbehalten. Diese Publikation darf weder elektronisch oder mechanisch reproduziert, elektronisch gespeichert oder übertragen, noch fotokopiert oder aufgenommen werden, es sei denn, Sie verfügen entweder über eine gültige Lizenz, gemäß der die Dokumentation in Übereinstimmung mit dem Lizenzvertrag reproduziert werden darf, oder Sie verfügen über eine schriftliche Genehmigung des Urheberrechtsinhabers.

Sophos und Sophos Anti-Virus sind eingetragene Warenzeichen der Sophos Limited. Alle anderen erwähnten Produkt- und Unternehmensnamen sind Marken oder eingetragene Marken 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 us¹⁰ know so we can promote your project in the DOC software success stories¹¹.

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 companies¹² 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 ACE¹³, TAO¹⁴, CIAO¹⁵, and CoSMIC¹⁶ web sites are maintained by the DOC Group¹⁷ at the Institute for Software Integrated Systems (ISIS)¹⁸ and the Center for Distributed Object Computing of Washington University, St. Louis¹⁹ for the development of open-source software as part of the open-source software community²⁰. 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 me²¹ know.

Douglas C. Schmidt²²

Quellen

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

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 122
- Abonnements 55
 - Auswahl 57
 - Hinzufügen 55
- Abonnieren von Software 55
- Active Directory
 - Importieren aus 28
- Adware 69
- Adware/PUA
 - Zulassen 70
- Aktivieren
 - Web-Schutz 71
- Alert-Symbole 39
- Alerts 39, 122
 - Abonnements 122
 - Beheben 40
 - E-Mail 123
 - Informationen zu erkannten Objekten 42
 - Löschen 42
 - Netzwerkstatus 126
 - Umgang mit 40
 - Update Manager 42
- alternative Update-Quelle 58
- Ändern von Rollen 16
- Anti-Virus 64
- Antivirus- und HIPS-Richtlinie 64
- Antivirus-Benachrichtigungen
 - Desktop 125
 - SNMP 124
- Anwendungen
 - Hinzufügen 84, 90
 - Sperren 92
 - Zulassen 84, 89, 91–92
- Arbeitsmodus, Wechsel in den interaktiven Modus 88
- Archivdateien 78
- Assistent zum Schützen von Computern
 - Funktionsauswahl 34
 - Zugangsdaten 34
- Ausschlüsse 80
 - geplante Scans 75
 - On-Access-Scans 73
- Auswahl der Software 50
- Auswahl von Abonnements 57

- automatische Bereinigung 45
- automatische Desinfektion 45
- automatische Updates 57

B

- Bandbreite
 - Verringern 58–59
- Bearbeiten von Richtlinien 26
- Beheben von Alerts
 - Bereinigungsstatus 40
 - Informationen zu erkannten Objekten 42
 - zu ergreifende Maßnahmen 40, 42
- Benachrichtigung 122
 - Desktop 125
 - SNMP 124
- Benutzeroberfläche 4–5
 - Endpoint-Ansicht 9
 - Update Manager-Ansicht 11
- Benutzerrollen
 - Anzeigen 16
- Berechtigungen 16
- Bereinigung 40, 44
 - automatisch 45
 - fehlgeschlagen 151
 - manuell 45
- Bereinigungsstatus 40
- Bereitstellung von Software 50
- Bootstrap-Verzeichnisse 35

C

- Computer mit aktuellem Schutz
 - Überprüfen 38
- Computer mit Problemen 38
- Computer-Details
 - Drucken 145
 - Kopieren 144
- Computerliste
 - Drucken von Daten 144
 - Kopieren von Daten 144
- Computersuche 28
 - Active Directory 28

D

- Dashboard
 - Bereiche 6
 - Konfigurieren 36
 - Sicherheitsstatussymbole 8

- Datei- und Druckerfreigabe 86
 - Zulassen 85
 - Datei- und Druckerfreigabe, Sperren 86
 - Datei, freigeben 86
 - Dateifreigabe, sperren 86
 - Datenverkehr im LAN, Zulassen 85
 - Desinfektion 44
 - automatisch 45
 - manuell 45
 - Desktop-Benachrichtigung 125
 - Device Control
 - Ausschließen eines Geräts von allen Richtlinien 116
 - Ausschließen von Geräten von einer Richtlinie 117
 - Auswahl der Gerätearten 114
 - Benachrichtigung 125
 - Controlled Devices 113
 - Ereignisse 113, 128
 - Erkennen und Sperren von Geräten 116
 - Erkennen und Zulassen von Geräten 115
 - Liste der ausgeschlossenen Geräte 118
 - Sperren von Geräten 116
 - Sperren von Netzwerkbrücken 113
 - Überblick 112
 - Drucken
 - Computer-Details 145
 - Computerlistendaten 144
 - Drucken von Reports 142
 - Drucker, freigeben 86
 - Druckerfreigabe, Sperren 86
- E**
- E-Mail-Benachrichtigungen
 - Antivirus und HIPS 123
 - Netzwerkstatus 126
 - Einrichten globaler Regeln 101, 103, 107
 - Endpoint-Ansicht 9
 - Drucken von Daten 144
 - Kopieren von Daten 144
 - Entfernen von Computern aus Gruppen 21
 - Ereignisprotokoll 127
 - Ereignisse 128
 - Device Control 128
 - Exportieren in eine Datei 131
 - Firewall 129
 - Manipulationsschutz 130
 - Erstellen von Gruppen 20
 - Erstellen von Reports 132, 141
 - Erstellen von Richtlinien 25
 - Erstinstallationsquelle 61
 - Erweiterungen 76
 - Exportieren von Reports 142
- F**
- Fehler
 - Löschen 42
 - Fehlersuche
 - ausstehende Alerts 147
 - Bereinigung 151
 - Fehler beim Erstellen einer neuen Update-Richtlinie 148
 - Firewall deaktiviert 146
 - Firewall nicht installiert 146
 - Gruppe „Nicht zugewiesen“ 147
 - Linux 149
 - Mac 148
 - Nicht aktuelle Computer 148
 - Nicht verwaltete Computer 147
 - Objekt zum Teil erkannt 150
 - On-Access-Scans 146
 - Option zum Duplizieren von Richtlinien deaktiviert 148
 - Option zum Duplizieren von Richtlinien deaktiviert nicht hinterlegt 148
 - Option zur Richtlinienerstellung deaktiviert 148
 - Option zur Richtlinienerstellung deaktiviert nicht hinterlegt 148
 - PUA, Folgeerscheinungen 152
 - PUA, Hohe Alert-Anzahl 150
 - PUA, nicht erkannt 150
 - Sophos Endpoint Security and Control:Installationsproblem 148
 - Verbindungsprobleme 149
 - Virus, Folgeerscheinung 151
 - Windows 2000 und höher 149
 - Zeitüberschreitung 149
 - fehlgeschlagene Bereinigung 151
 - Festlegen der primären Standorte 108
 - Filtern von ICMP-Meldungen 96
 - Firewall
 - Aktivieren 87
 - Deaktivieren 87
 - Einrichten 81
 - Ereignisse 129
 - Erstellen einer Regel 87, 104
 - erweiterte Konfiguration 88

Firewall (*Fortsetzung*)
Erweiterte Optionen 88
Hinzufügen von Anwendungen 84, 90
Hinzufügen von Prüfsummen 95
Zulassen der Datei- und Druckerfreigabe 85
Zulassen von Anwendungen 84, 89, 91–92
Firewall-Konfiguration
Exportieren 112
Importieren 112
Freigeben von Sicherheitssoftware in einem
Webserver 54

G

geplante Scans 74–75
Ausschließen von Objekten 75
geschützte Computer 36–37
geschütztes Netzwerk 36
Globale Regeln
Einstellung 101, 103, 107
Glossar 153
Gruppe „Nicht zugewiesen“ 20, 147
Gruppen 20
Entfernen von Computern 21
Erstellen 20
Gruppe „Nicht zugewiesen“ 20
Hinzufügen von Computern 21
Importieren aus Active Directory 28
Löschen 22
Umbenennen 22
Verschieben 22
verwendete Richtlinien 23

H

Hinzufügen einer Regel 102–103
Hinzufügen von Anwendungen 84, 90
Hinzufügen von Computern 28
Hinzufügen von Computern zu Gruppen 21
HIPS 64–65
HIPS-Benachrichtigungen
Desktop 125
E-Mail 123
SNMP 124
Host Intrusion Prevention System 65

I

ICMP-Meldungen
Erläuterung 97

ICMP-Meldungen (*Fortsetzung*)
Filtern 96
Importieren von Computern
aus einer Datei 30
In-the-Cloud-Technologie 68
Installationsproblem
Sophos Endpoint Security and Control 148
interaktiver Modus, Aktivieren 88
interaktiver Modus, allgemeine Informationen 88

J

Jetzt scannen 43

K

Konfiguration, Anwenden 109
Konfigurieren
zentrale Reports 109
Richtlinien 24
Konfigurieren des Dashboards 36
Konfigurieren des Update Managers 48
Konsolen-Zugriff 19
Kopieren
Computer-Details 144
Computerlistendaten 144

L

Laufzeitverhaltensanalyse 65
Löschen einer Gruppe 22
Löschen von Alerts 42
Löschen von Fehlern 42
Löschen von Richtlinien 27

M

Mac-Viren 77
Macintosh-Dateien
Scannen 77
Macintosh-Viren 77
Manipulationsschutz
Aktivieren 120
Ausschalten 120
Deaktivieren 120
Einschalten 120
Ereignisse 119, 130
Kennwortänderung 120
Überblick 119
Manuelle Bereinigung 45

Manuelle Desinfektion 45
manuelle Updates 62

N

Netzwerkfreigaben
unterstützt 51
Netzwerkstatus-Benachrichtigungen 126
neuer Anwender 19
Nicht aktuelle Computer 148
Auffinden 38
Updates 62
nicht interaktiver Modus, Wechsel in den 89
Nicht verwaltete Computer 147
Nutzungsstatistik 56

O

Objekt zum Teil erkannt 150
On-Access-Scans
Aktivieren 73
Ausschließen von Objekten 73
Beim Lesen 72
Beim Schreiben 72
Beim Umbenennen 72
Bereinigung 45
Deaktivieren 73
Einschalten 73

P

potenziell unerwünschte Anwendungen 69
Primärserver 58
Ändern der Zugangsdaten 59
Priorität, Scans 80
Prüfsummen 95
PUA 69
Folgeerscheinungen 152
Hohe Alert-Anzahl 150
nicht erkannt 150
Pufferüberlauf 65

R

Raw-Sockets, Zulassen 94
Regel
Hinzufügen 102–103
Regelpriorität 98
Removal Tool
Fremdsoftware 33

Removal-Tool (zur Entfernung von Fremdsoftware)
33

Report-Zeitpläne erstellen 141

Reports

Alert- und Ereignisverlauf 133
Alert-Übersicht 134
Alerts und Ereignisse nach Objektname 135
Alerts und Ereignisse nach Ort 137
Alerts und Ereignisse nach Zeit 136
Ausführen 141
Darstellung als Tabelle 142
Drucken 142
Endpoint-Richtlinienabweichung 138
Endpoint-Schutz nach Zeit 140
Ereignisse nach Benutzer 139
Erstellen 132
Exportieren 142
Layout 143
Richtlinienabweichung nach Uhrzeit 138
Schutz verwalteter Endpoints 140
Überblick 132
Update-Hierarchie 141
Zeitpläne 141

Richtlinien

Antivirus und HIPS 64
Bearbeiten 26
Durchsetzen 27
Erstellen 25
Konfigurieren 24
Löschen 27
Standard 24
Überblick 23
Überprüfen 27
Übertragen 22, 26
Umbenennen 26
zugehörige Gruppen 27
Zuweisen 22, 26

Rollen

Ändern 16
Bearbeiten 16
Hinzufügen von Benutzern oder Gruppen zu
16
vordefiniert 15

Rootkits

Scannen auf 78

S

Scan-Objekte 76
Scannen mit niedriger Priorität 80

- Scannen von Computern 43
 - sofort 43
 - Scans
 - Ausschlüsse 80
 - geplant 75
 - Schaltflächen der Symbolleiste 5
 - Schutz, Überprüfen 36
 - Schützen von Computern
 - Assistent zum Schützen von Computern 34
 - Funktionsauswahl 34
 - Voraussetzungen 32
 - Vorbereiten der Installation 32
 - Zugangsdaten 34
 - sekundäre Konfiguration, Erstellen 109
 - Sekundärserver 58–59
 - Setup 13
 - SNMP-Benachrichtigungen 124
 - Sofort-Scan 43
 - Sofort-Updates 62
 - Software
 - Abonnieren von Sicherheitssoftware 55
 - Auswahl 50
 - Sophos Endpoint Security and Control
 - Installationsproblem 148
 - Sophos Enterprise Manager 3
 - Sophos Live-Schutz
 - Aktivieren 68
 - Ausschalten 68
 - Deaktivieren 68
 - Einschalten 68
 - In-the-Cloud-Technologie 68
 - Überblick 68
 - Sophos Update Manager 48
 - Sortieren der Computer-Liste
 - Computer mit Problemen 38
 - Ungeschützte Computer 38
 - Sperren
 - Anwendungen 92
 - Datei- und Druckerfreigabe 86
 - Spyware 64
 - Standardeinstellungen globaler Regeln
 - nähere Informationen 99
 - Standort-Roaming 58
 - standortspezifische Konfiguration
 - Einrichten 108
 - Informationen 107
 - mit zwei Netzwerkadaptern 107
 - Suchen nach Computern
 - im Netzwerk 29
 - Importieren aus einer Datei 30
 - Suchen nach Computern (*Fortsetzung*)
 - in einem IP-Bereich 30
 - mit Active Directory 29
 - Symbole 10
 - Systemspeicher scannen 79
- ## T
- Trojaner 64
- ## U
- Übertragen von Richtlinien 22, 26
 - Überwachungsmodus 83
 - Umbenennen von Gruppen 22
 - Umbenennen von Richtlinien 26
 - Umgang mit Alerts 40
 - Ungeschützte Computer 38
 - unterstützte Netzwerkfreigaben 51
 - Update Manager 48
 - Alerts 42
 - Anzeige der Konfiguration 48
 - Auswahl einer Update-Quelle 49
 - Bereitstellung von Software 50
 - Konfigurieren 48
 - Protokollierung 53
 - Selbst-Updates 53
 - Übernahme der Konfigurationseinstellungen 54
 - Übersicht 54
 - unterstützte Netzwerkfreigaben 51
 - Updates 53
 - Zeitpläne 52
 - Update Manager-Ansicht 11
 - Update-Quelle 49
 - alternativ 58
 - primär 58
 - sekundär 58–59
 - Web-Server 54
 - Update-Server 48
 - Update-Zeitplan 52
 - Updates
 - automatisch 57
 - Bandbreite verringern 58–59
 - Erstinstallationsquelle 61
 - Freigeben von Sicherheitssoftware in einem Webserver 54
 - manuell 62
 - Nicht aktuelle Computer 62
 - Primäre Update-Quelle 58

Updates (*Fortsetzung*)

- Primärserver 58
- Protokollierung 61
- Proxy-Details 58–59
- Sekundäre Update-Quelle 58–59
- Sekundärserver 58–59
- sofort 62
- Standort-Roaming 58
- Zeitpläne 60

V

- Verbindungsprobleme 149
- verdächtige Dateien 66
- verdächtige Objekte
 - vorzeitig zulassen 67
 - Zulassen 67
- verdächtiges Verhalten
 - Erkennen 65
 - Sperren 65
- Versteckte Prozesse, Zulassen 93
- verwaltete Computer 10
- Viren 64
- Viren-Alerts
 - E-Mail 123
- Virus
 - Folgeerscheinungen 151
- Vollständige Systemüberprüfung 43
- vom Netzwerk getrennte Computer 10
- Vorbereitung 13
- vordefinierte Rollen 15
- vorzeitig zulassen
 - verdächtige Objekte 67

vorzeitig zulassen (*Fortsetzung*)

- Website 72

W

- Warnsymbole 10
- Web-Schutz 71
- Website
 - vorzeitig zulassen 72
 - Zulassen 72
- Würmer 64

Z

- Zeitplan für Updates 60
- Zeitüberschreitung 149
- zentrale Reports, Konfigurieren 109
- Zugriff auf Konsole 19
- Zulassen
 - Adware/PUA 70
 - Datei- und Druckerfreigabe 86
 - Datenverkehr im LAN 85
 - Raw-Sockets 94
 - verdächtige Objekte 67
 - Versteckte Prozesse 93
 - Website 72
- Zulassen der Datei- und Druckerfreigabe 85
- Zulassen von Anwendungen 84, 89, 91–92
- Zuweisen von Richtlinien 22, 26
- zwei Netzwerkadapter
 - Verwenden 107
- zwei Standorte 81, 107