

# SOPHOS

## Sophos Endpoint Security and Control Hilfe

Produktversion: 9.5  
Stand: Juni 2010



# Inhalt

1	Sophos Endpoint Security and Control .....	3
2	Die Startseite.....	4
3	Sophos Gruppen.....	5
4	Sophos Anti-Virus.....	8
5	Sophos Device Control.....	44
6	Sophos Data Control.....	46
7	Sophos Client Firewall.....	48
8	Sophos AutoUpdate.....	75
9	Sophos Manipulationsschutz.....	78
10	Fehlerbehebung.....	84
11	Glossar.....	92
12	Technischer Support.....	98
13	Rechtlicher Hinweis.....	99

# 1 Sophos Endpoint Security and Control

Sophos Endpoint Security and Control 9.5 ist eine integrierte Sicherheitssoftware-Suite.

**Sophos Anti-Virus** erkennt und bereinigt Viren, Trojaner, Würmer, Spyware, Adware und andere potenziell unerwünschte Anwendungen. Die HIPS-Technologie (Host Intrusion Prevention System) schützt den Computer vor verdächtigen Dateien, Rootkits, unbekanntem Viren und verdächtigem Verhalten. Außerdem werden Sie vor Bedrohungen geschützt, die von schädlichen und infizierten Websites ausgehen. Dank Sophos Live-Schutz lässt sich über ein "In-the-Cloud"-Verfahren sofort feststellen, ob eine Datei eine Bedrohung darstellt. Die Malware-Erkennung wird hierdurch erheblich verbessert, und es kommt nicht zu unerwünschten Erkennungen.

**Sophos Application Control** sperrt nicht zugelassene Anwendungen wie VoIP, Instant Messaging-Programme, File Sharing-Software und Spiele-Software.

**Sophos AutoUpdate** bietet sichere Updates. Zudem kann die Bandbreite bei langsamen Netzwerkverbindungen gedrosselt werden.

**Sophos Client Firewall** verhindert, dass sensible Daten über Würmer, Trojaner und Spyware entwendet werden und beugt zudem Hacker-Übergriffen vor.

**Sophos Data Control** schützt vor ungewollten Verlusten personenbezogener Daten auf verwalteten Computern.

**Sophos Device Control** sperrt nicht zugelassene externe Speichermedien und Wireless-Verbindungstechnik.

**Sophos Manipulationsschutz** verhindert, 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.

## 2 Die Startseite

Die **Startseite** wird beim Öffnen von **Sophos Endpoint Security and Control** im rechten Fensterbereich angezeigt. Über die Startseite können Sie die Software konfigurieren und verwenden.

Je nachdem, welche Aktion Sie mit Sophos Endpoint Security and Control ausführen, wird in diesem Bereich ein anderer Inhalt angezeigt. Durch Klicken auf die Schaltfläche **Start** in der Symbolleiste gelangen Sie wieder zur **Startseite**.

## 3 Sophos Gruppen

### 3.1 Allgemeine Informationen

Sophos Endpoint Security and Control beschränkt den Zugriff auf bestimmte Teile der Software auf Mitglieder bestimmter Sophos Gruppen.

Bei der Installation von Sophos Endpoint Security and Control werden alle Benutzer des Computers in Abhängigkeit ihrer Windows-Gruppen einer Sophos Gruppe zugewiesen.

Windows-Gruppe	Sophos Gruppe
Administratoren	SophosAdministrator
Hauptbenutzer	SophosPowerUser
Benutzer	SophosUser

Benutzer, die keiner Sophos Gruppe zugewiesen wurden, inklusive Gastbenutzer, können nur folgende Aufgaben ausführen:

- On-Access-Scans
- Rechtsklick-Scans

#### **SophosUsers**

SophosUsers können die genannten und folgende Aufgaben ausführen:

- Öffnen des Fensters von Sophos Endpoint Security and Control
- Einrichten und Ausführen von On-Demand-Scans
- Konfigurieren von Rechtsklick-Scans
- Verwalten (mit begrenzten Rechten) von Objekten in Quarantäne
- Erstellen und Konfigurieren von Firewall-Regeln

#### **SophosPowerUsers**

Zusätzlich zu den Rechten der SophosUsers besitzen SophosPowerUsers folgende Berechtigungen:

- Mehr Rechte im Quarantäne-Manager
- Zugriff auf den Authorization Manager

#### **SophosAdministrators**

SophosAdministrators können beliebige Komponenten von Sophos Endpoint Security and Control konfigurieren.

**Hinweis:** Wenn der Manipulationsschutz aktiviert ist, können Mitglieder der Gruppe **SophosAdministrators** die folgenden Aufgaben nur nach Angabe des Manipulationsschutz-Kennworts eingeben.

- Konfigurieren von On-Access-Scans.
- Konfigurieren der Erkennung verdächtigen Verhaltens.
- Deaktivieren des Manipulationsschutzes.

Weitere Informationen finden Sie unter [Allgemeine Informationen](#) (Seite 78).

## 3.2 Aufnahmen von Benutzern in eine Sophos Gruppe

Domänen-Administratoren und Mitglieder der Gruppe „Windows Administrators“ auf diesem Computer können die Mitgliedschaft in Sophos Gruppen ändern. Dies ist in der Regel erforderlich, um die Zugriffsrechte auf Sophos Endpoint Security and Control zu ändern.

So können Sie einen Benutzer in eine Sophos Gruppe aufnehmen:

1. Öffnen Sie die Computerverwaltung in Windows (Pfad siehe unten).
2. Klicken Sie im Konsolenstamm auf **Benutzer**.
3. Rechtsklicken Sie auf das Benutzerkonto **Eigenschaften**.
4. Klicken Sie auf der Registerkarte **Mitgliedschaft** auf **Hinzufügen**.
5. Geben Sie in das Feld **Geben Sie die zu verwendenden Objektnamen ein** den Namen einer Sophos Gruppe ein:
  - SophosAdministrator
  - SophosPowerUser
  - SophosUser
6. Wenn Sie den Namen der Sophos Gruppe auf seine Richtigkeit überprüfen möchten, klicken Sie auf **Namen überprüfen**.

Die Änderungen an den Zugriffsrechten auf Sophos Endpoint Security and Control werden bei der nächsten Anmeldung des Benutzers übernommen.

### Hinweise

- Klicken Sie zum Öffnen der Computerverwaltung auf **Start, Systemsteuerung**. Doppelklicken Sie auf **Verwaltung** und doppelklicken Sie anschließend auf **Computerverwaltung**.
- Wenn Sie einen Benutzer aus einer Sophos Benutzergruppe entfernen möchten, wählen Sie auf der Registerkarte **Mitgliedschaft** die gewünschte Gruppe im Bereich **Mitglied von** aus und klicken Sie anschließend auf **Entfernen**.

### 3.3 Konfigurieren der Benutzerrechte für den Quarantäne-Manager

Mitglieder der Gruppe **SophosAdministrator** können die Benutzerrechte für den Quarantäne-Manager konfigurieren.

1. Klicken Sie auf **Startseite > Anti-virus und HIPS > Anti-virus und HIPS konfigurieren > Konfigurieren > Benutzerrechte für Quarantäne-Manager** .
2. Geben Sie an, welche Benutzergruppen jeweils welche Maßnahmen ausführen dürfen.

**Hinweis:** Mit Ausnahme der Berechtigung zum **Zulassen** von Objekten beschränken sich die hier vergebenen Rechte auf den **Quarantäne-Manager**.

Option	Beschreibung
<b>Sektoren bereinigen</b>	Benutzer können die Bootsektoren von Disketten bereinigen.
<b>Dateien bereinigen</b>	Benutzer können Dokumente und Programme bereinigen.
<b>Dateien löschen</b>	Benutzer können infizierte Dateien löschen.
<b>Dateien verschieben</b>	Benutzer können infizierte Dateien in einen anderen Ordner verschieben.
<b>Zulassen</b>	Benutzer können verdächtige Objekten, Adware und PUA zulassen, die dann auf dem Computer ausgeführt werden können. Diese Berechtigung gilt für den <b>Authorization Manager</b> und den <b>Quarantäne-Manager</b> .

## 4 Sophos Anti-Virus

### 4.1 Wie unterscheiden sich On-Access-Scans von On-Demand-Scans?

#### On-Access-Scans

Die On-Access-Scanfunktion ist der Hauptmechanismus zum Schutz vor Viren und sonstigen Threats.

Beim Versuch, eine Datei zu kopieren, speichern, verschieben oder öffnen, scannt Sophos Anti-Virus die Datei. Der Zugriff wird nur erlaubt, wenn die Datei threatfrei ist bzw. zugelassen wurde.

Sophos Administratoren können zudem festlegen, dass Dateien beim Speichern, Erstellen oder Umbenennen gescannt werden. Weitere Informationen finden Sie unter [Ändern der Bedingungen für On-Access-Scans](#) (Seite 11).

#### On-Demand-Scans

Der Computerschutz von Sophos Anti-Virus wird durch **On-Demand-Scans** ergänzt.

On-Demand-Scans werden vom Benutzer eingeleitet. Dabei können einzelne Dateien oder der gesamte Computer gescannt werden.

Weitere Informationen finden Sie unter [Verfügbare Optionen](#) (Seite 14).

### 4.2 On-Access-Scans

#### 4.2.1 Konfigurieren von On-Access-Scans

So öffnen Sie das Dialogfeld mit den On-Access-Scan-Einstellungen:

- ❖ Klicken Sie auf **Startseite > Anti-virus und HIPS > Anti-virus und HIPS konfigurieren > Konfigurieren > On-Access-Scans**.
- [Scannen von Archivdateien](#) (Seite 22)
- [Scannen auf Macintosh-Viren](#) (Seite 22)
- [Scannen aller Dateien](#) (Seite 23)
- [Scannen auf Adware und PUA](#) (Seite 23)
- [Scannen auf verdächtige Dateien](#) (Seite 23)
- [Zurücksetzen der Prüfsummen gescannter Dateien](#) (Seite 9)

## 4.2.2 Zurücksetzen der Prüfsummen gescannter Dateien

Bei Updates von Sophos Anti-Virus und Neustarts des Computers wird die Liste der Prüfsummen gescannter Dateien zurückgesetzt. Die Liste wird dann wieder mit neuen Daten erstellt, wenn Dateien von Sophos Anti-Virus gescannt werden.

Wenn Sie den Computer nicht neu starten möchten, können Sie die Liste der Prüfsummen gescannter Dateien in Sophos Endpoint Security and Control zurücksetzen.

So setzen Sie die Prüfsummen gescannter Dateien zurück:

1. Klicken Sie auf **Startseite > Anti-virus und HIPS > Anti-virus und HIPS konfigurieren > Konfigurieren > On-Access-Scans**.
2. Klicken Sie auf der Registerkarte **Optionen** auf **Cache leeren**.

## 4.2.3 Festlegen von Dateierweiterungen

**Wichtig:** Wenn Sophos Endpoint Security and Control über eine Management-Konsole verwaltet wird, werden hier vorgenommene Änderungen eventuell nicht berücksichtigt.

Sie können festlegen, welche Dateien in On-Access-Scans einbezogen werden sollen.

1. Klicken Sie auf **Startseite > Anti-virus und HIPS > Anti-virus und HIPS konfigurieren > Konfigurieren > On-Access-Scans**.
2. Klicken Sie auf die Registerkarte **Erweiterungen** und stellen Sie folgende Optionen ein.

### Scannen aller Dateien

Wählen Sie diese Option, wenn alle Dateien, also unabhängig von ihrer Erweiterung, gescannt werden sollen.

### Scan-Objekte selbst bestimmen

Wählen Sie diese Option, um Scans auf Dateitypen zu beschränken, die in der Erweiterungsliste angegeben sind.



**Vorsicht:** Die Erweiterungsliste umfasst Dateitypen, bei denen Sophos Scans empfiehlt. Ändern Sie die Liste nur mit Bedacht (siehe unten).

Um eine Dateinamenerweiterung in die Liste aufzunehmen, klicken Sie auf **Hinzufügen**. Als Zeichenersatz können Sie das Platzhalterzeichen ? eingeben.

Um eine Dateinamenerweiterung aus der Liste zu entfernen, markieren Sie die Erweiterung und klicken auf **Entfernen**.

Um eine Dateinamenerweiterung in der Liste zu ändern, markieren Sie die Erweiterung und klicken auf **Bearbeiten**.

Wenn Sie **Scan-Objekte selbst bestimmen** wählen, wird automatisch die Option **Dateien ohne Erweiterung scannen** ausgewählt. Wenn Dateien ohne Erweiterung nicht gescannt werden sollen, deaktivieren Sie die Option **Dateien ohne Erweiterung scannen**.

## 4.2.4 Ausschließen von Objekten

**Wichtig:** Wenn Sophos Endpoint Security and Control über eine Management-Konsole verwaltet wird, werden hier vorgenommene Änderungen eventuell nicht berücksichtigt.

Sie können Dateien, Ordner oder Laufwerke von On-Access-Scans ausschließen.

1. Klicken Sie auf **Startseite > Anti-virus und HIPS > Anti-virus und HIPS konfigurieren > Konfigurieren > On-Access-Scans** .
2. Klicken Sie auf die Registerkarte **Ausschlüsse** und stellen Sie folgende Optionen ein.

### Ausgeschlossenes Objekt

Klicken Sie zur Angabe der Objekte, die nicht gescannt werden sollen, auf **Hinzufügen**. Geben Sie im Dialogfeld **Objekt ausschließen** den Typ und den Namen des Objekts an, das Sie vom Scan ausschließen möchten. Mehr zu diesem Thema finden Sie unter *Auswählen der ausgeschlossenen Objekte*.

Um Objekte aus der Ausschlussliste zu entfernen, klicken Sie auf **Entfernen**.

Um Objekte in der Ausschlussliste zu ändern, klicken Sie auf **Bearbeiten**.

### Auswählen der ausgeschlossenen Objekte

Wählen Sie im Dialogfeld **Objekt ausschließen** den **Objekttyp**.

Geben Sie den **Objektnamen** ein oder suchen Sie das Objekt über die Schaltfläche **Durchsuchen**.

**Hinweis:** Bei 64-Bit-Plattformen wird die Schaltfläche **Durchsuchen** im Dialog **Objekt ausschließen** nicht angezeigt.

Es folgen nun einige Hinweise zur Benennung von Objekten.

#### ■ **Dateiname**

Sie brauchen nur den Namen einer Datei angeben und Sophos Anti-Virus schließt alle Dateien mit diesem Namen aus, egal wo sie sich befinden. Zum Beispiel sorgt

`fred.bmp`

dafür, dass Sophos Anti-Virus alle Dateien namens „fred.bmp“ ausschließt.

#### ■ **Vollständiger Pfad**

Wenn Sie den genauen Pfad mitsamt Dateinamen angeben, schließt Sophos Anti-Virus nur diese Datei aus. Der Pfad kann das Laufwerk oder die Freigabe enthalten. Zum Beispiel sorgt

`C:\Sonstige\fred.bmp`

dafür, dass Sophos Anti-Virus die Datei „fred.bmp“ im Ordner „Sonstige“ auf Laufwerk C: ausschließt.

`\\Server1\Users\Fred\Letter.rtf`

sorgt dafür, dass Sophos Anti-Virus die Datei „Letter.rtf“ im Ordner „Fred“ auf der Freigabe „Users“ auf Server1 ausschließt.

Wenn Sie kein Laufwerk oder keine Freigabe angeben, übernimmt Sophos Anti-Virus den Pfad im Stammordner jedes Laufwerks oder jeder Freigabe.

#### ■ Teilpfad

Wenn Sie ein Laufwerk oder eine Freigabe angeben, schließt Sophos Anti-Virus alle darauf befindlichen Objekte aus. Zum Beispiel sorgt

A:

dafür, dass Sophos Anti-Virus alle Objekte auf Laufwerk A: ausschließt.

Wenn Sie einen Ordner angeben, schließt Sophos Anti-Virus alle in und unter diesem Ordner enthaltenen Objekte aus. Zum Beispiel sorgt

D:\Tools\

dafür, dass Sophos Anti-Virus alle Objekte auf Laufwerk D: im Ordner „Tools“ und allen Unterordnern ausschließt.

Sie können einen Ordner und einen Dateinamen angeben, woraufhin Sophos Anti-Virus alle Ordner und Dateinamen ausschließt, die damit übereinstimmen. Zum Beispiel sorgt

logs\log.txt

dafür, dass Sophos Anti-Virus die Datei „log.txt“ in jedem Ordner namens „logs“ auf jedem Laufwerk oder auf jeder Freigabe ausschließt.

#### Platzhalter

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.

#### Mehrere Dateinamenerweiterungen

Bei Dateinamen mit mehreren Erweiterungen wird die letzte Erweiterung als Erweiterung und die anderen werden als Teil des Dateinamens behandelt. Beispiel:

„[dateiname].[erweiterung1].[erweiterung2]“ bedeutet, dass der Dateiname „[dateiname].[erweiterung1]“ lautet und die Erweiterung „[erweiterung2]“ ist.

#### Namenskonventionen

Der Dateiname oder Pfad wird mit den Namenskonventionen abgeglichen (ein Ordnername kann beispielsweise Leerzeichen enthalten, aber nicht ausschließlich Leerzeichen).

## 4.2.5 Ändern der Bedingungen für On-Access-Scans

**Wichtig:** Wenn Sophos Endpoint Security and Control über eine Management-Konsole verwaltet wird, werden hier vorgenommene Änderungen eventuell nicht berücksichtigt.

Standardmäßig werden Dateien in Sophos Anti-Virus beim Kopieren, Verschieben oder Öffnen gescannt.

Sophos Administratoren können zudem festlegen, dass Dateien beim Speichern, Erstellen oder Umbenennen gescannt werden.

1. Klicken Sie auf **Startseite > Anti-virus und HIPS > Anti-virus und HIPS konfigurieren > Konfigurieren > On-Access-Scans**.
2. Klicken Sie auf die Registerkarte **Scannen** und stellen Sie folgende Optionen ein.

Scan-Zeitpunkte	Option
Kopieren, Verschieben oder Öffnen	<b>Beim Lesen</b>
Speichern oder Erstellen	<b>Beim Schreiben</b>
Umbenennen	<b>Beim Umbenennen</b>

#### 4.2.6 Vorübergehende Deaktivierung der On-Access-Scans

Wenn Sie in die SophosAdministrator-Gruppe eingegliedert sind, muss On-Access-Scanning unter bestimmten Umständen (z.B. aus Wartungsgründen oder zur Fehlerbehebung) vorübergehend deaktiviert werden. Es können jedoch weiterhin On-Demand-Scans ausgeführt werden.

Sophos Endpoint Security and Control behält die hier vorgenommenen Änderungen bei, auch wenn Sie den Computer später neu starten. Der Computer bleibt so lange ungeschützt, bis die On-Access-Scans wieder aktiviert werden.

1. Klicken Sie auf **Startseite > Anti-virus und HIPS > Anti-virus und HIPS konfigurieren > Konfigurieren > On-Access-Scans**.
2. Deaktivieren Sie das Kontrollkästchen **On-Access-Scans für diesen Computer aktivieren**.

#### 4.2.7 Erkennen von verdächtigem Verhalten und Pufferüberläufen

**Wichtig:** Wenn Sophos Endpoint Security and Control über eine Management-Konsole verwaltet wird, werden hier vorgenommene Änderungen eventuell nicht berücksichtigt.

Die Erkennung verdächtigen Verhaltens führt mit Hilfe von Sophos HIPS (Host Intrusion Prevention System) eine dynamische Verhaltensanalyse aller auf dem Computer ausgeführten Programme durch, um Aktivitäten zu erkennen und zu sperren, die wahrscheinlich schädlich sind. 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-Attacken.

**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.

Mitglieder der Gruppe „SophosAdministrator“ können die Einstellungen in Zusammenhang mit verdächtigem Verhalten und Pufferüberläufen ändern:

1. Klicken Sie auf **Startseite > Anti-virus und HIPS > Anti-virus und HIPS konfigurieren > Konfigurieren > Erkennung verdächtigen Verhaltens** zur Anzeige
2. Verfahren Sie im Dialogfeld **Erkennung verdächtigen Verhaltens** wie folgt:
  - Aktivieren/Deaktivieren Sie je nach Bedarf das Kontrollkästchen **Erkennung verdächtigen Verhaltens**.
  - Aktivieren/Deaktivieren Sie je nach Bedarf das Kontrollkästchen **Erkennung von Pufferüberläufen**.
  - Standardmäßig werden verdächtiges Verhalten und Pufferüberläufe *erkannt*, jedoch nicht *gesperrt* (die Option **Nur benachrichtigen** ist aktiviert).



**Vorsicht:** Es wird empfohlen, dass Sie Sophos Anti-Virus eine Zeit lang im Erkennungsmodus ausführen und die gewünschten Programme erlauben, bevor Sie das automatische Sperren verdächtigen Verhaltens und von Pufferüberläufen aktivieren. Dadurch wird das Sperren von Programmen vermieden, die täglich genutzt werden.

Um das *Sperren* verdächtigen Verhaltens und von Pufferüberläufen und die *Erkennung* zu aktivieren, deaktivieren Sie das Kontrollkästchen **Nur benachrichtigen**.

## 4.2.8 Scannen auf Controlled Applications

*Controlled Applications* sind Anwendungen, deren Ausführung durch die Sicherheitsrichtlinie des Unternehmens unterbunden wird.

Das Scannen auf Controlled Applications ist eine Komponente von On-Demand-Scans und wird von der Management-Konsole über die Application Control-Richtlinie aktiviert bzw. deaktiviert.

Weitere Informationen zu On-Access-Scans entnehmen Sie bitte dem Abschnitt [Wie unterscheiden sich On-Access-Scans von On-Demand-Scans?](#) (Seite 8).

## 4.2.9 Deaktivieren des Scannens auf Controlled Applications

**Wichtig:** Wenn Sophos Endpoint Security and Control über eine Management-Konsole verwaltet wird, werden hier vorgenommene Änderungen eventuell nicht berücksichtigt.

Bei aktivierten Scans auf Controlled Applications ist die Installation einiger Anwendungen mitunter nicht möglich. Mitglieder der Gruppe „SophosAdministrator“ können das Scannen auf Controlled Applications auf dem Computer vorübergehend deaktivieren.

Verfahren Sie hierzu wie folgt:

1. Klicken Sie im Menü **Konfigurieren** auf **Application Control**.
2. Deaktivieren Sie das Kontrollkästchen **On-Access-Scans aktivieren**.

## 4.3 On-Demand-Scans

### 4.3.1 Verfügbare Optionen

#### **vollständige Überprüfung**

Scan des gesamten Computers, einschließlich des Bootsektors und Systemspeichers, der jederzeit eingeleitet werden kann.

- [Ausführen eines vollständigen Computer-Scans](#) (Seite 17)

#### **Rechtsklick-Scan**

Scan von Dateien, Ordnern oder Laufwerken in Windows Explorer, der jederzeit eingeleitet werden kann.

- [Rechtsklick-Scans](#) (Seite 18)

#### **Individueller Scan**

Scan ausgewählter Dateien oder Ordner. Sie können individuelle Scans manuell durchführen oder zeitlich planen und automatisch ausführen lassen.

- [Ausführen von individuellen Scans](#) (Seite 20)
- [Planen eines individuellen Scans](#) (Seite 20)

### 4.3.2 Festlegen von Dateierweiterungen

**Wichtig:** Wenn Sophos Endpoint Security and Control über eine Management-Konsole verwaltet wird, werden hier vorgenommene Änderungen eventuell nicht berücksichtigt.

Sie können festlegen, welche Dateien in On-Demand-Scans einbezogen werden sollen.

1. Klicken Sie im Menü **Konfigurieren** auf **Erweiterungen und Ausschlüsse für On-Demand-Scans**.

2. Klicken Sie auf die Registerkarte **Erweiterungen** und stellen Sie folgende Optionen ein.

#### **Scannen aller Dateien**

Wählen Sie diese Option, wenn alle Dateien, also unabhängig von ihrer Erweiterung, gescannt werden sollen.

#### **Scan-Objekte selbst bestimmen**

Wählen Sie diese Option, um Scans auf Dateitypen zu beschränken, die in der Erweiterungsliste angegeben sind.



**Vorsicht:** Die Erweiterungsliste umfasst Dateitypen, bei denen Sophos Scans empfiehlt. Ändern Sie die Liste nur mit Bedacht (siehe unten).

Um eine Dateinamenerweiterung in die Liste aufzunehmen, klicken Sie auf **Hinzufügen**. Als Zeichenersatz können Sie das Platzhalterzeichen ? eingeben.

Um eine Dateinamenerweiterung aus der Liste zu entfernen, markieren Sie die Erweiterung und klicken auf **Entfernen**.

Um eine Dateinamenerweiterung in der Liste zu ändern, markieren Sie die Erweiterung und klicken auf **Bearbeiten**.

Wenn Sie **Scan-Objekte selbst bestimmen** wählen, wird automatisch die Option **Dateien ohne Erweiterung scannen** ausgewählt. Wenn Dateien ohne Erweiterung nicht gescannt werden sollen, deaktivieren Sie die Option **Dateien ohne Erweiterung scannen**.

### 4.3.3 Ausschließen von Objekten

**Wichtig:** Wenn Sophos Endpoint Security and Control über eine Management-Konsole verwaltet wird, werden hier vorgenommene Änderungen eventuell nicht berücksichtigt.

Sie können Dateien, Ordner oder Laufwerke von On-Demand-Scans ausschließen.

**Hinweis:** Die nachfolgend erläuterte Vorgehensweise gilt für *alle* On-Demand-Scans. Um Objekte von einem *bestimmten* On-Demand-Scan auszuschließen, lesen Sie [Erstellen eines individuellen Scans](#) (Seite 18).

1. Klicken Sie auf **Startseite > Anti-virus und HIPS > Anti-virus und HIPS konfigurieren > Konfigurieren > On-Demand-Erweiterungen und -Ausschlüsse** .
2. Klicken Sie auf die Registerkarte **Ausschlüsse**. Nehmen Sie die folgenden Einstellungen vor:

#### **Ausgeschlossenes Objekt**

Klicken Sie zur Angabe der Objekte, die nicht gescannt werden sollen, auf **Hinzufügen**. Geben Sie im Dialogfeld **Objekt ausschließen** den Typ und den Namen des Objekts an, das Sie vom Scan ausschließen möchten. Mehr zu diesem Thema finden Sie unter *Auswählen der ausgeschlossenen Objekte*.

Um Objekte aus der Ausschlussliste zu entfernen, klicken Sie auf **Entfernen**.

Um Objekte in der Ausschlussliste zu ändern, klicken Sie auf **Bearbeiten**.

## Auswählen der ausgeschlossenen Objekte

Wählen Sie im Dialogfeld **Objekt ausschließen** den **Objekttyp**.

Geben Sie den **Objektnamen** ein oder suchen Sie das Objekt über die Schaltfläche **Durchsuchen**.

**Hinweis:** Bei 64-Bit-Plattformen wird die Schaltfläche **Durchsuchen** im Dialog **Objekt ausschließen** nicht angezeigt.

Es folgen nun einige Hinweise zur Benennung von Objekten.

### ■ **Dateiname**

Sie brauchen nur den Namen einer Datei angeben und Sophos Anti-Virus schließt alle Dateien mit diesem Namen aus, egal wo sie sich befinden. Zum Beispiel sorgt

`fred.bmp`

dafür, dass Sophos Anti-Virus alle Dateien namens „fred.bmp“ ausschließt.

### ■ **Vollständiger Pfad**

Wenn Sie den genauen Pfad mitsamt Dateinamen angeben, schließt Sophos Anti-Virus nur diese Datei aus. Der Pfad kann das Laufwerk oder die Freigabe enthalten. Zum Beispiel sorgt

`C:\Sonstige\fred.bmp`

dafür, dass Sophos Anti-Virus die Datei „fred.bmp“ im Ordner „Sonstige“ auf Laufwerk C: ausschließt.

`\\Server1\Users\Fred\Letter.rtf`

sorgt dafür, dass Sophos Anti-Virus die Datei „Letter.rtf“ im Ordner „Fred“ auf der Freigabe „Users“ auf Server1 ausschließt.

Wenn Sie kein Laufwerk oder keine Freigabe angeben, übernimmt Sophos Anti-Virus den Pfad im Stammordner jedes Laufwerks oder jeder Freigabe.

### ■ **Teilpfad**

Wenn Sie ein Laufwerk oder eine Freigabe angeben, schließt Sophos Anti-Virus alle darauf befindlichen Objekte aus. Zum Beispiel sorgt

`A:`

dafür, dass Sophos Anti-Virus alle Objekte auf Laufwerk A: ausschließt.

Wenn Sie einen Ordner angeben, schließt Sophos Anti-Virus alle in und unter diesem Ordner enthaltenen Objekte aus. Zum Beispiel sorgt

`D:\Tools\`

dafür, dass Sophos Anti-Virus alle Objekte auf Laufwerk D: im Ordner „Tools“ und allen Unterordnern ausschließt.

Sie können einen Ordner und einen Dateinamen angeben, woraufhin Sophos Anti-Virus alle Ordner und Dateinamen ausschließt, die damit übereinstimmen. Zum Beispiel sorgt

`logs\log.txt`

dafür, dass Sophos Anti-Virus die Datei „log.txt“ in jedem Ordner namens „logs“ auf jedem Laufwerk oder auf jeder Freigabe ausschließt.

### Platzhalter

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.

### Mehrere Dateinamenerweiterungen

Bei Dateinamen mit mehreren Erweiterungen wird die letzte Erweiterung als Erweiterung und die anderen werden als Teil des Dateinamens behandelt. Beispiel:

„[dateiname].[erweiterung1].[erweiterung2]“ bedeutet, dass der Dateiname „[dateiname].[erweiterung1]“ lautet und die Erweiterung „[erweiterung2]“ ist.

### Namenskonventionen

Der Dateiname oder Pfad wird mit den Namenskonventionen abgeglichen (ein Ordnername kann beispielsweise Leerzeichen enthalten, aber nicht ausschließlich Leerzeichen).

## 4.3.4 Ausführen eines vollständigen Computer-Scans

**Hinweis:** Mit **Computer scannen** werden keine Macintosh-Dateien auf Windows-Systemen gescannt. Wenn Sophos Anti-Virus ausführbare Macintosh-Dateien scannen soll, müssen Sie einen individuellen On-Demand-Scan einrichten und das Scannen von Macintosh-Dateien für diesen Scan aktivieren.

Weitere Informationen zu angepassten On-Demand-Scans finden Sie unter [Erstellen eines individuellen Scans](#) (Seite 18).

Weitere Informationen zu Macintosh-Dateien finden Sie unter [Scannen auf Macintosh-Viren](#) (Seite 22).

So leiten Sie einen vollständigen Computer-Scan (inkl. Bootsektor und Arbeitsspeicher) ein:

- ❖ Klicken Sie auf der **Startseite** im Bereich **Antivirus und HIPS** auf **Computer scannen**. Weitere Informationen zur **Startseite** finden Sie unter [Die Startseite](#) (Seite 4).

Es wird ein Fortschrittsdialogfeld angezeigt und die **Aktivitäts-Zusammenfassung** wird im **Sophos Endpoint Security and Control**-Fenster angezeigt.

Werden Threats oder Controlled Applications gefunden, klicken Sie auf **Details** und lesen Sie den Abschnitt *Objekte in Quarantäne verwalten*.

### 4.3.5 Konfigurieren von Rechtsklick-Scans

**Wichtig:** Wenn Sophos Endpoint Security and Control auf diesem Computer über eine Management-Konsole verwaltet wird, werden hier vorgenommene Änderungen *dennoch berücksichtigt*.

❖ Klicken Sie auf **Startseite > Anti-virus und HIPS > Anti-virus und HIPS konfigurieren > Konfigurieren > Rechtsklick-Scans**.

- [Scannen von Archivdateien](#) (Seite 22)
- [Scannen auf Macintosh-Viren](#) (Seite 22)
- [Scannen aller Dateien](#) (Seite 23)
- [Scannen auf Adware und PUA](#) (Seite 23)
- [Scannen auf verdächtige Dateien](#) (Seite 23)

### 4.3.6 Rechtsklick-Scans

Sie können Dateien, Ordner und Laufwerke in Windows Explorer oder auf dem Desktop einem Rechtsklick-Scan unterziehen.

1. Wählen Sie nun das zu scannende Objekt (Datei, Order oder Laufwerk).  
Sie können mehrere Dateien und Ordner auf einmal auswählen.
2. Rechtsklicken Sie und wählen Sie den Menüpunkt **Mit Sophos Anti-Virus scannen**.

Werden Threats oder Controlled Applications gefunden, klicken Sie auf **Details** und lesen Sie den Abschnitt *Objekte in Quarantäne verwalten*.

### 4.3.7 Individuelle Scans

#### 4.3.7.1 Erstellen eines individuellen Scans

1. Klicken Sie auf der **Startseite** im Bereich **Antivirus und HIPS** auf **Scans**.  
Weitere Informationen zur **Startseite** finden Sie unter [Die Startseite](#) (Seite 4).
2. Klicken Sie auf **Neuer Scan**.
3. Geben Sie im Textfeld **Scan-Name** einen Namen für den Scan ein.
4. Wählen Sie im Bereich **Scan-Objekte** die zu scannenden Laufwerke und Ordner aus. Aktivieren Sie dazu das Kontrollkästchen links neben jedem Laufwerk oder Ordner. Eine Beschreibung der Symbole in den Kästchen finden Sie im Abschnitt [Darstellung der Scan-Objekte](#) (Seite 19).

**Hinweis:** Laufwerke oder Ordner, die nicht verfügbar sind (weil sie offline sind oder gelöscht wurden), werden durchgestrichen dargestellt. Sie werden aus dem Bereich **Scan-Objekte** entfernt, wenn sie deaktiviert sind oder es eine Änderung in der Auswahl des übergeordneten Laufwerks oder Ordners gibt.

5. Um einen weiteren Scan zu konfigurieren, klicken Sie auf **Scan konfigurieren**. (Weitere Informationen finden Sie unter [Konfigurieren eines individuellen Scans](#) (Seite 19).)
6. Um einen Zeitplan für den Scan einzustellen, klicken Sie auf **Scan planen**. (Weitere Informationen finden Sie unter [Planen eines individuellen Scans](#) (Seite 20).)
7. Klicken Sie auf **Speichern**, um den Scan zu speichern, und auf **Speichern/Start**, um den Scan zu speichern und zu starten.

#### 4.3.7.2 Darstellung der Scan-Objekte

Im Bereich **Scan-Objekte** werden im Kästchen neben den jeweiligen Objekten (Laufwerk oder Ordner) je nach Scanumfang unterschiedliche Symbole angezeigt. Die folgende Tabelle bietet eine Übersicht über die Symbole.

Symbol	Erklärung
<input type="checkbox"/>	Das Objekt und alle darunter liegenden Objekte sind für den Scan <i>nicht ausgewählt</i> .
<input checked="" type="checkbox"/>	Das Objekt und alle darunter liegenden Objekte sind für den Scan <i>ausgewählt</i> .
<input checked="" type="checkbox"/>	Das Objekt ist teilweise ausgewählt: Einige Unterobjekte sind für den Scan ausgewählt.
<input checked="" type="checkbox"/>	Das Objekt und alle darunter liegenden Objekte sind von diesem Scan ausgeschlossen.
<input checked="" type="checkbox"/>	Das Objekt ist teilweise ausgeschlossen: Das Objekt ist ausgewählt, doch einige Unterobjekte sind von diesem Scan ausgeschlossen.
<input checked="" type="checkbox"/>	Das Objekt ist mitsamt den Unterobjekten aufgrund einer On-Demand-Ausnahme von allen On-Demand-Scans ausgeschlossen. Nähere Informationen hierzu finden Sie unter <a href="#">Ausschließen von Objekten</a> (Seite 10).

#### 4.3.7.3 Konfigurieren eines individuellen Scans

1. Klicken Sie auf der **Startseite** im Bereich **Antivirus und HIPS** auf **Scans**.  
Weitere Informationen zur **Startseite** finden Sie unter [Die Startseite](#) (Seite 4).
2. Wählen Sie den gewünschten Scan aus der Liste **Verfügbare Scans** aus und klicken Sie auf **Bearbeiten**.
3. Klicken Sie auf **Scan konfigurieren**.
  - [Scannen von Archivdateien](#) (Seite 22)
  - [Scannen auf Macintosh-Viren](#) (Seite 22)
  - [Scannen aller Dateien](#) (Seite 23)
  - [Scannen auf Adware und PUA](#) (Seite 23)
  - [Scannen auf verdächtige Dateien](#) (Seite 23)

- [Scannen auf Rootkits](#) (Seite 20)

#### 4.3.7.4 Scannen auf Rootkits

**Wichtig:** Wenn Sophos Endpoint Security and Control über eine Management-Konsole verwaltet wird, werden hier vorgenommene Änderungen eventuell nicht berücksichtigt.

Wenn Sie eine vollständige Systemprüfung auf einem Computer durchführen, wird der Computer auch auf Rootkits gescannt (wenn Sie ein Mitglied der SophosAdministrator-Gruppe sind).

Sie können auch im Rahmen eines individuellen Scans auf Rootkits scannen.

So scannen Sie auf Rootkits:

1. Klicken Sie auf der **Startseite** im Bereich **Antivirus und HIPS** auf **Scans**.  
Weitere Informationen zur **Startseite** finden Sie unter [Die Startseite](#) (Seite 4).
2. Wählen Sie den gewünschten Scan aus der Liste **Verfügbare Scans** aus und klicken Sie auf **Bearbeiten**.
3. Klicken Sie auf **Scan konfigurieren**.
4. Markieren Sie auf der Registerkarte **Optionen** das Kontrollkästchen **Rootkits scannen**.

#### 4.3.7.5 Planen eines individuellen Scans

Wenn Sie ein Mitglied der Gruppe "SophosAdministrator" sind, können Sie individuelle Scans einrichten und auch Scans von anderen Benutzern ansehen und bearbeiten.

1. Klicken Sie auf der **Startseite** im Bereich **Antivirus und HIPS** auf **Scans**.  
Weitere Informationen zur **Startseite** finden Sie unter [Die Startseite](#) (Seite 4).
2. Wählen Sie den gewünschten Scan aus der Liste **Verfügbare Scans** aus und klicken Sie auf **Bearbeiten**.
3. Klicken Sie auf **Zeitplan für Scan einrichten**.
4. Wählen Sie im Dialogfeld **Zeitplan für Scan einrichten** die Option **Zeitplan aktivieren**.  
Geben Sie an, an welchen Tagen der Scan stattfinden soll.  
Durch Klick auf **Hinzufügen** können Sie bestimmte Uhrzeiten festlegen.  
Um eine Uhrzeit zu entfernen oder zu ändern, markieren Sie sie und klicken Sie jeweils auf **Entfernen** oder **Ändern**.
5. Geben Sie *Benutzernamen* und *Kennwort* ein. Das Kennwortfeld darf nicht leer bleiben.  
Bei diesem geplanten Scan gelten die Zugriffsrechte dieses Benutzers.

#### 4.3.7.6 Ausführen von individuellen Scans

**Hinweis:** Geplante individuelle Scans können nicht manuell ausgeführt werden. Geplante Scans werden in der Liste **Verfügbare Scans** mit einem Uhrensymbol angezeigt.

1. Klicken Sie auf der **Startseite** im Bereich **Antivirus und HIPS** auf **Scans**.  
Weitere Informationen zur **Startseite** finden Sie unter [Die Startseite](#) (Seite 4).

2. Wählen Sie den gewünschten Scan aus der Liste **Verfügbare Scans** aus und klicken Sie auf **Start**.

Es wird ein Fortschrittsdialog angezeigt und die **Zusammenfassung der Aktivitäten** erscheint im Sophos Endpoint Security and Control-Fenster.

Werden Threats oder Controlled Applications gefunden, klicken Sie auf **Details** und lesen Sie den Abschnitt *Objekte in Quarantäne verwalten*.

#### 4.3.7.7 Umbenennen eines individuellen Scans

1. Klicken Sie auf der **Startseite** im Bereich **Antivirus und HIPS** auf **Scans**.  
Weitere Informationen zur **Startseite** finden Sie unter [Die Startseite](#) (Seite 4).
2. Wählen Sie den gewünschten Scan aus der Liste **Verfügbare Scans** aus und klicken Sie auf **Bearbeiten**.
3. Geben Sie in das Feld **Scan-Name** den neuen Namen des Scans ein.

#### 4.3.7.8 Öffnen des Protokolls

1. Klicken Sie auf der **Startseite** im Bereich **Antivirus und HIPS** auf **Scans**.  
Weitere Informationen zur **Startseite** finden Sie unter [Die Startseite](#) (Seite 4).
2. Klicken Sie in der Liste **Verfügbare Scans** auf den individuellen Scan und dann auf **Zusammenfassung**.
3. Klicken Sie im unteren Bereich des Dialogfensters **Zusammenfassung** auf den Link.

Aus der Protokollseite können Sie das Protokoll in die Zwischenablage kopieren, es per E-Mail versenden oder ausdrucken.

Wenn Sie im Protokoll bestimmten Text suchen, klicken Sie auf **Suchen** und geben Sie den gewünschten Text in das Suchfeld ein.

#### 4.3.7.9 Aufrufen der Zusammenfassung eines individuellen Scans

1. Klicken Sie auf der **Startseite** im Bereich **Antivirus und HIPS** auf **Scans**.  
Weitere Informationen zur **Startseite** finden Sie unter [Die Startseite](#) (Seite 4).
2. Klicken Sie in der Liste **Verfügbare Scans** auf den individuellen Scan und dann auf **Zusammenfassung**.

#### 4.3.7.10 Löschen eines individuellen Scans

1. Klicken Sie auf der **Startseite** im Bereich **Antivirus und HIPS** auf **Scans**.  
Weitere Informationen zur **Startseite** finden Sie unter [Die Startseite](#) (Seite 4).
2. Wählen Sie den gewünschten Scan aus der Liste **Verfügbare Scans** aus und klicken Sie auf **Löschen**.

## 4.4 Scan-Optionen

### 4.4.1 Scannen von Archivdateien

**Wichtig:** Wenn Sophos Endpoint Security and Control über eine Management-Konsole verwaltet wird, werden hier vorgenommene Änderungen eventuell nicht berücksichtigt.

**Hinweis:** Aus folgenden Gründen empfiehlt sich die Auswahl dieser Option nicht:

- Das Scannen in Archivdateien wird erheblich verlangsamt.
- Auch wenn diese Option nicht aktiviert ist, wird eine aus einem Archiv extrahierte Datei beim Öffnen gescannt.
- Auch wenn diese Option nicht aktiviert ist, werden Dateien gescannt, die mit dynamischen Komprimierungsprogrammen (PKLite, LZEXE und Diet) gepackt wurden.

Es empfiehlt sich jedoch, die Option zu aktivieren, wenn Sie Archive oder komprimierte Dateien herunterladen und per E-Mail versenden und vorab scannen möchten.

So scannen Sie in Archivdateien:

1. Öffnen Sie die Einstellungen des zu konfigurierenden Scans. Entsprechende Anweisungen hierzu enthalten Sie über einen der folgenden Links:
  - [Konfigurieren von On-Access-Scans](#) (Seite 8)
  - [Konfigurieren von Rechtsklick-Scans](#) (Seite 18)
  - [Konfigurieren eines individuellen Scans](#) (Seite 19)
2. Markieren Sie auf der Registerkarte **Optionen** das Kontrollkästchen **Archivdateien scannen**.

### 4.4.2 Scannen auf Macintosh-Viren

**Wichtig:** Wenn Sophos Endpoint Security and Control über eine Management-Konsole verwaltet wird, werden hier vorgenommene Änderungen eventuell nicht berücksichtigt.

Sophos Anti-Virus kann beim Scannen von Windows-Systemen auch Macintosh-Dateien einbeziehen.

1. Öffnen Sie die Einstellungen des zu konfigurierenden Scans. Entsprechende Anweisungen hierzu enthalten Sie über einen der folgenden Links:
  - [Konfigurieren von On-Access-Scans](#) (Seite 8)
  - [Konfigurieren von Rechtsklick-Scans](#) (Seite 18)
  - [Konfigurieren eines individuellen Scans](#) (Seite 19)
2. Markieren Sie auf der Registerkarte **Optionen** das Kontrollkästchen **Macintosh-Viren einbeziehen**.

### 4.4.3 Scannen aller Dateien

**Wichtig:** Wenn Sophos Endpoint Security and Control über eine Management-Konsole verwaltet wird, werden hier vorgenommene Änderungen eventuell nicht berücksichtigt.

Sie können auch alle Dateien scannen lassen; dies bremst jedoch die Arbeitsgeschwindigkeit des Computers ab.

1. Öffnen Sie die Einstellungen des zu konfigurierenden Scans. Entsprechende Anweisungen hierzu enthalten Sie über einen der folgenden Links:
  - [Konfigurieren von On-Access-Scans](#) (Seite 8)
  - [Konfigurieren von Rechtsklick-Scans](#) (Seite 18)
  - [Konfigurieren eines individuellen Scans](#) (Seite 19)
2. Markieren Sie auf der Registerkarte **Optionen** das Kontrollkästchen **Alle Dateien scannen**.

### 4.4.4 Scannen auf Adware und PUA

**Wichtig:** Wenn Sophos Endpoint Security and Control über eine Management-Konsole verwaltet wird, werden hier vorgenommene Änderungen eventuell nicht berücksichtigt.

1. Öffnen Sie die Einstellungen des zu konfigurierenden Scans. Entsprechende Anweisungen hierzu enthalten Sie über einen der folgenden Links:
  - [Konfigurieren von On-Access-Scans](#) (Seite 8)
  - [Konfigurieren von Rechtsklick-Scans](#) (Seite 18)
  - [Konfigurieren eines individuellen Scans](#) (Seite 19)
2. Markieren Sie auf der Registerkarte **Optionen** das Kontrollkästchen **Adware und PUA einbeziehen**.

### 4.4.5 Scannen auf verdächtige Dateien

**Wichtig:** Wenn Sophos Endpoint Security and Control über eine Management-Konsole verwaltet wird, werden hier vorgenommene Änderungen eventuell nicht berücksichtigt.

Unter einer *verdächtigen Datei* ist eine Datei zu verstehen, die Virenmerkmale aufweist.

So scannen Sie auf verdächtige Dateien:

1. Öffnen Sie die Einstellungen des zu konfigurierenden Scans. Entsprechende Anweisungen hierzu enthalten Sie über einen der folgenden Links:
  - [Konfigurieren von On-Access-Scans](#) (Seite 8)
  - [Konfigurieren von Rechtsklick-Scans](#) (Seite 18)
  - [Konfigurieren eines individuellen Scans](#) (Seite 19)

2. Markieren Sie auf der Registerkarte **Optionen** das Kontrollkästchen **Verdächtige Dateien (HIPS) einbeziehen**.

## 4.5 Sophos Live-Schutz

### 4.5.1 Allgemeine Informationen

Sophos Live-Schutz stellt fest, ob eine verdächtige Datei einen Threat darstellt. Handelt es sich um einen Threat, werden umgehend die in der Bereinigungskonfiguration von Sophos Anti-Virus festgelegten Maßnahmen ergriffen.

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

Sophos Live-Schutz bietet die folgenden Optionen:

#### ■ 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 Dateidaten (z.B. die Prüfsumme der Datei und weitere Attribute) 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 verdächtig eingestuft wird, anhand der Dateidaten jedoch keine eindeutige Klassifizierung möglich ist, können Sie Sophos gestatten, ein Dateisample anzufordern. 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“).

### 4.5.2 Aktivieren/Deaktivieren der Optionen von Sophos Live-Schutz

**Wichtig:** Wenn Sophos Endpoint Security and Control über eine Management-Konsole verwaltet wird, werden hier vorgenommene Änderungen eventuell nicht berücksichtigt.

Mitglieder der Gruppe **SophosAdministrators** können die Optionen von Sophos Live-Schutz aktivieren bzw. deaktivieren:

1. Klicken Sie auf **Startseite > Anti-virus und HIPS > Anti-virus und HIPS konfigurieren > Konfigurieren > Sophos Live-Schutz** .

2. 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**.

Die Option ist nur verfügbar, wenn Sie **Live-Schutz aktivieren** ausgewählt haben.

### Hinweis

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

## 4.5.3 Aufrufen des Protokolls von Sophos Live-Schutz

Die zum Online-Scan an Sophos übertragenen Dateidaten sowie die Statusänderungen im Anschluss an den Scanvorgang werden im Scan-Protokoll des Computers festgehalten.

Wenn Sophos Live-Schutz aktiviert ist, können Sie folgende Informationen dem Protokoll entnehmen:

- Den Pfad aller Dateien, zu denen Daten an Sophos übermittelt wurden.
- Den Zeitpunkt der Übertragung.
- Bei fehlgeschlagener Übertragung: Ursache (sofern bekannt).
- Den aktuellen Status der Datei (beispielsweise „Virus/Spyware“, wenn die Datei als schädlich eingestuft wurde).

So können Sie das Scan-Protokoll anzeigen:

- Klicken Sie auf der **Startseite** unter **Antivirus und HIPS** auf **Antivirus- und HIPS-Protokoll öffnen**.

Nähere Informationen zur **Startseite** finden Sie unter [Die Startseite](#) (Seite 4).

Aus der Protokollseite können Sie das Protokoll in die Zwischenablage kopieren, es per E-Mail versenden oder ausdrucken.

Zum Suchen nach Text im Protokoll klicken Sie auf **Suchen** und geben den gesuchten Text ein.

## 4.6 Web-Schutz

**Wichtig:** Wenn Sophos Endpoint Security and Control über eine Management-Konsole verwaltet wird, werden hier vorgenommene Änderungen eventuell nicht berücksichtigt.

Sophos Anti-Virus bietet mehr Sicherheit vor Threats im Internet: Die Funktion unterbindet 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.

1. Klicken Sie auf **Startseite > Anti-virus und HIPS > Anti-virus und HIPS konfigurieren > Konfigurieren > Web-Schutz**.
2. Aktivieren/deaktivieren Sie im Dialogfeld **Web-Schutz** die Option **Zugriff auf schädliche Websites sperren**. Standardmäßig ist der Zugriff auf eine schädliche Website gesperrt. Nähere Informationen zum Zulassen einer als schädlich eingestuft Website finden Sie unter [Zulassen von Websites](#) (Seite 27).

## 4.7 Zulassen von Objekten

### 4.7.1 Zulassen von Adware und PUA

**Wichtig:** Wenn Sophos Endpoint Security and Control über eine Management-Konsole verwaltet wird, werden hier vorgenommene Änderungen eventuell nicht berücksichtigt.

Wenn Sie Adware oder eine Anwendung ausführen möchten, die von Sophos Anti-Virus als potenziell unerwünscht klassifiziert wurde, können Sie diese Anwendung zulassen.

Verfahren Sie hierzu wie folgt:

1. Klicken Sie auf **Startseite > Anti-virus und HIPS > Anti-virus und HIPS konfigurieren > Konfigurieren > Autorisierung**.
2. Rufen Sie die Registerkarte **Adware/PUA** auf. Wählen Sie die gewünschte Adware/PUA aus der Liste **Bekannte Adware/PUA** aus.
3. Klicken Sie auf **Hinzufügen**.

Die Adware oder PUA wird in der Liste **Zugelassene Adware/PUA** angezeigt.

**Hinweis:** Sie können Adware und PUA auch im Quarantäne-Manager zulassen. Anweisungen hierzu entnehmen Sie bitte dem Abschnitt [Adware und PUA in Quarantäne](#) (Seite 30).

### 4.7.2 Sperren zugelassener Adware und PUA

So lässt sich die Ausführung zugelassener Adware und PUA verhindern:

1. Klicken Sie auf **Startseite > Anti-virus und HIPS > Anti-virus und HIPS konfigurieren > Konfigurieren > Autorisierung**.
2. Rufen Sie die Registerkarte **Adware/PUA** auf. Wählen Sie die gewünschte Adware/PUA aus der Liste **Zugelassene Adware/PUA** aus.
3. Klicken Sie auf **Entfernen**.

### 4.7.3 Zulassen verdächtiger Objekte

**Wichtig:** Wenn Sophos Endpoint Security and Control über eine Management-Konsole verwaltet wird, werden hier vorgenommene Änderungen eventuell nicht berücksichtigt.

Wenn Sie ein Objekt zulassen möchten, das Sophos Anti-Virus als verdächtig eingestuft hat, tun Sie Folgendes:

1. Klicken Sie auf **Startseite > Anti-virus und HIPS > Anti-virus und HIPS konfigurieren > Konfigurieren > Autorisierung**.
2. Klicken Sie auf die Registerkarte, die dem erkannten Objekt entspricht (z.B. **Pufferüberlauf**).
3. Wählen Sie das verdächtige Objekt aus der Liste **bekannter Objekte** aus.
4. Klicken Sie auf **Hinzufügen**.

Das verdächtige Objekt wird in der Liste **Zugelassen** aufgeführt.

**Hinweis:** Sie können verdächtige Objekte auch im Quarantäne-Manager zulassen. Anweisungen hierzu entnehmen Sie bitte den folgenden Abschnitten:

- [Verdächtige Dateien in Quarantäne](#) (Seite 31)
- [Verdächtiges Verhalten in Quarantäne](#) (Seite 33)

#### 4.7.4 Zulassen bestimmter Objekte

Objekte, die Sophos Endpoint Security and Control als verdächtig einstufen könnte, können bereits vorab zugelassen werden.

Verfahren Sie dazu wie folgt:

1. Klicken Sie auf **Startseite > Anti-virus und HIPS > Anti-virus und HIPS konfigurieren > Konfigurieren > Autorisierung**.
2. Klicken Sie auf die Registerkarte, die dem erkannten Objekt entspricht (z.B. **Pufferüberlauf**).
3. Klicken Sie auf **Neuer Eintrag**.
4. Suchen Sie das gewünschte Objekt und doppelklicken Sie darauf.

Das verdächtige Objekt wird in der Liste **Zugelassen** aufgeführt.

#### 4.7.5 Zulassen von Websites

**Wichtig:** Wenn Sophos Endpoint Security and Control über eine Management-Konsole verwaltet wird, werden hier vorgenommene Änderungen eventuell nicht berücksichtigt.

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.



**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.

So lassen Sie eine Website zu:

1. Klicken Sie auf **Startseite > Anti-virus und HIPS > Anti-virus und HIPS konfigurieren > Konfigurieren > Autorisierung**.
2. Klicken Sie auf die Registerkarte **Website**.

3. Klicken Sie auf **Hinzufügen**, um eine Website in einem der verfügbaren Formate hinzuzufügen.

Sie können den Domännennamen, die IP-Adresse oder die IP-Adresse mit Subnetzmaske einer Website hinzufügen.

Die Website wird in der Liste der **zugelassenen Websites** aufgeführt.

## 4.8 Verwalten von Objekten in Quarantäne

### 4.8.1 Allgemeine Informationen

Der Quarantäne-Manager ermöglicht den Umgang mit Objekten, die bei Scans gefunden wurden und nicht automatisch gelöscht wurden. Objekte gelangen aus folgenden Gründe in den Quarantäne-Manager:

- Es wurden keine Bereinigungsoptionen (bereinigen, löschen, verschieben) für den Scan ausgewählt, bei dem das Objekt erkannt wurde.
- Es wurde zwar eine Bereinigungsoption für den Scan ausgewählt, mit dem das Objekt erkannt wurde, dabei ist jedoch ein Problem aufgetreten.
- Das Objekt ist mehrfach infiziert und weist weiterhin Threats auf.
- Es wurde nur ein Threat-Fragment erkannt. Der Threat lässt sich nur über eine vollständige Systemüberprüfung ermitteln. Lesen Sie dazu [Ausführen eines vollständigen Computer-Scans](#) (Seite 17).
- Das Objekt weist verdächtiges Verhalten auf.
- Bei dem Objekt handelt es sich um eine Controlled Application.

**Hinweis:** Bei On-Access-Scans erkannte Adware, PUA und Infektionen mit mehreren Komponenten werden immer im Quarantäne-Manager aufgelistet. Die automatische Bereinigung von Adware, PUAs und Infektionen, die aus mehreren Komponenten bestehen, ist bei On-Access-Scans nicht möglich.

Eine Bereinigungsoption ist möglicherweise aufgrund nicht ausreichender Zugriffsrechte fehlgeschlagen. Wenn Sie über mehr Rechte verfügen, können Sie Objekte über den Quarantäne-Manager bearbeiten.

Beim Scannen von Websites erkannte Threats werden nicht im Quarantäne-Manager aufgeführt, da die Threats nicht auf Ihren Computer heruntergeladen werden. Aus diesem Grund sind keine Maßnahmen erforderlich.

## 4.8.2 Viren/Spyware in Quarantäne

**Hinweis:** In diesem Zusammenhang wird *Virus* für Viren, Würmer, Trojaner oder andere schädliche Software verwendet.

1. Klicken Sie auf der **Startseite** im Bereich **Antivirus und HIPS** auf **Quarantäne-Objekte verwalten**.

Weitere Informationen zur **Startseite** finden Sie unter [Die Startseite](#) (Seite 4).

2. Wählen Sie im Dropdown-Menü **Anzeigen** die Option **Viren/Spyware** aus.

In den Spalten werden Informationen zu allen Objekten angezeigt.

Im Bereich **Name** wird das von Sophos Anti-Virus erkannte Objekt angezeigt. Um mehr über Viren/Spyware zu erfahren, klicken Sie auf den Namen, woraufhin Sophos Anti-Virus Sie zu der Analyse der Viren/Spyware auf der Sophos Website leitet.

Im Bereich **Details** werden der Name und der Speicherort des Objekts angezeigt. Wenn ein Objekt mit einem Rootkit in Zusammenhang steht, wird es als „Versteckt“ angezeigt. Wenn neben dem Objektnamen der Link [**mehr**] angezeigt wird, bedeutet dies, dass das Objekt durch eine Infektion mit mehreren Komponenten infiziert wurde. Klicken Sie auf den Link, um eine Liste der Komponenten zu sehen, die zu der Infektion gehören. Wenn eine der Komponenten mit einem Rootkit in Zusammenhang steht, wird sie im Dialogfeld als „Versteckt“ angezeigt.

Im Bereich **Verfügbare Maßnahmen** werden die Maßnahmen angezeigt, die für das Objekt ergriffen werden können. Wenn das Objekt nicht versteckt ist, stehen drei Maßnahmen zur Auswahl: Bereinigen, Löschen und Verschieben (siehe unten). Wenn Sie auf eine der Maßnahmen klicken, wird sie für das Objekt nach der Bestätigung ausgeführt. Versteckte Dateien können nur bereinigt werden.

### Vorgehensweise

Die folgenden Optionen stehen zur Auswahl:

#### Alles markieren/Aufheben

Klicken Sie auf diese Schaltflächen, um alle Objekte auszuwählen oder von der Auswahl auszunehmen. Somit können Sie dieselbe Maßnahme für eine Gruppe von Objekten durchführen. Um ein bestimmtes Objekt auszuwählen oder von der Auswahl auszunehmen, klicken Sie auf das Kontrollkästchen links neben dem Objektnamen.

#### Entfernen

Klicken Sie auf diese Schaltfläche, um markierte Objekte aus der Liste zu entfernen, wenn Sie sicher sind, dass sie keine Viren/Spyware enthalten. Dadurch werden die Objekte jedoch nicht von der Festplatte gelöscht.

#### Maßnahme durchführen

Klicken Sie darauf, um die verfügbaren Maßnahmen anzuzeigen, die für die ausgewählten Objekte ergriffen werden können.

- Klicken Sie auf **Bereinigen**, um einen Virus oder Spyware aus ausgewählten Objekten zu entfernen. Durch die Bereinigung von Dokumenten werden keine durch Viren entstandene Schäden rückgängig gemacht.

**Hinweis:** Um einige Viren bzw. Spywareobjekte, die aus mehreren Komponenten bestehen, vollständig von Ihrem Computer zu beseitigen, müssen Sie den Computer neu starten. Sie können bestimmen, ob der Neustart sofort oder später erfolgen soll. Die abschließenden Bereinigungs-schritte werden nach dem Neustart durchgeführt.

- Klicken Sie auf **Löschen**, um ausgewählte Objekte von Ihrem Computer zu löschen. Verwenden Sie diese Funktion mit großer Sorgfalt.
- Klicken Sie auf **Verschieben nach**, um markierte Objekte in einen anderen Ordner zu verschieben. Die Objekte werden in den Ordner verschoben, der angegeben wurde, als die Bereinigung eingerichtet wurde. Das Verschieben einer ausführbaren Datei senkt das Risiko, dass diese Datei gestartet wird. Verwenden Sie diese Funktion mit großer Sorgfalt.



**Vorsicht:** Wenn Sie eine infizierte Datei löschen oder verschieben, kann es sein, dass Ihr Computer nicht mehr richtig funktioniert, da er die Datei nicht finden kann. Außerdem kann eine infizierte Datei Teil einer Mehrfachinfektion sein, weshalb das Löschen oder Verschieben dieser Datei nicht die Infektion von Ihrem Computer entfernt. Kontaktieren Sie in diesem Falle den technischen Support von Sophos für Unterstützung bei der Handhabung der Objekte.

Im Abschnitt [Technischer Support](#) (Seite 98) wird erläutert, wie Sie Kontakt zum technischen Support aufnehmen können.

Anweisungen zur Konfiguration der zu ergreifenden Maßnahme entnehmen Sie bitte dem Abschnitt [Konfigurieren der Benutzerrechte für den Quarantäne-Manager](#) (Seite 7).

### 4.8.3 Adware und PUA in Quarantäne

1. Klicken Sie auf der **Startseite** im Bereich **Antivirus und HIPS** auf **Quarantäne-Objekte verwalten**.

Weitere Informationen zur **Startseite** finden Sie unter [Die Startseite](#) (Seite 4).

2. Wählen Sie im Dropdown-Menü **Anzeigen** die Option **Adware/PUA** aus.

In den Spalten werden Informationen zu allen Objekten angezeigt.

Im Bereich **Name** wird das von Sophos Anti-Virus erkannte Objekt angezeigt. Um mehr über die Adware oder PUA zu erfahren, klicken Sie auf den Namen, woraufhin Sophos Anti-Virus Sie zu der Analyse der Adware oder PUA auf der Sophos Website leitet.

**Details** zeigt den Subtyp der Adware oder PUA an. Wenn ein Objekt mit einem Rootkit in Zusammenhang steht, wird es als „Versteckt“ angezeigt. Wenn neben dem Subtyp ein **[mehr]**-Link erscheint, bedeutet dies, dass das Objekt Teil einer Adware/PUA mit mehreren Komponenten ist. Klicken Sie auf den Link, um eine Liste der Komponenten zu sehen, die zu der Adware oder PUA gehören. Wenn eine der Komponenten mit einem Rootkit in Zusammenhang steht, wird sie im Dialogfeld als „Versteckt“ angezeigt.

Im Bereich **Verfügbare Maßnahmen** werden die Maßnahmen angezeigt, die für das Objekt ergriffen werden können. Es gibt zwei Maßnahmen: Zulassen und Bereinigen (siehe unten). Wenn Sie auf eine der Maßnahmen klicken, wird sie für das Objekt nach der Bestätigung ausgeführt.

## Vorgehensweise

Die folgenden Optionen stehen zur Verfügung:

### Alles markieren/Aufheben

Klicken Sie auf diese Schaltflächen, um alle Objekte auszuwählen oder von der Auswahl auszunehmen. Somit können Sie dieselbe Maßnahme für eine Gruppe von Objekten durchführen. Um ein bestimmtes Objekt auszuwählen oder von der Auswahl auszunehmen, klicken Sie auf das Kontrollkästchen links neben dem Objektnamen.

### Entfernen

Klicken Sie auf diese Schaltfläche, um die ausgewählten Objekte aus der Liste zu entfernen. Dadurch werden die Objekte jedoch nicht von der Festplatte gelöscht.

### Maßnahme durchführen

Klicken Sie darauf, um die verfügbaren Maßnahmen anzuzeigen, die für die ausgewählten Objekte ergriffen werden können.

- Klicken Sie auf **Zulassen**, um ausgewählte Objekte auf dem Computer zuzulassen. Auf diese Weise werden die Objekte zur Liste erlaubter Adware und PUA hinzugefügt, damit Sophos Anti-Virus die Ausführung auf dem Computer nicht verhindert.
- Klicken Sie auf **Bereinigen**, um alle bekannten Komponenten ausgewählter Objekte von dem Computer für alle Anwender zu entfernen. Nur Mitglieder der Gruppen „Windows Administrators“ und „SophosAdministrator“ können Adware und PUA vom Computer entfernen.

**Hinweis:** Zur vollständigen Bereinigung von Adware und PUA, die sich aus mehreren Komponenten zusammensetzen, und versteckten Dateien ist unter Umständen ein Neustart erforderlich. Sie können bestimmen, ob der Neustart sofort oder später erfolgen soll. Die abschließenden Bereinigungsschritte werden nach dem Neustart durchgeführt.

Anweisungen zur Konfiguration der zu ergreifenden Maßnahmen entnehmen Sie bitte dem Abschnitt [Konfigurieren der Benutzerrechte für den Quarantäne-Manager](#) (Seite 7).

Zur Anzeige der Liste bekannter und zugelassener Adware und PUA klicken Sie auf **Autorisierung konfigurieren**.

## 4.8.4 Verdächtige Dateien in Quarantäne

Unter einer *verdächtigen Datei* ist eine Datei zu verstehen, die Virenmerkmale aufweist.

1. Klicken Sie auf der **Startseite** im Bereich **Antivirus und HIPS** auf **Quarantäne-Objekte verwalten**.

Weitere Informationen zur **Startseite** finden Sie unter [Die Startseite](#) (Seite 4).

2. Wählen Sie im Dropdown-Menü **Anzeigen** die Option **Verdächtige Dateien** aus.

In den Spalten werden Informationen zu allen Objekten angezeigt.

Im Bereich **Name** wird das von Sophos Anti-Virus erkannte Objekt angezeigt. Um mehr über die verdächtige Datei zu erfahren, klicken Sie auf den Namen, woraufhin Sophos Anti-Virus Sie zu der Analyse der verdächtigen Datei auf der Sophos Website leitet.

Im Bereich **Details** werden der Name und der Speicherort des Objekts angezeigt. Wenn ein Objekt mit einem Rootkit in Zusammenhang steht, wird es als „Versteckt“ angezeigt.

Im Bereich **Verfügbare Maßnahmen** werden die Maßnahmen angezeigt, die für das Objekt ergriffen werden können. Wenn das Objekt nicht versteckt ist, stehen drei Maßnahmen zur Auswahl: Zulassen, Löschen und Verschieben (siehe unten). Wenn Sie auf eine der Maßnahmen klicken, wird sie für das Objekt nach der Bestätigung ausgeführt. Versteckte Dateien können nur zugelassen werden.

### Vorgehensweise

Folgende Optionen stehen zur Auswahl:

#### Alles markieren/Aufheben

Klicken Sie auf diese Schaltflächen, um alle Objekte auszuwählen oder von der Auswahl auszunehmen. Somit können Sie dieselbe Maßnahme für eine Gruppe von Objekten durchführen. Um ein bestimmtes Objekt auszuwählen oder von der Auswahl auszunehmen, klicken Sie auf das Kontrollkästchen links neben dem Objektnamen.

#### Entfernen

Klicken Sie auf diese Schaltfläche, um die ausgewählten Objekte aus der Liste zu entfernen. Dadurch werden die Objekte jedoch nicht von der Festplatte gelöscht.

#### Maßnahme durchführen

Klicken Sie darauf, um die verfügbaren Maßnahmen anzuzeigen, die für die ausgewählten Objekte ergriffen werden können.

- Klicken Sie auf **Zulassen**, um ausgewählte Objekte auf dem Computer zuzulassen. Auf diese Weise werden die Objekte zur Liste erlaubter verdächtiger Objekte hinzugefügt, damit Sophos Anti-Virus den Zugriff auf sie nicht verhindert.
- Klicken Sie auf **Löschen**, um ausgewählte Objekte von Ihrem Computer zu löschen. Verwenden Sie diese Funktion mit großer Sorgfalt.
- Klicken Sie auf **Verschieben nach**, um markierte Objekte in einen anderen Ordner zu verschieben. Die Objekte werden in den Ordner verschoben, der angegeben wurde, als die Bereinigung eingerichtet wurde. Das Verschieben einer ausführbaren Datei senkt das Risiko, dass diese Datei gestartet wird. Verwenden Sie diese Funktion mit großer Sorgfalt.



**Vorsicht:** Wenn Sie eine infizierte Datei löschen oder verschieben, kann es sein, dass Ihr Computer nicht mehr richtig funktioniert, da er die Datei nicht finden kann.

Anweisungen zur Konfiguration der zu ergreifenden Maßnahmen entnehmen Sie bitte dem Abschnitt [Konfigurieren der Benutzerrechte für den Quarantäne-Manager](#) (Seite 7).

Um eine Liste erlaubter verdächtiger Dateien anzusehen, klicken Sie auf **Autorisierung konfigurieren**.

## 4.8.5 Verdächtiges Verhalten in Quarantäne

*Verdächtiges Verhalten* bezeichnet eine scheinbar schädliche Aktivität.

1. Klicken Sie auf der **Startseite** im Bereich **Antivirus und HIPS** auf **Quarantäne-Objekte verwalten**.  
Weitere Informationen zur **Startseite** finden Sie unter [Die Startseite](#) (Seite 4).
2. Wählen Sie im Dropdown-Menü **Anzeigen** die Option **Verdächtiges Verhalten** aus.

In den Spalten werden Informationen zu allen Objekten angezeigt.

Im Bereich **Name** wird das von Sophos Anti-Virus erkannte Objekt angezeigt. Um mehr über das Verhalten zu erfahren, klicken Sie auf den Namen, woraufhin Sophos Anti-Virus Sie zu der Analyse des Verhaltens auf der Sophos Website leitet.

Im Bereich **Details** werden der Name und der Speicherort des Objekts angezeigt.

Im Bereich **Verfügbare Maßnahmen** werden die Maßnahmen angezeigt, die für das Objekt ergriffen werden können. Wenn Sie das Sperren verdächtigen Verhaltens aktiviert haben, gibt es nur eine Maßnahme: Zulassen (siehe unten). Wenn Sie auf die Maßnahme klicken, wird sie für das Objekt nach der Bestätigung ausgeführt.

### Vorgehensweise

Folgende Optionen stehen zur Verfügung:

#### Alles markieren/Aufheben

Klicken Sie auf diese Schaltflächen, um alle Objekte auszuwählen oder von der Auswahl auszunehmen. Somit können Sie dieselbe Maßnahme für eine Gruppe von Objekten durchführen. Um ein bestimmtes Objekt auszuwählen oder von der Auswahl auszunehmen, klicken Sie auf das Kontrollkästchen links neben dem Objektnamen.

#### Entfernen

Klicken Sie auf diese Schaltfläche, um die ausgewählten Objekte aus der Liste zu entfernen. Dadurch werden die Objekte jedoch nicht von der Festplatte gelöscht.

#### Maßnahme durchführen

Klicken Sie darauf, um die verfügbaren Maßnahmen anzuzeigen, die für die ausgewählten Objekte ergriffen werden können.

- Klicken Sie auf **Zulassen**, um ausgewählte Objekte auf dem Computer zuzulassen. Auf diese Weise werden die Objekte zur Liste erlaubter verdächtiger Objekte hinzugefügt, damit Sophos Anti-Virus den Zugriff auf sie nicht verhindert.

Anweisungen zur Konfiguration der zu ergreifenden Maßnahmen entnehmen Sie bitte dem Abschnitt [Konfigurieren der Benutzerrechte für den Quarantäne-Manager](#) (Seite 7).

Um eine Liste erlaubter verdächtiger Dateien anzusehen, klicken Sie auf **Autorisierung konfigurieren**.

## 4.8.6 Controlled Applications in Quarantäne

*Controlled Applications* sind Anwendungen, deren Ausführung durch die Sicherheitsrichtlinie des Unternehmens unterbunden wird.

1. Klicken Sie auf der **Startseite** im Bereich **Antivirus und HIPS** auf **Quarantäne-Objekte verwalten**.

Weitere Informationen zur **Startseite** finden Sie unter [Die Startseite](#) (Seite 4).

2. Wählen Sie im Dropdown-Menü **Anzeigen** die Option **Controlled Applications** aus.

In den Spalten werden Informationen zu allen Objekten angezeigt.

Im Bereich **Name** wird das von Sophos Anti-Virus erkannte Objekt angezeigt. Um mehr über die Controlled Application zu erfahren, klicken Sie auf den Namen, woraufhin Sophos Anti-Virus Sie zu der Analyse der Controlled Application auf der Sophos Website leitet.

Im Bereich **Details** wird der Subtyp der Controlled Application angezeigt. Wird ein **[mehr]**-Link neben dem Subtyp angezeigt, können Sie auf ihn klicken, um eine Liste anderer Komponenten anzusehen, die Teil der Controlled Application sind.

Im Bereich **Verfügbare Maßnahmen** werden die Maßnahmen angezeigt, die für das Objekt ergriffen werden können. Das Entfernen des Objekts aus der Liste ist die einzige Maßnahme, die für Controlled Applications ergriffen werden kann, und wird nachfolgend beschrieben.

### Vorgehensweise

Die folgenden Optionen stehen zur Verfügung:

#### Alles markieren/Aufheben

Klicken Sie auf diese Schaltflächen, um alle Objekte auszuwählen oder von der Auswahl auszunehmen. Somit können Sie dieselbe Maßnahme für eine Gruppe von Objekten durchführen. Um ein bestimmtes Objekt auszuwählen oder von der Auswahl auszunehmen, klicken Sie auf das Kontrollkästchen links neben dem Objektname.

#### Entfernen

Klicken Sie darauf, um ausgewählte Objekte von der Liste zu entfernen. Dadurch werden die Objekte jedoch nicht von der Festplatte gelöscht. Controlled Applications müssen von der zentralen Konsole erlaubt werden, bevor sie Sie verwenden können.

## 4.9 Konfigurieren von Alerts

### 4.9.1 Desktop-Benachrichtigungen

**Wichtig:** Wenn Sophos Endpoint Security and Control über eine Management-Konsole verwaltet wird, werden hier vorgenommene Änderungen eventuell nicht berücksichtigt.

Bei Auswahl dieser Option zeigt Sophos Anti-Virus Desktop-Benachrichtigungen an, wenn ein Threat gefunden wurde. Die Option beschränkt sich auf On-Access-Scans.

1. Klicken Sie auf **Startseite > Anti-virus und HIPS > Anti-virus und HIPS konfigurieren > Alerts > Benachrichtigungen** .
2. Klicken Sie im Dialogfeld **Benachrichtigungen** auf die Registerkarte **Desktop-Benachrichtigungen**. Nehmen Sie die folgenden Einstellungen vor:

#### **Aktivieren der Desktop-Benachrichtigung**

Wählen Sie diese Option, damit Sophos Anti-Virus Desktop-Benachrichtigungen anzeigt, wenn ein Threat gefunden wurde.

#### **Bei folgenden Ereignissen eine Benachrichtigung senden**

Wählen Sie die Ereignisse, bei denen Sophos Anti-Virus Desktop-Benachrichtigungen anzeigen soll.

#### **Benutzerdefinierte Nachricht**

In dieses Textfeld können Sie eine Nachricht eingeben, die an das Ende der Standard-Nachricht angefügt wird.

## **4.9.2 Konfigurieren von E-Mail-Benachrichtigungen**

**Wichtig:** Wenn Sophos Endpoint Security and Control über eine Management-Konsole verwaltet wird, werden hier vorgenommene Änderungen eventuell nicht berücksichtigt.

Damit Sophos Anti-Virus beim Erkennen eines Threats oder Auftreten eines Fehlers E-Mail-Benachrichtigungen senden kann, gehen Sie folgendermaßen vor: Die Anweisungen gelten für On-Access-Scans, On-Demand-Scans und Rechtsklick-Scans.

1. Klicken Sie auf **Startseite > Anti-virus und HIPS > Anti-virus und HIPS konfigurieren > Alerts > Benachrichtigungen** .

2. Klicken Sie im Dialogfeld **Benachrichtigung** auf die Registerkarte **E-Mail-Benachrichtigung**. Nehmen Sie die folgenden Einstellungen vor:

#### **E-Mail-Benachrichtigung aktivieren**

Wählen Sie diese Option aus, wenn Sophos Anti-Virus E-Mail-Benachrichtigungen senden soll.

#### **Bei folgenden Ereignissen eine Benachrichtigung senden**

Wählen Sie die Ereignisse, bei denen Sophos Anti-Virus E-Mail-Benachrichtigungen senden soll. Ein **Scan-Fehler** liegt beispielsweise auch dann vor, wenn Sophos Anti-Virus auf ein Objekt nicht zugreifen konnte.

Sophos Anti-Virus sendet keine E-Mail-Benachrichtigungen über Threats, die beim Scannen von Websites erkannt wurden, da diese Threats nicht auf Ihren Computer heruntergeladen werden. Aus diesem Grund sind keine Maßnahmen erforderlich.

#### **Empfänger**

Klicken Sie auf **Hinzufügen** oder **Entfernen**, um E-Mail-Adressen hinzuzufügen oder zu entfernen, an die die Benachrichtigungen gesendet werden sollen. Klicken Sie auf **Bearbeiten**, um eine hinzugefügte E-Mail-Adresse zu ändern.

#### **SMTP konfigurieren**

Klicken Sie auf diese Schaltfläche, um die Einstellungen für den SMTP-Server und die Sprache der E-Mail-Benachrichtigungen zu ändern. (Siehe folgende Tabelle.)

<b>Konfigurieren der SMTP-Einstellungen</b>	
<b>SMTP-Server</b>	Geben Sie in das Textfeld den Hostnamen oder die IP-Adresse des SMTP-Servers ein. Klicken Sie auf <b>Test</b> , um zu prüfen, ob eine Verbindung zum SMTP-Server hergestellt werden kann. (Dadurch wird <i>keine</i> Test-E-Mail gesendet.)
<b>SMTP-Senderadresse</b>	Geben Sie in das Textfeld eine E-Mail-Adresse ein, an die nicht zustellbare Benachrichtigungen und Nicht-Zustellbarkeitsmeldungen gesendet werden können.
<b>SMTP-Antwortadresse</b>	Da E-Mail-Benachrichtigungen von einem Systemkonto gesendet werden, können Sie in das Textfeld eine E-Mail-Adresse eingeben, an die Antworten auf E-Mail-Benachrichtigungen gesendet werden können.
<b>Sprache</b>	Klicken Sie auf den Drop-Down-Pfeil und wählen Sie die Sprache, in der die E-Mail-Benachrichtigungen gesendet werden sollen.

### 4.9.3 Konfigurieren von SNMP-Benachrichtigungen

**Wichtig:** Wenn Sophos Endpoint Security and Control über eine Management-Konsole verwaltet wird, werden hier vorgenommene Änderungen eventuell nicht berücksichtigt.

Im Folgenden wird die Einrichtung von SNMP-Benachrichtigungen beschrieben. Die Anweisungen gelten für On-Access-Scans, On-Demand-Scans und Rechtsklick-Scans.

1. Klicken Sie auf **Startseite > Anti-virus und HIPS > Anti-virus und HIPS konfigurieren > Alerts > Benachrichtigungen** .
2. Klicken Sie im Dialogfeld **Benachrichtigungen** auf die Registerkarte **SNMP-Benachrichtigungen**. Nehmen Sie die folgenden Einstellungen vor:

#### **SNMP-Benachrichtigungen aktivieren**

Aktivieren Sie diese Option, wenn Sophos Anti-Virus SNMP-Benachrichtigungen senden soll.

#### **Bei folgenden Ereignissen eine Benachrichtigung senden**

Wählen Sie in diesem Bereich die auslösenden Ereignisse für das Senden einer SNMP-Benachrichtigung aus. Ein **Scan-Fehler** liegt beispielsweise auch dann vor, wenn Sophos Anti-Virus auf ein Objekt nicht zugreifen konnte.

Sophos Anti-Virus sendet keine SNMP-Benachrichtigungen über Bedrohungen, die beim Scannen von Websites erkannt wurden, da diese Bedrohungen nicht auf Ihren Computer heruntergeladen werden. Aus diesem Grund sind keine Maßnahmen erforderlich.

#### **SNMP-Trapziel**

Geben Sie in das Textfeld die IP-Adresse oder den Namen des Computers ein, an den die Benachrichtigungen gesendet werden.

#### **SNMP-Community**

Geben Sie in das Textfeld den Namen der SNMP-Community ein.

#### **Test**

Klicken Sie auf diese Schaltfläche, um eine Test-SNMP-Benachrichtigung an das von Ihnen angegebene Ziel der SNMP-Trap zu senden.

### 4.9.4 Ereignis-Protokollierung

Gehen Sie folgendermaßen vor, damit Sophos Anti-Virus Benachrichtigungen zum Ereignisprotokoll von Windows 2000 oder höher hinzufügen kann, wenn ein Threat entdeckt wurde oder ein Fehler aufgetreten ist. Die Anweisungen gelten für On-Access-Scans, On-Demand-Scans und Rechtsklick-Scans.

1. Klicken Sie auf **Startseite > Anti-virus und HIPS > Anti-virus und HIPS konfigurieren > Alerts > Benachrichtigungen** .

2. Klicken Sie im Dialogfeld **Benachrichtigung** auf die Registerkarte **Ereignisprotokoll**. Nehmen Sie die folgenden Einstellungen vor:

#### **Ereignisprotokoll aktivieren**

Wählen Sie diese Option, damit Sophos Anti-Virus Benachrichtigungen an das Windows-Ereignisprotokoll sendet.

#### **Bei folgenden Ereignissen eine Benachrichtigung senden**

Wählen Sie die Ereignisse, bei denen Sophos Anti-Virus Benachrichtigungen senden soll. Ein **Scan-Fehler** liegt beispielsweise auch dann vor, wenn Sophos Anti-Virus auf ein Objekt nicht zugreifen konnte.

Sophos Anti-Virus sendet keine Benachrichtigungen über Threats, die beim Scannen von Websites erkannt wurden, da diese Threats nicht auf Ihren Computer heruntergeladen werden. Aus diesem Grund sind keine Maßnahmen erforderlich.

## 4.10 Scan-Protokoll

### 4.10.1 Konfigurieren des Scan-Protokolls

Das Scan-Protokoll des Computers befindet sich unter:

```
C:\Dokumente und Einstellungen\All
Users\Anwendungsdaten\Sophos\Sophos
Anti-Virus\logs\SAV.txt
```

1. Klicken Sie auf **Startseite > Anti-virus und HIPS > Anti-virus und HIPS-Protokoll > Protokoll konfigurieren**.
2. Aktivieren Sie im Dialogfeld **Protokoll für diesen Computer konfigurieren** die nachfolgend beschriebenen Optionen.

#### **Protokollgrad**

Um nichts mehr zu protokollieren, klicken Sie auf **Keines**. Bei Auswahl der Option **Normal** werden Zusammenfassungen, Fehlermeldungen usw. protokolliert. Bei Auswahl der Option **Ausführlich** wird ein umfassendes Protokoll mit Angaben zu den gescannten Dateien, Hauptabschnitten eines Scans usw. erstellt.

#### **Protokollarchiv**

Um die Protokolldatei monatlich zu archivieren, wählen Sie **Archiv aktivieren**. Die Archivdateien werden im selben Ordner wie die Protokolldatei gespeichert. Legen Sie unter **Anzahl der Archivdateien** fest, wie viele Archivdateien maximal erstellt werden können, bevor jeweils die älteste Datei gelöscht wird. Wählen Sie **Protokoll komprimieren**, um die Größe der Protokolldatei zu reduzieren.

### 4.10.2 Öffnen des Scan-Protokolls

- ❖ Klicken Sie auf der **Startseite** unter **Antivirus und HIPS** auf **Antivirus- und HIPS-Protokoll öffnen**.

Weitere Informationen zur **Startseite** finden Sie unter [Die Startseite](#) (Seite 4).

Aus der Protokollseite können Sie das Protokoll in die Zwischenablage kopieren, es per E-Mail versenden oder ausdrucken.

Wenn Sie im Protokoll bestimmten Text suchen, klicken Sie auf **Suchen** und geben Sie den gewünschten Text in das Suchfeld ein.

## 4.11 Bereinigung

### 4.11.1 Allgemeine Informationen

Durch eine Bereinigung werden Threats vom Computer entfernt. Dabei wird eine der folgenden Aktionen durchgeführt:

- Entfernen eines Virus aus einer Datei oder dem Bootsektor
- Verschieben oder Löschen einer verdächtigen Datei
- Löschen einer Adware oder PUA

Von Threats bereits durchgeführte Maßnahmen werden jedoch nicht rückgängig gemacht.

Durch die Bereinigung von Dokumenten werden keine Änderungen durch den Virus rückgängig gemacht.

Die Bereinigung von Programmen sollte nur als temporäre Maßnahme zum Einsatz kommen. Ersetzen Sie die bereinigten Programme durch eine Kopie vom Original-Datenträger oder eine virenfreie Sicherungskopie.

Threats, die beim Scannen von Websites erkannt wurden, werden nicht bereinigt, da sie nicht auf Ihren Computer heruntergeladen werden. Aus diesem Grund müssen in diesem Falle keine Maßnahmen ergriffen werden.

### 4.11.2 Automatisches Bereinigen von Viren/Spyware

**Wichtig:** Wenn Sophos Endpoint Security and Control über eine Management-Konsole verwaltet wird, werden hier vorgenommene Änderungen eventuell nicht berücksichtigt.

Wenn On-Access-Scans aktiviert wurden oder wenn ein On-Demand- oder Rechtsklick-Scan ausgeführt wird, erfüllt Sophos Anti-Virus automatisch folgende Funktionen:

- Bereinigung der meisten infizierten Objekte
- Sicherung infizierter Objekte auf andere Weise

**Hinweis:** Eine automatische Bereinigung von Bedrohungen mit verschiedenen Komponenten steht für On-Access-Scans nicht zur Verfügung. Um Infektionen mit mehreren Komponenten von Ihrem Computer zu entfernen, verwenden Sie den Quarantäne-Manager. Der Quarantäne-Manager wird im Abschnitt [Adware und PUA in Quarantäne](#) (Seite 30) beschrieben.

Alle Maßnahmen, die Sophos Anti-Virus bei infizierten Objekten ergreift, werden im Protokoll für diesen Computer oder im Protokoll für On-Demand-Scans erfasst. Nähere Informationen

hierzu finden Sie unter [Öffnen des Scan-Protokolls](#) (Seite 38) oder [Öffnen des Protokolls](#) (Seite 21).

Um einige Infektionen, die aus mehreren Komponenten bestehen, vollständig von Ihrem Computer zu entfernen, müssen Sie den Computer neu starten. Sie können bestimmen, ob der Neustart sofort oder später erfolgen soll. Die abschließenden Bereinigungs Schritte werden nach dem Neustart durchgeführt.

1. Öffnen Sie die Einstellungen des zu konfigurierenden Scans. Entsprechende Anweisungen hierzu enthalten Sie über einen der folgenden Links:

- [Konfigurieren von On-Access-Scans](#) (Seite 8)
- [Konfigurieren von Rechtsklick-Scans](#) (Seite 18)
- [Konfigurieren eines individuellen Scans](#) (Seite 19)

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

3. Wählen Sie im Bereich **Viren/Spyware** die Option **Infizierte Objekte automatisch bereinigen**, wenn Sophos Anti-Virus infizierte Disketten-Bootsektoren, Dokumente, Programme und sonstige Objekte sofort bereinigen soll.

Durch die Bereinigung von Dokumenten werden keine durch Viren entstandene Schäden rückgängig gemacht. (Unter [Bereinigungs-Details](#) (Seite 42) erfahren Sie, wo Sie auf der Sophos Website Näheres zu den Folgeerscheinungen der entsprechenden Viren finden können.)

4. Sophos Anti-Virus kann infizierte Dateien auch auf andere Weise bereinigen. Sie können andere Maßnahmen wählen, die Sophos Anti-Virus bei infizierten Dateien durchführen soll, wenn eine automatische Bereinigung nicht erwünscht ist oder fehlschlägt:

- Klicken Sie auf **Zugriff verweigern**, damit Dateien nicht geöffnet, kopiert oder verschoben werden.
- Klicken Sie auf **Löschen**, um die Datei zu beseitigen.
- Klicken Sie auf **Zugriff verweigern und verschieben nach**, um die Datei in einen anderen Ordner zu verschieben, den Sie über **Durchsuchen** auswählen können.

Das Verschieben einer ausführbaren Datei senkt das Risiko, dass diese Datei gestartet wird.

Eine Infektion mit mehreren Komponenten kann nicht automatisch verschoben werden.



**Vorsicht:** Diese Optionen sollten Sie nur nach Rücksprache mit dem technischen Support von Sophos verwenden. Ansonsten können Sie von Sophos Anti-Virus erkannte Viren/Spyware über den Quarantäne-Manager von Ihrem Computer entfernen. Der Quarantäne-Manager wird im Abschnitt [Adware und PUA in Quarantäne](#) (Seite 30) beschrieben.

**Hinweis:** Im Abschnitt [Viren/Spyware in Quarantäne](#) (Seite 29) wird die Entfernung von Viren/Spyware über den Quarantäne-Manager beschrieben.

### 4.11.3 Automatisches Bereinigen von Adware und PUA

Bei On-Demand- und Rechtsklick-Scans ist eine automatische Entfernung von Adware und PUA möglich.

**Hinweis:** Die automatische Entfernung von Adware und PUA ist über On-Access-Scans nicht möglich. Verwenden Sie in diesem Fall den Quarantäne-Manager. Der Quarantäne-Manager wird im Abschnitt [Adware und PUA in Quarantäne](#) (Seite 30) beschrieben.

Alle Maßnahmen, die Sophos Anti-Virus gegen Adware und PUA ergreift, werden im Protokoll für diesen Computer oder im Protokoll für die On-Demand-Scans erfasst. Nähere Informationen hierzu finden Sie unter [Öffnen des Scan-Protokolls](#) (Seite 38) oder [Öffnen des Protokolls](#) (Seite 21).

Da Adware und PUA aus mehreren Komponenten bestehen kann, muss zur vollständigen Entfernung der Computer neu gestartet werden. Sie können bestimmen, ob der Neustart sofort oder später erfolgen soll. Die abschließenden Bereinigungs Schritte werden nach dem Neustart durchgeführt.

1. Öffnen Sie die Einstellungen des zu konfigurierenden Scans. Entsprechende Anweisungen hierzu enthalten Sie über einen der folgenden Links:
  - [Konfigurieren von On-Access-Scans](#) (Seite 8)
  - [Konfigurieren von Rechtsklick-Scans](#) (Seite 18)
  - [Konfigurieren eines individuellen Scans](#) (Seite 19)
2. Klicken Sie auf die Registerkarte **Bereinigung**.
3. Wählen Sie im Bereich **Adware und PUA** die Option **Adware/PUA automatisch bereinigen**, damit Sophos Anti-Virus alle bekannten Adware- und PUA-Komponenten für alle Anwender vom Computer entfernen kann.

Die Bereinigung macht keine Änderungen rückgängig, die von der Adware/PUA bereits vorgenommen wurden. (Unter [Bereinigungs-Details](#) (Seite 42) erfahren Sie, wo Sie auf der Sophos Website Näheres zu den Folgeerscheinungen der entsprechenden Adware/PUA finden können.)

**Hinweis:** Im Abschnitt [Adware und PUA in Quarantäne](#) (Seite 30) wird die Entfernung von Adware und PUA über den Quarantäne-Manager beschrieben.

### 4.11.4 Automatisches Bereinigen verdächtiger Dateien

**Wichtig:** Wenn Sophos Endpoint Security and Control über eine Management-Konsole verwaltet wird, werden hier vorgenommene Änderungen eventuell nicht berücksichtigt.

Bei On-Access-, On-Demand- und Rechtsklick-Scans kann Sophos Anti-Virus verdächtige Dateien automatisch löschen oder verschieben.

Unter einer *verdächtigen Datei* ist eine Datei zu verstehen, die Virenmerkmale aufweist.

1. Öffnen Sie die Einstellungen des zu konfigurierenden Scans. Entsprechende Anweisungen hierzu enthalten Sie über einen der folgenden Links:

- [Konfigurieren von On-Access-Scans](#) (Seite 8)
- [Konfigurieren von Rechtsklick-Scans](#) (Seite 18)
- [Konfigurieren eines individuellen Scans](#) (Seite 19)

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

3. Wählen Sie im Bereich **Verdächtige Dateien** die unten beschriebenen Optionen aus.

- Klicken Sie auf **Zugriff verweigern**, damit Dateien nicht geöffnet, kopiert oder verschoben werden.
- Klicken Sie auf **Löschen**, um die Datei zu beseitigen.
- Klicken Sie auf **Zugriff verweigern und verschieben nach**, um die Datei in einen anderen Ordner zu verschieben, den Sie über **Durchsuchen** auswählen können. Das Verschieben einer ausführbaren Datei senkt das Risiko, dass diese Datei gestartet wird.



**Vorsicht:** Diese Optionen sollten Sie nur nach Rücksprache mit dem technischen Support von Sophos verwenden. Ansonsten können Sie von Sophos Anti-Virus erkannte Viren/Spyware über den Quarantäne-Manager von Ihrem Computer entfernen. Der Quarantäne-Manager wird im Abschnitt [Verdächtige Dateien in Quarantäne](#) (Seite 31) beschrieben.

**Hinweis:** Im Abschnitt [Verdächtige Dateien in Quarantäne](#) (Seite 31) wird die Entfernung von verdächtigen Dateien über den Quarantäne-Manager beschrieben.

#### 4.11.5 Bereinigungs-Details

Wenn Threats auf Ihrem Computer erkannt werden, empfiehlt sich, die zugehörige Analyse und die Bereinigungshinweise auf der Sophos Website zu Rate zu ziehen. Sie können diese Daten über die folgenden Komponenten abrufen:

- Desktop-Benachrichtigungen (On-Access-Scans)
- Scanfortschrittsfenster (On-Demand- und Rechtsklick-Scans)
- Quarantäne-Manager (alle Scan-Arten)

##### **Abrufen von Threat-Details über Desktop-Benachrichtigungen**

Wenn die On-Access-Scanfunktion auf Ihrem Computer aktiviert ist, wird eine Desktop-Benachrichtigung angezeigt, wenn Sophos Anti-Virus einen Threat erkennt. Klicken Sie im Meldungsfenster auf den Namen des Threats, über den Sie mehr erfahren möchten.

Sophos Anti-Virus stellt eine Verbindung zur Threat-Analyse auf der Sophos Website her.

### **Abrufen von Threat-Details über das Scanfortschrittsfenster**

Klicken Sie bei On-Demand- oder Rechtsklick-Scans im Protokoll, das im Scanfortschrittsfenster angezeigt wird, oder in der Scanübersicht, die nach dem Scan angezeigt wird, auf den Namen des Threats, über den Sie mehr erfahren möchten.

Sophos Anti-Virus stellt eine Verbindung zur Threat-Analyse auf der Sophos Website her.

### **Abrufen von Threat-Details über den Quarantäne-Manager**

1. Klicken Sie auf der **Startseite** im Bereich **Antivirus und HIPS** auf **Quarantäne-Objekte verwalten**. Nähere Informationen zur **Startseite** finden Sie unter [Die Startseite](#) (Seite 4).
2. Klicken Sie in der Spalte **Name** auf den Namen des Threats, über den Sie sich informieren möchten.

Sophos Anti-Virus stellt eine Verbindung zur Threat-Analyse auf der Sophos Website her.

## 5 Sophos Device Control

### 5.1 Allgemeine Informationen

Wenn Sophos Endpoint Security and Control auf dem Computer nicht von einer Management-Konsole verwaltet wird, ist Device Control *nicht* verfügbar.

Device Control wird über eine Management-Konsole aktiviert bzw. deaktiviert. Wenn Device Control aktiviert ist, wird unter Umständen verhindert, dass ein Gerät zu Wartungs- oder Problembhebungszwecken an den Computer angeschlossen wird. In diesem Fall sollten Sie Device Control auf dem entsprechenden Computer deaktivieren. Nähere Informationen hierzu finden Sie unter [Device Control vorübergehend deaktivieren](#) (Seite 44).

### 5.2 Welche Geräte kann Device Control überwachen?

Device Control erlaubt/sperrt die folgenden Gerätearten auf diesem Computer: *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 Hardwareverschlüsselung)

#### Netzwerkgeräte

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

Unter Umständen befindet sich die Device Control-Richtlinie im Modus **Netzwerkbrücken sperren**, in dem Wireless- oder Modemnetzwerkadapter deaktiviert werden, wenn der Computer an ein physisches Netzwerk (in der Regel per Ethernet) angeschlossen ist. Wenn der Computer von dem physischen Netzwerk getrennt wird, wird der Wireless- oder Modemnetzwerkadapter wieder aktiviert.

#### Kurze Reichweite

- Bluetooth-Schnittstellen
- Infrarot-Schnittstellen (IrDA)

### 5.3 Device Control vorübergehend deaktivieren

**Wichtig:** Wenn Sophos Endpoint Security and Control über eine Management-Konsole verwaltet wird, werden hier vorgenommene Änderungen eventuell nicht berücksichtigt.

Wenn Sie Mitglied der Gruppe „SophosAdministrator“ sind und aus Wartungs- oder Fehlerbehebungsgründen eine Verbindung zu einem Gerät an diesem Computer herstellen

möchten (z.B. zum Installieren von Software von einer CD-ROM), können Sie Device Control vorübergehend deaktivieren.

So deaktivieren Sie Device Control auf dem Computer:

1. Klicken Sie im Menü **Konfigurieren** auf **Device Control**.
2. Deaktivieren Sie das Kontrollkästchen **Device Control aktivieren** .

## 5.4 Konfigurieren des Device Control-Protokolls

1. Klicken Sie im Menü **Konfigurieren** auf **Device Control**.
2. Wählen Sie im Bereich **Protokollierungsstufe** eine der folgenden Optionen aus:
  - Bei Auswahl der Option **Keine Protokollierung** wird nichts protokolliert.
  - Bei Auswahl der Option **Normal** werden Zusammenfassungen, Fehlermeldungen usw. protokolliert.
  - Bei Auswahl der Option **Ausführlich** werden zusätzliche Aktivitäten protokolliert. Da die Protokollgröße bei Auswahl dieser Einstellung rapide ansteigt, sollte sie nur zur Problembeseitigung aktiviert werden.
3. Befolgen Sie im Bereich **Protokollarchivierung** die Anweisungen auf dem Bildschirm.

## 5.5 Öffnen des Device Control-Protokolls

- ❖ Klicken Sie auf der **Startseite** unter **Device Control** auf **Device Control-Protokoll anzeigen**. Weitere Informationen zur **Startseite** finden Sie unter [Die Startseite](#) (Seite 4).

Aus der Protokollseite können Sie das Protokoll in die Zwischenablage kopieren, es per E-Mail versenden oder ausdrucken.

Wenn Sie im Protokoll bestimmten Text suchen, klicken Sie auf **Suchen** und geben Sie den gewünschten Text in das Suchfeld ein.

## 6 Sophos Data Control

### 6.1 Allgemeine Informationen

Wenn Sophos Endpoint Security and Control auf dem Computer nicht von einer Management-Konsole verwaltet wird, ist Data Control *nicht* verfügbar.

Data Control wird über eine von der Management-Konsole ausgegebene Richtlinie aktiviert bzw. deaktiviert. Mitglieder der Gruppe „SophosAdministrator“ können Data Control jedoch zur Fehlersuche auf dem Computer vorübergehend deaktivieren: Nähere Informationen hierzu finden Sie unter [Data Control vorübergehend deaktivieren](#) (Seite 46).

### 6.2 Data Control vorübergehend deaktivieren

**Wichtig:** Wenn Sophos Endpoint Security and Control über eine Management-Konsole verwaltet wird, werden hier vorgenommene Änderungen eventuell nicht berücksichtigt.

Mitglieder der Gruppe „SophosAdministrator“ können Data Control zur Fehlersuche auf dem Computer vorübergehend deaktivieren:

1. Klicken Sie im Menü **Konfigurieren** auf **Data Control**.
2. Deaktivieren Sie das Kontrollkästchen **Data Control aktivieren**.

### 6.3 Hinzufügen von Dateien zu einem Speichergerät

Wenn Data Control auf dem Computer aktiviert ist, sperrt die Data Control-Richtlinie unter Umständen jegliche Versuche, Dateien anhand einer der folgenden Methoden zu einem überwachten Speichergerät hinzuzufügen:

- Speichern von Daten in einer Anwendung
- Kopieren über einen DOS-Befehl
- Erstellen einer neuen Datei auf dem Gerät mit Windows Explorer

Wenn Sie in einer Desktop-Benachrichtigung hierauf hingewiesen werden, speichern Sie die Datei zunächst auf der Festplatte oder einem Netzlaufwerk und kopieren Sie sie dann mit Windows Explorer auf das Speichergerät.

### 6.4 Konfigurieren des Data Control-Protokolls

1. Klicken Sie im Menü **Konfigurieren** auf **Data Control**.
2. Wählen Sie im Bereich **Protokollierungsstufe** eine der folgenden Optionen aus:
  - Bei Auswahl der Option **Keine Protokollierung** wird nichts protokolliert.
  - Bei Auswahl der Option **Normal** werden Zusammenfassungen, Fehlermeldungen usw. protokolliert.

- Bei Auswahl der Option **Ausführlich** werden zusätzliche Aktivitäten protokolliert. Da die Protokollgröße bei Auswahl dieser Einstellung rapide ansteigt, sollte sie nur beim Testen neuer Data Control-Regeln aktiviert werden.

3. Befolgen Sie im Bereich **Protokollarchivierung** die Anweisungen auf dem Bildschirm.

## 6.5 Öffnen des Data Control-Protokolls

- ❖ Klicken Sie auf der **Startseite** unter **Data Control** auf **Data Control-Protokoll anzeigen**. Weitere Informationen zur **Startseite** finden Sie unter [Die Startseite](#) (Seite 4).

Aus der Protokollseite können Sie das Protokoll in die Zwischenablage kopieren, es per E-Mail versenden oder ausdrucken.

Wenn Sie im Protokoll bestimmten Text suchen, klicken Sie auf **Suchen** und geben Sie den gewünschten Text in das Suchfeld ein.

## 7 Sophos Client Firewall

### 7.1 Vorbereitung

Je nach Installationsart muss die Firewall bei der Erstinstallation möglicherweise konfiguriert werden. Die Firewall kann anhand der folgenden Methoden installiert werden:

- Installation auf einem Netzwerkcomputer; Verwaltung über eine Management-Konsole
- Installation auf einem Einzelplatzrechner; Verwaltung über den Computer

#### Verwaltung der Firewall über eine Management-Konsole

Wenn die Firewall über eine Management-Konsole installiert und verwaltet wird, wird Datenfluss in Einklang mit den Richtlinienregeln zugelassen oder gesperrt.

Sofern die Firewall nicht von der Richtlinie in den Modus „interaktiv“ (siehe unten) versetzt wird, werden keine Benutzermeldungen angezeigt und die Firewall muss nicht konfiguriert werden.

#### Verwaltung der Firewall über den Computer

Bei der Verwaltung der Firewall über den Computer sollten Regeln für den Netzwerkzugriff gängiger Anwendungen und Dienste (z.B. Browser, E-Mail-Clients) erstellt werden.

Anweisungen hierzu entnehmen Sie bitte dem Abschnitt [Allgemeine Informationen](#) (Seite 48).

Anfänglich befindet sich die Firewall im Modus „interaktiv“ (siehe unten). Betreiben Sie die Firewall vorübergehend in diesem Modus, damit Sie Anwendungen und Dienste zulassen bzw. sperren können.

Wenn die Firewall konfiguriert wurde und gängige Anwendungen erkennt, empfiehlt sich, in einen nicht-interaktiven Modus zu wechseln.

Nähere Informationen hierzu finden Sie unter [Auswählen eines nicht interaktiven Modus](#) (Seite 55).

#### Der Modus „interaktiv“

Im Modus „interaktiv“ gibt der Benutzer an, ob Datenfluss und Anwendungen, denen keine Regel zugewiesen wurde, zugelassen oder gesperrt werden sollen

Nähere Informationen zum Umgang mit Firewall-Meldungen entnehmen Sie bitte dem Abschnitt [Allgemeine Informationen](#) (Seite 55).

### 7.2 Konfigurieren der Firewall

#### 7.2.1 Allgemeine Informationen

Vor dem Aktivieren der Firewall können Sie sie zunächst konfigurieren. Wenn Sophos Endpoint Security and Control auf dem Computer jedoch über eine Management-Konsole verwaltet wird, werden hier vorgenommene Änderungen nicht berücksichtigt.

Im Folgenden werden gängige Funktionen aufgeführt:

- [Aktivieren des interaktiven Modus](#) (Seite 55)
- [Filtern von ICMP-Meldungen](#) (Seite 53)
- [Zulassen des gesamten Dateiflusses in einem lokalen Netzwerk](#) (Seite 51)
- [Zulassen von FTP-Downloads](#) (Seite 50)
- [Erstellen einer globalen Regel](#) (Seite 60)
- [Zulassen einer Anwendung](#) (Seite 52)
- [Zulassen versteckter Prozesse](#) (Seite 65)
- [Zulassen von Raw-Sockets](#) (Seite 66)
- [Authentifizieren von Anwendungen mit Hilfe von Prüfsummen](#) (Seite 67)

## 7.2.2 Vorübergehende Deaktivierung der Firewall

Wenn Sie in die SophosAdministrator-Gruppe eingegliedert sind, muss die Firewall unter bestimmten Umständen (z.B. aus Wartungsgründen oder zur Fehlerbehebung) vorübergehend deaktiviert werden.

Sophos Endpoint Security and Control behält die hier vorgenommenen Änderungen bei, auch wenn Sie den Computer später neu starten. Der Computer bleibt so lange ungeschützt, bis die Firewall wieder aktiviert wird.

1. Klicken Sie auf der **Startseite** unter **Firewall** auf **Firewall konfigurieren**.  
Weitere Informationen zur **Startseite** finden Sie unter [Die Startseite](#) (Seite 4).
2. Aktivieren Sie unter **Konfigurationen** jeweils das Kontrollkästchen **Gesamten Datenfluss zulassen** neben dem primären oder sekundären Standort.

## 7.2.3 Zulassen eines E-Mail-Programms

**Wichtig:** Wenn Sophos Endpoint Security and Control über eine Management-Konsole verwaltet wird, werden hier vorgenommene Änderungen eventuell nicht berücksichtigt.

1. Klicken Sie auf der **Startseite** unter **Firewall** auf **Firewall konfigurieren**.  
Weitere Informationen zur **Startseite** finden Sie unter [Die Startseite](#) (Seite 4).
2. Klicken Sie im Bereich **Konfigurationen** neben dem zu konfigurierenden Standort auf **Konfigurieren**.
3. Klicken Sie auf die Registerkarte **Anwendungen**.
4. Klicken Sie auf **Hinzufügen**, suchen Sie das gewünschte E-Mail-Programm und wählen Sie es durch einen Doppelklick aus.

Das E-Mail-Programm wird als vertrauenswürdige Anwendung zugelassen.

Vertrauenswürdige Anwendungen erhalten uneingeschränkten Vollzugriff auf das Netzwerk und das Internet. Größere Sicherheit bieten die von Sophos vordefinierten Regeln:

1. Klicken Sie in der Liste der zugelassenen Anwendungen auf das E-Mail-Programm.

2. Klicken Sie auf **Regel > Regeln aus Voreinstellungen hinzufügen > E-Mail-Client** .

## 7.2.4 Zulassen eines Webbrowsers

**Hinweis:** Durch die Zulassung eines bestimmten Webbrowsers wird automatisch auch der FTP-Zugriff freigegeben.

1. Klicken Sie auf der **Startseite** unter **Firewall** auf **Firewall konfigurieren**.  
Weitere Informationen zur **Startseite** finden Sie unter [Die Startseite](#) (Seite 4).
2. Klicken Sie im Bereich **Konfigurationen** neben dem zu konfigurierenden Standort auf **Konfigurieren**.
3. Klicken Sie auf die Registerkarte **Anwendungen**.
4. Klicken Sie auf **Hinzufügen**, suchen Sie das gewünschte Browser-Programm und wählen Sie es durch einen Doppelklick aus.

Das Browser-Programm wird als vertrauenswürdige Anwendung zugelassen.

Vertrauenswürdige Anwendungen erhalten uneingeschränkten Vollzugriff auf das Netzwerk und das Internet. Größere Sicherheit bieten die von Sophos vordefinierten Regeln:

1. Klicken Sie in der Liste der zugelassenen Anwendungen auf das Browser-Programm.
2. Klicken Sie auf **Regel > Regeln aus Voreinstellungen hinzufügen > Browser** .

## 7.2.5 Zulassen von FTP-Downloads

**Hinweis:** Wenn Sie den Einsatz eines Webbrowsers mit Zugriff auf FTP-Server zugelassen haben, müssen FTP-Downloads nicht extra zugelassen werden.

1. Klicken Sie auf der **Startseite** unter **Firewall** auf **Firewall konfigurieren**.  
Weitere Informationen zur **Startseite** finden Sie unter [Die Startseite](#) (Seite 4).
2. Klicken Sie im Bereich **Konfigurationen** neben dem zu konfigurierenden Standort auf **Konfigurieren**.
3. Klicken Sie auf die Registerkarte **Anwendungen**.
4. Klicken Sie auf **Hinzufügen**, suchen Sie das FTP-Programm und wählen Sie es durch einen Doppelklick aus.

Das FTP-Programm wird als vertrauenswürdige Anwendung zugelassen.

Vertrauenswürdige Anwendungen erhalten uneingeschränkten Vollzugriff auf das Netzwerk und das Internet. Größere Sicherheit bieten die von Sophos vordefinierten Regeln:

1. Klicken Sie in der Liste der zugelassenen Anwendungen auf das FTP-Programm.
2. Klicken Sie auf **Regel > Regeln aus Voreinstellungen hinzufügen > FTP-Client** .

## 7.2.6 Zulassen des gesamten Dateiflusses in einem lokalen Netzwerk

So lassen Sie den gesamten Datenfluss zwischen Computern in einem lokalen Netzwerk (Local Area Network) zu:

1. Klicken Sie auf der **Startseite** unter **Firewall** auf **Firewall konfigurieren**.  
Weitere Informationen zur **Startseite** finden Sie unter [Die Startseite](#) (Seite 4).
2. Klicken Sie im Bereich **Konfigurationen** neben dem zu konfigurierenden Standort auf **Konfigurieren**.
3. Öffnen Sie die Registerkarte **LAN** und wählen Sie:
  - Klicken Sie auf **Erkennen**, um das LAN zu suchen und in die Liste der Netzwerkadressen aufzunehmen.
  - Klicken Sie auf **Hinzufügen**. Wählen Sie im Dialogfenster **Adresse wählen** das **Adressenformat** aus und geben Sie den Namen oder die IP-Adresse der Domäne ein. Klicken Sie danach auf **Hinzufügen**.
4. Klicken Sie auf **OK**, um das Fenster zu schließen.
5. 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.

## 7.2.7 Datei- und Druckerfreigabe im lokalen Netz

**Hinweis:** Wenn Sie den gesamten Datenfluss zwischen Computern in einem lokalen Netzwerk (LAN) zugelassen haben, brauchen Sie nicht extra eine Datei- und Druckerfreigabe einzurichten.

So lassen Sie die gesamte Datei- und Druckerfreigabe im lokalen Netzwerk zu:

1. Klicken Sie auf der **Startseite** unter **Firewall** auf **Firewall konfigurieren**.  
Weitere Informationen zur **Startseite** finden Sie unter [Die Startseite](#) (Seite 4).
2. Klicken Sie im Bereich **Konfigurationen** neben dem zu konfigurierenden Standort auf **Konfigurieren**.
3. Öffnen Sie die Registerkarte **LAN** und wählen Sie:
  - Klicken Sie auf **Erkennen**, um das LAN zu suchen und in die Liste der Netzwerkadressen aufzunehmen.
  - Klicken Sie auf **Hinzufügen**. Wählen Sie im Dialogfenster **Adresse wählen** das **Adressenformat** aus und geben Sie den Namen oder die IP-Adresse der Domäne ein. Klicken Sie danach auf **Hinzufügen**.
4. Klicken Sie auf **OK**, um das Fenster zu schließen.
5. Wählen Sie in der Liste der **LAN-Einstellungen** **NetBIOS**, um in einem lokalen Netzwerk die Datei- und Druckerfreigabe zu ermöglichen.

Nähere Informationen zum Sperren oder Zulassen der Datei- und Druckerfreigabe auf Netzwerken, die sich nicht in der Liste der **LAN-Einstellungen** befinden, entnehmen Sie bitte folgenden Abschnitten:

- [Sperren unerwünschter Datei- und Druckerfreigabe](#) (Seite 63)
- [Zulassen der flexiblen Steuerung der Datei- und Druckerfreigabe](#) (Seite 52)

Nähere Informationen zum Zulassen des gesamten Datenflusses in einem lokalen Netzwerk können Sie dem Abschnitt [Zulassen des gesamten Dateiflusses in einem lokalen Netzwerk](#) (Seite 51) entnehmen.

## 7.2.8 Zulassen der flexiblen Steuerung der Datei- und Druckerfreigabe

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. Klicken Sie auf der **Startseite** unter **Firewall** auf **Firewall konfigurieren**.  
Weitere Informationen zur **Startseite** finden Sie unter [Die Startseite](#) (Seite 4).
2. Klicken Sie im Bereich **Konfigurationen** neben dem zu konfigurierenden Standort auf **Konfigurieren**.
3. Deaktivieren Sie auf der Registerkarte **LAN** die Option **Datei- und Druckerfreigabe für andere Netzwerke sperren**.

## 7.2.9 Zulassen einer Anwendung

1. Klicken Sie auf der **Startseite** unter **Firewall** auf **Firewall konfigurieren**.  
Weitere Informationen zur **Startseite** finden Sie unter [Die Startseite](#) (Seite 4).
2. Klicken Sie im Bereich **Konfigurationen** neben dem zu konfigurierenden Standort auf **Konfigurieren**.
3. Klicken Sie auf die Registerkarte **Anwendungen**.
4. Klicken Sie auf **Hinzufügen**, suchen Sie die gewünschte Anwendung und wählen Sie sie durch einen Doppelklick aus.

Die Anwendung wird daraufhin als „vertrauenswürdig“ zugelassen.

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 63)
- [Übernahme vordefinierter Anwendungsregeln](#) (Seite 63)

## 7.2.10 Sperren einer Anwendung

1. Klicken Sie auf der **Startseite** unter **Firewall** auf **Firewall konfigurieren**.  
Weitere Informationen zur **Startseite** finden Sie unter [Die Startseite](#) (Seite 4).
2. Klicken Sie im Bereich **Konfigurationen** neben dem zu konfigurierenden Standort auf **Konfigurieren**.
3. Klicken Sie auf die Registerkarte **Anwendungen**.
4. Wird die Anwendung nicht aufgeführt, klicken Sie auf **Hinzufügen**, suchen Sie die Anwendung und doppelklicken Sie darauf.
5. Wählen Sie die Anwendung aus der Liste aus und klicken Sie anschließend auf **Sperren**.

## 7.2.11 Filtern von ICMP-Meldungen

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 53) werden die ICMP-Meldungstypen beschrieben.

So filtern Sie ICMP-Meldungen:

1. Klicken Sie auf der **Startseite** unter **Firewall** auf **Firewall konfigurieren**.  
Weitere Informationen zur **Startseite** finden Sie unter [Die Startseite](#) (Seite 4).
2. Klicken Sie im Bereich **Konfigurationen** neben dem zu konfigurierenden Standort auf **Konfigurieren**.
3. Wählen Sie auf der Registerkarte **ICMP** die Option **Eingehend** oder **Ausgehend**, um eingehende bzw. ausgehende Meldungen des angegebenen Typs zuzulassen.

## 7.2.12 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.
<b>Quelldrosselung</b>	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-Übertragungsrates durch die Quelle zu verstehen.
<b>Umleitung</b>	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.
<b>Router-Ankündigung, Router-Anfrage</b>	Die Meldung macht Hosts auf Router aufmerksam. Router versenden regelmäßig ihre IP-Adressen über <b>Router-Ankündigungsmeldungen</b> . Mitunter fordern Hosts mittels <b>Router-Anfragen</b> Router-Adressen an. Die Antwort durch den Router erfolgt über <b>Router-Ankündigungen</b> .
<b>Datagramm-Zeitüberschreitung</b>	Meldung eines Routers, wenn ein Datagramm die maximale Routeranzahl erreicht hat.
<b>Datagramm-Parameterproblem</b>	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.
<b>Zeitstempel-Anforderung, Zeitstempel-Antwort</b>	Dient der zeitlichen Synchronisierung von Hosts und der Schätzung der Transitzeit.
<b>Informations-Anforderung, Informations-Antwort</b>	Veraltet. Die Meldungen wurden zur Bestimmung der Internetwork-Adressen von Hosts eingesetzt, gelten jetzt aber als veraltet und sollten nicht mehr verwendet werden.
<b>Adressmasken-Anforderung, Adressmasken-Antwort</b>	Meldung zur Ermittlung der Subnetz-Maske (d.h. der Adressabschnitte, die das Netzwerk definieren). Ein Host sendet eine <b>Adressmasken-Anforderung</b> an einen Router und empfängt eine <b>Adressmasken-Antwort</b> .

### 7.2.13 Wiederherstellen der Firewall-Voreinstellungen

1. Klicken Sie auf der **Startseite** unter **Firewall** auf **Firewall konfigurieren**.  
Weitere Informationen zur **Startseite** finden Sie unter [Die Startseite](#) (Seite 4).
2. Klicken Sie im Bereich **Konfiguration verwalten** auf **Voreinstellungen**.

## 7.3 Arbeiten im interaktiven Modus

### 7.3.1 Allgemeine Informationen

Im interaktiven Modus wird ein *Lerndialogfenster* angezeigt, wenn eine unbekannte Anwendung oder ein unbekannter Dienst Netzwerkzugriff anfordert. Der Benutzer kann angeben, ob Datenfluss einmal zugelassen oder gesperrt werden soll oder ob eine Regel dafür erstellt werden soll.

Der interaktive Modus umfasst die folgenden Lerndialoge:

- [Lerndialoge zu versteckten Prozessen](#) (Seite 56)
- [Protokoll-Lerndialoge](#) (Seite 56)
- [Anwendungs-Lerndialoge](#) (Seite 56)
- [Raw-Socket-Lerndialoge](#) (Seite 56)
- [Prüfsummenlerndialoge](#) (Seite 57)

### 7.3.2 Aktivieren des interaktiven Modus

1. Klicken Sie auf der **Startseite** unter **Firewall** auf **Firewall konfigurieren**.  
Weitere Informationen zur **Startseite** finden Sie unter [Die Startseite](#) (Seite 4).
2. Klicken Sie im Bereich **Konfigurationen** neben dem zu konfigurierenden Standort auf **Konfigurieren**.
3. Klicken Sie auf der Registerkarte **Allgemein** unter **Arbeitsmodus** auf **Interaktiv**.

### 7.3.3 Auswählen eines nicht interaktiven Modus

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 wählen Sie einen nicht interaktiven Modus aus:

1. Klicken Sie auf der **Startseite** unter **Firewall** auf **Firewall konfigurieren**.  
Weitere Informationen zur **Startseite** finden Sie unter [Die Startseite](#) (Seite 4).
2. Klicken Sie im Bereich **Konfigurationen** neben dem zu konfigurierenden Standort auf **Konfigurieren**.
3. Klicken Sie auf der Registerkarte **Allgemein** unter **Arbeitsmodus** auf die Option **Datenfluss ohne passende Regel zulassen** oder **Datenfluss ohne passende Regel sperren**.

### 7.3.4 Lerndialoge zu versteckten Prozessen

Wenn eine Anwendung eine andere Anwendung startet, um für sie auf das Netzwerk zuzugreifen, so handelt es sich hierbei um einen versteckten Prozess. Gelegentlich machen sich Schadprogramme diese Technik zunutze, um eine Firewall zu umgehen: Sie starten eine vertrauenswürdige Anwendung, die für Sie auf das Netzwerk zugreift, auf das sie selbst keinen Zugriff haben.

Im Lerndialog zu versteckten Prozessen werden Informationen zum versteckten Prozess und zur auslösenden Anwendung angezeigt.

- [Aktivieren von Lerndialogen zu versteckten Prozessen](#) (Seite 56)

### 7.3.5 Aktivieren von Lerndialogen zu versteckten Prozessen

Im interaktiven Modus kann die Firewall bei Erkennung eines neuen Launchers einen Lerndialog anzeigen.

Wenn Sie im interaktiven Modus arbeiten und diese Option deaktiviert ist, können neue Launcher keine versteckten Prozesse starten.

So aktivieren Sie Lerndialoge zu versteckten Prozessen:

1. Klicken Sie auf der **Startseite** unter **Firewall** auf **Firewall konfigurieren**.  
Weitere Informationen zur **Startseite** finden Sie unter [Die Startseite](#) (Seite 4).
2. Klicken Sie im Bereich **Konfigurationen** neben dem zu konfigurierenden Standort auf **Konfigurieren**.
3. Klicken Sie auf die Registerkarte **Prozesse**.
4. Aktivieren Sie das Kontrollkästchen **Vor neuen Launchern warnen**.

### 7.3.6 Protokoll-Lerndialoge

Wenn die Firewall Datenbewegungen im Netzwerk erkennt, die keiner bestimmten Anwendung zuzuordnen sind, werden Sie zur Erstellung einer Protokollregel aufgefordert.

Im Protokoll-Lerndialog werden das Protokoll und die Remote-Adresse angezeigt.

### 7.3.7 Anwendungs-Lerndialoge

Wenn die Firewall einen bisher nicht geregelten Netzwerkzugriff durch eine Anwendung erkennt, werden Sie zur Erstellung einer Anwendungsregel aufgefordert.

Im Anwendungs-Lerndialog werden der Remote-Dienst und die Remote-Adresse angezeigt.

### 7.3.8 Raw-Socket-Lerndialoge

Raw-Sockets erlauben Prozessen die Steuerung der Datenbewegungen im Netzwerk und können für illegale Zwecke missbraucht werden.

Wenn die Firewall einen bisher nicht geregelten Raw-Socket-Netzwerkzugriff erkennt, werden Sie zur Erstellung einer Raw-Socket-Regel aufgefordert.

Im Raw-Socket-Lerndialog die Raw-Socket-Details angezeigt.

- [Aktivieren von Raw-Socket-Lerndialogen](#) (Seite 57)

### 7.3.9 Aktivieren von Raw-Socket-Lerndialogen

Im interaktiven Modus kann die Firewall Lerndialoge anzeigen, wenn die Firewall einen bisher nicht geregelten Raw-Socket-Netzwerkzugriff erkennt.

Wenn Sie im interaktiven Modus arbeiten und diese Option deaktiviert ist, wird Raw-Sockets der Netzwerkzugriff verweigert.

So aktivieren Sie Raw-Socket-Lerndialoge:

1. Klicken Sie auf der **Startseite** unter **Firewall** auf **Firewall konfigurieren**.  
Weitere Informationen zur **Startseite** finden Sie unter [Die Startseite](#) (Seite 4).
2. Klicken Sie im Bereich **Konfigurationen** neben dem zu konfigurierenden Standort auf **Konfigurieren**.
3. Klicken Sie auf die Registerkarte **Prozesse**.
4. Aktivieren Sie das Kontrollkästchen **Vor dem Gebrauch von Raw-Sockets warnen**.

### 7.3.10 Prüfsummenlerndialoge

Wenn die Firewall eine neue oder geänderte Anwendung erkennt, wird ein Prüfsummenlerndialog geöffnet.

Wenn die Anwendung Netzwerkzugriff erhalten soll, müssen Sie die Prüfsumme (eine eindeutige Kennung) in die Prüfsummenliste aufnehmen.

Wählen Sie eine der folgenden Optionen:

- **Zu den Prüfsummen dieser Anwendung hinzufügen:** Mehrere Versionen derselben Anwendung werden zugelassen.
- **Vorhandene Prüfsumme dieser Anwendung ersetzen:** Alle bestehenden Prüfsummen einer Anwendung werden durch die Prüfsumme der Zugriff anfordernden Anwendung ersetzt, wodurch ausschließlich die neueste Version dieser Anwendung zugelassen wird.
- **Anwendung sperren, bis sie neu gestartet wird:** Die Anwendung wird in diesem Fall gesperrt.

### 7.3.11 Aktivieren von Prüfsummenlerndialogen

Im interaktiven Modus kann die Firewall Lerndialoge anzeigen, wenn neue oder geänderte Anwendungen erkannt werden.

Wenn Sie im interaktiven Modus arbeiten und diese Option deaktiviert ist, wird Anwendungen der Netzwerkzugriff verweigert.

So aktivieren Sie Prüfsummenlerndialoge:

1. Klicken Sie auf der **Startseite** unter **Firewall** auf **Firewall konfigurieren**.  
Weitere Informationen zur **Startseite** finden Sie unter [Die Startseite](#) (Seite 4).
2. Klicken Sie im Bereich **Konfigurationen** neben dem zu konfigurierenden Standort auf **Konfigurieren**.
3. Aktivieren Sie im Bereich **Sperren** das Kontrollkästchen **Anwendungen anhand von Prüfsummen authentifizieren**.

## 7.4 Firewall-Konfigurationsdateien

### 7.4.1 Allgemeine Informationen

Sie können mit Sophos Client Firewall allgemeine Firewalleinstellungen und -regeln als Konfigurationsdatei exportieren. Diese Funktion umfasst folgende Optionen:

- Sichern und Wiederherstellen der Firewallkonfiguration.
- Speichern der allgemeinen Einstellungskonfiguration und deren Übertragung auf mehrere Computer.
- Erstellen von Anwendungsregeln auf einem Computer und Export und Einsatz der Regeln auf anderen Computern mit den gleichen Anwendungen.
- Kombination der Konfiguration von Einzelcomputern zur Erstellung einer Richtlinie für alle Computer im Netzwerk.

### 7.4.2 Exportieren einer Firewall-Konfigurationsdatei

1. Klicken Sie auf der **Startseite** unter **Firewall** auf **Firewall konfigurieren**.  
Weitere Informationen zur **Startseite** finden Sie unter [Die Startseite](#) (Seite 4).
2. Klicken Sie auf **Exportieren**.
3. Geben Sie der Konfigurationsdatei einen Namen, wählen Sie den gewünschten Speicherort aus und klicken Sie auf **Speichern**.

### 7.4.3 Importieren einer Firewall-Konfigurationsdatei

1. Klicken Sie auf der **Startseite** unter **Firewall** auf **Firewall konfigurieren**.  
Weitere Informationen zur **Startseite** finden Sie unter [Die Startseite](#) (Seite 4).
2. Klicken Sie auf **Importieren**.
3. Wählen Sie die gewünschte Konfigurationsdatei und klicken Sie auf **Öffnen**.
4. Befolgen Sie die Anweisungen auf dem Bildschirm.

## 7.5 Firewall-Regeln

### 7.5.1 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.

### 7.5.2 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**.

## 7.5.3 Globale Regeln

### 7.5.3.1 Erstellen einer globalen Regel

**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. Klicken Sie auf der **Startseite** unter **Firewall** auf **Firewall konfigurieren**.  
Weitere Informationen zur **Startseite** finden Sie unter [Die Startseite](#) (Seite 4).
2. Klicken Sie im Bereich **Konfigurationen** neben dem zu konfigurierenden Standort auf **Konfigurieren**.
3. Klicken Sie auf die Registerkarte **Globale Regel**.
4. Klicken Sie auf **Hinzufügen**.
5. 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.
6. 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 59).
7. Wählen Sie im Bereich **Ereignisse, für die die Regel zutreffen soll** die Bedingungen aus, die eine Verbindung erfüllen muss, damit die Regel greift.
8. Wählen Sie im Bereich **Maßnahmen, die die Regel ergreifen soll** **Zulassen** oder **Sperren** aus.

9. 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.
10. Klicken Sie im Bereich **Regelbeschreibung** auf einen unterstrichenen Wert. Wenn Sie beispielsweise auf den Link **TCP** klicken, wird das Dialogfeld **Protokoll wählen** geöffnet.

### 7.5.3.2 Ändern einer globalen Regel

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

So ändern Sie eine globale Regel:

1. Klicken Sie auf der **Startseite** unter **Firewall** auf **Firewall konfigurieren**.  
Weitere Informationen zur **Startseite** finden Sie unter [Die Startseite](#) (Seite 4).
2. Klicken Sie im Bereich **Konfigurationen** neben dem zu konfigurierenden Standort auf **Konfigurieren**.
3. Klicken Sie auf die Registerkarte **Globale Regel**.
4. Wählen Sie die gewünschte Regel aus der **Regelliste** aus.
5. Klicken Sie auf **Bearbeiten**.  
Nähere Informationen zu den Einstellungen globaler Regeln können Sie dem Abschnitt [Erstellen einer globalen Regel](#) (Seite 60) entnehmen.

### 7.5.3.3 Kopieren einer globalen Regel

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

1. Klicken Sie auf der **Startseite** unter **Firewall** auf **Firewall konfigurieren**.  
Weitere Informationen zur **Startseite** finden Sie unter [Die Startseite](#) (Seite 4).
2. Klicken Sie im Bereich **Konfigurationen** neben dem zu konfigurierenden Standort auf **Konfigurieren**.
3. Klicken Sie auf die Registerkarte **Globale Regel**.
4. Wählen Sie die gewünschte Regel aus der **Regelliste** aus.
5. Klicken Sie auf **Kopieren**.

### 7.5.3.4 Ändern der Priorität von globalen Regeln

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. Klicken Sie auf der **Startseite** unter **Firewall** auf **Firewall konfigurieren**.  
Weitere Informationen zur **Startseite** finden Sie unter [Die Startseite](#) (Seite 4).
2. Klicken Sie im Bereich **Konfigurationen** neben dem zu konfigurierenden Standort auf **Konfigurieren**.
3. Klicken Sie auf die Registerkarte **Globale Regel**.
4. Klicken Sie in der **Regelliste** auf die Regel, die Sie nach oben oder unter verschieben möchten.
5. Klicken Sie auf **Nach oben** oder **Nach unten**.

#### 7.5.3.5 Löschen einer globalen Regel

1. Klicken Sie auf der **Startseite** unter **Firewall** auf **Firewall konfigurieren**.  
Weitere Informationen zur **Startseite** finden Sie unter [Die Startseite](#) (Seite 4).
2. Klicken Sie im Bereich **Konfigurationen** neben dem zu konfigurierenden Standort auf **Konfigurieren**.
3. Klicken Sie auf die Registerkarte **Globale Regel**.
4. Wählen Sie die gewünschte Regel aus der **Regelliste** aus.
5. Klicken Sie auf **Entfernen**.

### 7.5.4 Sperren

#### 7.5.4.1 Aktivieren/Deaktivieren des Sperrens modifizierter Prozesse

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. Klicken Sie auf der **Startseite** unter **Firewall** auf **Firewall konfigurieren**.  
Weitere Informationen zur **Startseite** finden Sie unter [Die Startseite](#) (Seite 4).
2. Klicken Sie im Bereich **Konfigurationen** neben dem zu konfigurierenden Standort auf **Konfigurieren**.
3. 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.

### 7.5.4.2 Sperren unerwünschter Datei- und Druckerfreigabe

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. Klicken Sie auf der **Startseite** unter **Firewall** auf **Firewall konfigurieren**.  
Weitere Informationen zur **Startseite** finden Sie unter [Die Startseite](#) (Seite 4).
2. Klicken Sie im Bereich **Konfigurationen** neben dem zu konfigurierenden Standort auf **Konfigurieren**.
3. Aktivieren Sie auf der Registerkarte **LAN** die Option **Datei- und Druckerfreigabe für andere Netzwerke sperren**.

## 7.5.5 Anwendungsregeln

### 7.5.5.1 Übernahme vordefinierter Anwendungsregeln

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. Klicken Sie auf der **Startseite** unter **Firewall** auf **Firewall konfigurieren**.  
Weitere Informationen zur **Startseite** finden Sie unter [Die Startseite](#) (Seite 4).
2. Klicken Sie im Bereich **Konfigurationen** neben dem zu konfigurierenden Standort auf **Konfigurieren**.
3. Klicken Sie auf die Registerkarte **Anwendungen**.
4. Wählen Sie die Anwendung aus der Liste aus und klicken Sie anschließend auf den Pfeil neben der Option **Regel**.
5. Richten Sie den Mauszeiger auf **Regeln aus Voreinstellungen hinzufügen** und klicken Sie auf eine vordefinierte Regel.

### 7.5.5.2 Erstellen einer Anwendungsregel

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

1. Klicken Sie auf der **Startseite** unter **Firewall** auf **Firewall konfigurieren**.  
Weitere Informationen zur **Startseite** finden Sie unter [Die Startseite](#) (Seite 4).

2. Klicken Sie im Bereich **Konfigurationen** neben dem zu konfigurierenden Standort auf **Konfigurieren**.
3. Klicken Sie auf die Registerkarte **Anwendungen**.
4. Wählen Sie die Anwendung aus der Liste aus und klicken Sie anschließend auf **Regel**. Sie können auch auf die Anwendung in der Liste doppelklicken.
5. Klicken Sie im Dialogfeld **Anwendungsregeln** auf **Hinzufügen**.
6. 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.
7. Wählen Sie im Bereich **Ereignisse, für die die Regel zutreffen soll** die Bedingungen aus, die eine Verbindung erfüllen muss, damit die Regel greift.
8. Wählen Sie im Bereich **Maßnahmen, die die Regel ergreifen soll Zulassen** oder **Sperren** aus.
9. Bei Auswahl der Option **Stateful Inspection** basieren die Antworten des Remote-Computers auf der ersten Verbindung.
10. Klicken Sie im Bereich **Regelbeschreibung** auf einen unterstrichenen Wert. Wenn Sie beispielsweise auf den Link **TCP** klicken, wird das Dialogfeld **Protokoll wählen** geöffnet.

### 7.5.5.3 Ändern einer Anwendungsregel

1. Klicken Sie auf der **Startseite** unter **Firewall** auf **Firewall konfigurieren**.  
Weitere Informationen zur **Startseite** finden Sie unter [Die Startseite](#) (Seite 4).
2. Klicken Sie im Bereich **Konfigurationen** neben dem zu konfigurierenden Standort auf **Konfigurieren**.
3. Klicken Sie auf die Registerkarte **Anwendungen**.
4. Wählen Sie die Anwendung aus der Liste aus und klicken Sie anschließend auf **Regel**. Sie können auch auf die Anwendung in der Liste doppelklicken.
5. Klicken Sie im Dialogfeld **Anwendungsregeln** auf **Bearbeiten**.
6. 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.
7. Wählen Sie im Bereich **Ereignisse, für die die Regel zutreffen soll** die Bedingungen aus, die eine Verbindung erfüllen muss, damit die Regel greift.
8. Wählen Sie im Bereich **Maßnahmen, die die Regel ergreifen soll Zulassen** oder **Sperren** aus.
9. Bei Auswahl der Option **Stateful Inspection** basieren die Antworten des Remote-Computers auf der ersten Verbindung.
10. Klicken Sie im Bereich **Regelbeschreibung** auf einen unterstrichenen Wert. Wenn Sie beispielsweise auf den Link **TCP** klicken, wird das Dialogfeld **Protokoll wählen** geöffnet.

#### 7.5.5.4 Kopieren einer Anwendungsregel

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

1. Klicken Sie auf der **Startseite** unter **Firewall** auf **Firewall konfigurieren**.  
Weitere Informationen zur **Startseite** finden Sie unter [Die Startseite](#) (Seite 4).
2. Klicken Sie im Bereich **Konfigurationen** neben dem zu konfigurierenden Standort auf **Konfigurieren**.
3. Klicken Sie auf die Registerkarte **Anwendungen**.
4. Wählen Sie die Anwendung aus der Liste aus und klicken Sie anschließend auf **Regel**.  
Sie können auch auf die Anwendung in der Liste doppelklicken.
5. Klicken Sie im Dialogfeld **Anwendungsregeln** auf **Kopieren**.

#### 7.5.5.5 Ändern der Priorität von Anwendungsregeln

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

So können Sie die Priorität von Anwendungsregeln ändern:

1. Klicken Sie auf der **Startseite** unter **Firewall** auf **Firewall konfigurieren**.  
Weitere Informationen zur **Startseite** finden Sie unter [Die Startseite](#) (Seite 4).
2. Klicken Sie im Bereich **Konfigurationen** neben dem zu konfigurierenden Standort auf **Konfigurieren**.
3. Klicken Sie auf die Registerkarte **Anwendungen**.
4. Wählen Sie die Anwendung aus der Liste aus und klicken Sie anschließend auf **Regel**.  
Sie können auch auf die Anwendung in der Liste doppelklicken.
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**.

#### 7.5.5.6 Löschen einer Anwendungsregel

1. Klicken Sie auf der **Startseite** unter **Firewall** auf **Firewall konfigurieren**.  
Weitere Informationen zur **Startseite** finden Sie unter [Die Startseite](#) (Seite 4).
2. Klicken Sie im Bereich **Konfigurationen** neben dem zu konfigurierenden Standort auf **Konfigurieren**.
3. Klicken Sie auf die Registerkarte **Anwendungen**.
4. Wählen Sie die Anwendung aus der Liste aus und klicken Sie anschließend auf **Regel**.
5. Klicken Sie im Dialogfeld **Anwendungsregeln** auf **Entfernen**.

#### 7.5.5.7 Zulassen versteckter Prozesse

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

Gelegentlich machen sich Schadprogramme diese Technik zunutze, um eine Firewall zu umgehen: Sie starten eine vertrauenswürdige Anwendung, die für sie auf das Netzwerk zugreift, auf das sie selbst keinen Zugriff haben.

Die Firewall sendet bei der ersten Erkennung eines versteckten Prozesses eine Meldung an die Management-Konsole (falls vorhanden).

So erlauben Sie Anwendungen den Start versteckter Prozesse:

1. Klicken Sie auf der **Startseite** unter **Firewall** auf **Firewall konfigurieren**.  
Weitere Informationen zur **Startseite** finden Sie unter [Die Startseite](#) (Seite 4).
2. Klicken Sie im Bereich **Konfigurationen** neben dem zu konfigurierenden Standort auf **Konfigurieren**.
3. Klicken Sie auf die Registerkarte **Prozesse**.
4. Klicken Sie im oberen Bereich auf **Hinzufügen**.
5. Suchen Sie die gewünschte Anwendung und doppelklicken Sie darauf.

Im interaktiven Modus kann die Firewall bei Erkennung eines neuen Launchers einen Lerndialog anzeigen.

- [Aktivieren des interaktiven Modus](#) (Seite 55)
- [Aktivieren von Lerndialogen zu versteckten Prozessen](#) (Seite 56)

#### 7.5.5.8 Zulassen von Raw-Sockets

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.

Die Firewall sendet bei der ersten Erkennung eines Raw-Sockets eine Meldung an die Management-Konsole (falls vorhanden).

So lassen Sie den Zugriff über Raw-Sockets zu:

1. Klicken Sie auf der **Startseite** unter **Firewall** auf **Firewall konfigurieren**.  
Weitere Informationen zur **Startseite** finden Sie unter [Die Startseite](#) (Seite 4).
2. Klicken Sie im Bereich **Konfigurationen** neben dem zu konfigurierenden Standort auf **Konfigurieren**.
3. Klicken Sie auf die Registerkarte **Prozesse**.
4. Klicken Sie auf **Hinzufügen**.
5. Suchen Sie die gewünschte Anwendung und doppelklicken Sie darauf.

Im interaktiven Modus kann die Firewall bei Erkennung eines neuen Raw-Sockets einen Lerndialog anzeigen.

- [Aktivieren des interaktiven Modus](#) (Seite 55)
- [Aktivieren von Raw-Socket-Lerndialogen](#) (Seite 57)

### 7.5.5.9 Authentifizieren von Anwendungen mit Hilfe von Prüfsummen

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. Falls eine Prüfsumme nicht erkannt wird oder sich geändert hat, wird die entsprechende Anwendung gesperrt. Im interaktiven Modus wird ein Lerndialog geöffnet, in dem der Benutzer über die weitere Vorgehensweise entscheiden darf.

Außerdem sendet die Firewall bei der ersten Erkennung einer neuen oder geänderten Anwendung auch eine Meldung an die Management-Konsole (falls vorhanden).

So fügen Sie eine neue Prüfsumme hinzu:

1. Klicken Sie auf der **Startseite** unter **Firewall** auf **Firewall konfigurieren**.  
Weitere Informationen zur **Startseite** finden Sie unter [Die Startseite](#) (Seite 4).
2. Klicken Sie im Bereich **Konfigurationen** neben dem zu konfigurierenden Standort auf **Konfigurieren**.
3. Klicken Sie auf die Registerkarte **Prüfsummen**.
4. Klicken Sie auf **Hinzufügen**.
5. Suchen Sie die gewünschte Anwendung und doppelklicken Sie darauf.

Im interaktiven Modus kann die Firewall Lerndialoge anzeigen, wenn neue oder geänderte Anwendungen erkannt werden.

- [Aktivieren des interaktiven Modus](#) (Seite 55)
- [Aktivieren von Lerndialogen zu versteckten Prozessen](#) (Seite 56)

## 7.6 Standortspezifische Konfiguration

### 7.6.1 Allgemeine Informationen

Die standortspezifische Konfiguration ist eine Funktion von Sophos Client Firewall, bei der Computern je nach Standort Regeln zugewiesen werden.

Wenn Laptops beispielsweise nicht im Büro eingesetzt werden, müssen ihnen möglicherweise strengere Firewallregeln zugewiesen werden, da der zusätzliche Schutz durch die Netzwerk-Firewall wegfällt.

Wenn Sie diese Funktion nutzen möchten, legen Sie zunächst Ihre primären Standorte fest (z.B. die Büronetzwerke). Wenn die Firewall erkennt, dass eine Verbindung zu einem primären Standort besteht, findet die primäre Konfiguration Anwendung.

- [Festlegen der primären Standorte](#) (Seite 68)

Legen Sie jetzt die sekundäre Konfiguration fest. Wenn die Firewall erkennt, dass **keine** Verbindung zu einem primären Standort besteht, greift die sekundäre Konfiguration.

- [Festlegen des sekundären Standorts](#) (Seite 68)

## 7.6.2 Festlegen der primären Standorte

Wenn die Firewall feststellt, dass eine Verbindung zu einem primären Standort besteht, wird die primäre Konfiguration angewandt.

1. Klicken Sie auf der **Startseite** unter **Firewall** auf **Firewall konfigurieren**.  
Weitere Informationen zur **Startseite** finden Sie unter [Die Startseite](#) (Seite 4).
2. Klicken Sie auf die Registerkarte **Standortererkennung**.
3. Klicken Sie im Bereich **Erkennungsmethode** auf die Schaltfläche **Konfigurieren** neben der gewünschten Option:

Option	Beschreibung
<b>Standort über DNS erkennen</b>	Sie können eine Liste mit Domännennamen und erwarteten IP-Adressen erstellen, die Ihren primären Standorten entsprechen.
<b>Standort über Gateway-MAC-Adresse erkennen</b>	Sie können eine Liste mit Gateway-MAC-Adressen erstellen, die Ihren primären Standorten entsprechen.

In beiden Fällen untersucht die Firewall die Liste der primären Standorte oder löst diese auf. Wenn eine Übereinstimmung vorliegt, wird davon ausgegangen, dass eine Verbindung zu einem primären Standort besteht.

4. Befolgen Sie die Anweisungen auf dem Bildschirm.

## 7.6.3 Festlegen des sekundären Standorts

Wenn die Firewall feststellt, dass keine Verbindung zum primären Standort besteht, wird auf die Konfiguration des sekundären Standorts zurückgegriffen.

1. Klicken Sie auf der **Startseite** unter **Firewall** auf **Firewall konfigurieren**.  
Weitere Informationen zur **Startseite** finden Sie unter [Die Startseite](#) (Seite 4).
2. Aktivieren Sie das Kontrollkästchen **Konfiguration für einen sekundären Standort**.

Konfigurieren Sie den sekundären Standort. Weitere Informationen können Sie dem Abschnitt *Konfigurieren der Firewall* entnehmen.

## 7.7 Firewall-Meldungen

### 7.7.1 Allgemeine Informationen

Standardmäßig meldet die Firewall Änderungen, Ereignisse und Fehler an die Management-Konsole.

#### 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 die Management-Konsole abweichen. Dies ist kein Zufall. In diesem Fall können Sie Alerts zu Abweichungen von der Richtlinie an die Management-Konsole **deaktivieren**.

Weitere Informationen finden Sie unter [Aktivieren/Deaktivieren der Meldungen über lokale Änderungen](#) (Seite 69).

### Firewall-Ereignisse

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

Sie können Ereignismeldungen an die Management-Konsole deaktivieren.

Weitere Informationen finden Sie unter [Deaktivieren von Meldungen über unbekanntes Datenbewegungen](#) (Seite 70).

## 7.7.2 Aktivieren/Deaktivieren der Meldungen über lokale Änderungen

Wenn Ihre 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 die Management-Konsole. 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. Klicken Sie auf der **Startseite** unter **Firewall** auf **Firewall konfigurieren**.  
Weitere Informationen zur **Startseite** finden Sie unter [Die Startseite](#) (Seite 4).
2. Klicken Sie im Bereich **Konfigurationen** neben dem zu konfigurierenden Standort auf **Konfigurieren**.
3. Deaktivieren Sie auf der Registerkarte **Allgemein** unter **Meldungen** die Option **Lokal geänderte globale Regeln, Anwendungen, Prozesse und Prüfsummen an die Management-Konsole melden**.

Wenn Sie die Meldungen wieder aktivieren möchten, markieren Sie die Option.

### 7.7.3 Deaktivieren von Meldungen über unbekannte Datenbewegungen

Sie können die Meldungen der Firewall über unbekannte Datenbewegungen an die Management-Konsole deaktivieren. Datenbewegungen, die keinen Regeln entsprechen, werden von der Firewall als „unbekannt“ eingestuft.

So deaktivieren Sie die Meldungen:

1. Klicken Sie auf der **Startseite** unter **Firewall** auf **Firewall konfigurieren**.  
Weitere Informationen zur **Startseite** finden Sie unter [Die Startseite](#) (Seite 4).
2. Klicken Sie im Bereich **Konfigurationen** neben dem zu konfigurierenden Standort auf **Konfigurieren**.
3. Aktivieren Sie auf der Karte **Allgemein** unter **Sperren** das Kontrollkästchen **Anwendungen anhand von Prüfsummen authentifizieren**.
4. Deaktivieren Sie unter **Meldungen** das Kontrollkästchen **Neue und geänderte Anwendungen an die Management-Konsole melden**.

### 7.7.4 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 deaktivieren Sie die Firewall-Fehlermeldungen:

1. Klicken Sie auf der **Startseite** unter **Firewall** auf **Firewall konfigurieren**.  
Weitere Informationen zur **Startseite** finden Sie unter [Die Startseite](#) (Seite 4).
2. Klicken Sie im Bereich **Konfigurationen** neben dem zu konfigurierenden Standort auf **Konfigurieren**.
3. Deaktivieren Sie auf der Registerkarte **Allgemein** unter **Meldungen** die Option **Fehler an die Management-Konsole melden**.

### 7.7.5 Konfigurieren von Desktop-Benachrichtigungen

Sie können festlegen, welche Firewall-Meldungen in den Sprechblasen auf dem Desktop angezeigt werden sollen.

Im interaktiven Modus werden Meldungen zu unbekanntem Anwendungen und Datenfluss nicht in Form von Sprechblasen, sondern von Lerndialogen angezeigt.

1. Klicken Sie auf der **Startseite** unter **Firewall** auf **Firewall konfigurieren**.  
Weitere Informationen zur **Startseite** finden Sie unter [Die Startseite](#) (Seite 4).
2. Klicken Sie im Bereich **Konfigurationen** neben dem zu konfigurierenden Standort auf **Konfigurieren**.
3. Wählen Sie auf der Registerkarte **Allgemein** im Bereich **Desktop-Benachrichtigungen** eine der folgenden Optionen aus:
  - Wenn Sprechblasenmeldungen bei Warnungen und Fehlern angezeigt werden sollen, wählen Sie die Option **Warnmeldungen und Fehler anzeigen** aus.

- Wenn Sprechblasenmeldungen bei unbekanntem Anwendungen und Datenbewegungen angezeigt werden sollen, wählen Sie die Option **Unbekannte Anwendungen und Datenbewegungen anzeigen** aus.

## 7.8 Firewall-Protokolle

### 7.8.1 Der Log Viewer

Mit dem Log Viewer von Sophos Client Firewall können Sie nähere Informationen aufrufen, filtern und speichern. Folgende Optionen stehen zur Auswahl:

- Alle Verbindungen
- Zugelassene oder gesperrte Verbindungen
- Firewall-Ereignisse
- Das Systemprotokoll

### 7.8.2 Öffnen des Firewall Log Viewers

- ❖ Klicken Sie auf der **Startseite** unter **Firewall** auf **Firewall-Protokoll öffnen**. Weitere Informationen zur **Startseite** finden Sie unter [Die Startseite](#) (Seite 4).

### 7.8.3 Konfigurieren des Firewall-Protokolls

Größe und Inhalt des Firewall-Protokolls lassen sich ändern:

1. Klicken Sie auf der **Startseite** unter **Firewall** auf **Firewall konfigurieren**. Weitere Informationen zur **Startseite** finden Sie unter [Die Startseite](#) (Seite 4).
2. Öffnen Sie die Registerkarte **Protokoll**.
3. Um die Größe des Protokolls zu bestimmen, wählen Sie eine der folgenden Optionen:
  - Wenn Sie das Datenbankwachstum nicht einschränken möchten, klicken Sie auf **Alle Datensätze behalten**.
  - Klicken Sie zum Entfernen alter Datensätze auf **Alte Datensätze löschen** und konfigurieren Sie die **Einstellungen zum Löschen des Protokolls**.
4. Unter **Einstellungen zum Löschen des Protokolls** stehen Ihnen weitere Optionen zur Auswahl:
  - Klicken Sie auf die Option **Datensätze löschen nach** und legen Sie anschließend eine Zahl im Feld **Tage** fest.
  - Klicken Sie auf das Kontrollkästchen **Nicht mehr behalten als** und legen Sie eine Zahl im Feld **Datensätze** fest.
  - Klicken Sie auf das Kontrollkästchen **Größe unter** und legen Sie eine Zahl im Feld **MB** fest.

## 7.8.4 Ein-/Ausblenden von Elementen im Firewall Log Viewer

1. Klicken Sie auf der **Startseite** unter **Firewall** auf **Firewall-Protokoll öffnen**.  
Weitere Informationen zur **Startseite** finden Sie unter [Die Startseite](#) (Seite 4).
2. Klicken Sie im Menü **Ansicht** auf **Layout**.
3. Wählen Sie im Dialogfeld **Ansicht anpassen** die Elemente aus, die ein- bzw. ausgeblendet werden sollen:
  - Die **Konsolenstruktur** wird im linken Fensterbereich angezeigt.
  - Die **Symbolleiste** wird im oberen Bereich des Firewall Log Viewers angezeigt.
  - Die **Beschreibungsleiste** wird über den Daten im rechten Fensterbereich angezeigt.
  - Die **Statusleiste** wird im unteren Bereich des Firewall Log Viewers angezeigt.

## 7.8.5 Anpassen des Datenformats

Sie können festlegen, in welchem Format Objekte im Firewall-Protokoll dargestellt werden sollen. Die folgenden Optionen stehen zur Auswahl:

- Darstellung von Ports als Zahl oder Name, z.B. **80** oder **HTTP**.
- Darstellung von Anwendungen in Form von Symbolen und/oder Dateipfaden.
- Angabe der Einheit der Datenübertragungsrate (**KB** oder **MB**).
- Ein-/Ausblenden der Gitternetzlinien.

So können Sie das Datenformat anpassen:

1. Klicken Sie auf der **Startseite** unter **Firewall** auf **Firewall-Protokoll öffnen**.  
Weitere Informationen zur **Startseite** finden Sie unter [Die Startseite](#) (Seite 4).
2. Klicken Sie im Menü **Ansicht** auf **Anpassen**.
3. Wählen Sie die gewünschten Optionen aus.

## 7.8.6 Ein-/Ausblenden von Spalten im Firewall Log Viewer

1. Klicken Sie auf der **Startseite** unter **Firewall** auf **Firewall-Protokoll öffnen**.  
Weitere Informationen zur **Startseite** finden Sie unter [Die Startseite](#) (Seite 4).
2. Klicken Sie auf ein Objekt im Konsolenstamm, zu dem Spalten im Fenster „Details“ angezeigt werden.
3. Wählen Sie im Menü **Ansicht** die Option **Spalten hinzufügen/entfernen**.  
Oder rechtsklicken Sie auf eine Spaltenüberschrift.
4. Verfahren Sie im Dialogfenster **Spalten** anhand einer der folgenden Methoden:
  - Deaktivieren Sie zum Ausblenden einer Spalte das entsprechende Kontrollkästchen.
  - Markieren Sie zum Einblenden einer Spalte das entsprechende Kontrollkästchen.

## 7.8.7 Umsortieren der Spalten im Firewall Log Viewer

1. Klicken Sie auf der **Startseite** unter **Firewall** auf **Firewall-Protokoll öffnen**.  
Weitere Informationen zur **Startseite** finden Sie unter [Die Startseite](#) (Seite 4).
2. Klicken Sie auf ein Objekt im Konsolenstamm, zu dem Spalten im Fenster „Details“ angezeigt werden.
3. Wählen Sie im Menü **Ansicht** die Option **Spalten hinzufügen/entfernen**.  
Oder rechtsklicken Sie auf eine Spaltenüberschrift.
4. Klicken Sie im Dialogfeld **Spalten** auf einen Spaltennamen und klicken Sie anschließend zum Ändern der Spaltenposition auf **Nach oben** bzw. **Nach unten**.

### Hinweise

- Sie können Spaltenüberschriften auch mit der Maus nach links oder rechts verschieben und so die Spaltenposition ändern. Die neue Spaltenposition ist beim Ziehen der Spalte markiert.
- Sie können die Spaltengröße durch Ziehen der Spaltenüberschriften mit der Maus variieren.

## 7.8.8 Filtern der Datensätze im Firewall-Protokoll

Sie können die Firewall Datensätze durch Erstellen von Filtern sortieren.

So können Sie die Firewall Datensätze filtern:

1. Klicken Sie auf der **Startseite** unter **Firewall** auf **Firewall-Protokoll öffnen**.  
Weitere Informationen zur **Startseite** finden Sie unter [Die Startseite](#) (Seite 4).
2. Wählen Sie das gewünschte Protokoll im Konsolenstamm aus.
3. Klicken Sie im Menü **Maßnahme** auf **Filter hinzufügen**.
4. Befolgen Sie die Anweisungen des **Filter-Assistenten**.

Der Filter wird im Konsolenstamm unmittelbar unter dem Knoten des gewünschten Protokolls angezeigt.

## 7.8.9 Exportieren aller Firewall-Protokolldatensätze

So exportieren Sie alle Firewall-Protokolldatensätze in eine Text- oder CSV-Datei:

1. Klicken Sie auf der **Startseite** unter **Firewall** auf **Firewall-Protokoll öffnen**.  
Weitere Informationen zur **Startseite** finden Sie unter [Die Startseite](#) (Seite 4).
2. Wählen Sie das gewünschte Protokoll im Konsolenstamm aus.
3. Rechtsklicken Sie auf die Liste und klicken Sie auf **Alle Datensätze exportieren**.
4. Geben Sie einen Dateinamen in das Textfeld **Dateiname** ein.
5. Wählen Sie aus dem Dropdown-Menü **Dateityp** den gewünschten Dateityp aus.

## 7.8.10 Exportieren ausgewählter Firewall-Protokolldatensätze

So exportieren Sie ausgewählte Firewall-Protokolldatensätze in eine Text- oder CSV-Datei:

1. Klicken Sie auf der **Startseite** unter **Firewall** auf **Firewall-Protokoll öffnen**.  
Weitere Informationen zur **Startseite** finden Sie unter [Die Startseite](#) (Seite 4).
2. Wählen Sie das gewünschte Protokoll im Konsolenstamm aus.
3. Wählen Sie die gewünschten Einträge aus.  
Wenn die Einträge häufig aktualisiert werden, deaktivieren Sie im Menü **Ansicht** das Kontrollkästchen **Automatische Aktualisierung**.
4. Klicken Sie im Menü **Maßnahme** auf **Ausgewählte Datensätze exportieren**.
5. Geben Sie einen Dateinamen in das Textfeld **Dateiname** ein.
6. Wählen Sie aus dem Dropdown-Menü **Dateityp** den gewünschten Dateityp aus.

## 8 Sophos AutoUpdate

### 8.1 Sofort-Updates

Standardmäßig sucht Sophos AutoUpdate im 5-Minuten-Takt nach Updates, wenn Computer permanent mit dem Unternehmensnetzwerk verbunden sind, bzw. im 60-Minuten-Takt, wenn Computer nicht permanent mit dem Unternehmensnetzwerk verbunden sind.

Wenn Sie eine Internet- oder Netzwerkverbindung per Einwahl herstellen, führt Sophos AutoUpdate bei Verbindungsherstellung und daraufhin alle 60 Minuten ein Update durch.

So veranlassen Sie ein Sofort-Update:

- ❖ Rechtsklicken Sie auf das Sophos Endpoint Security and Control-Symbol im Statusbereich der Taskleiste und wählen Sie die Option **Jetzt updaten**.

### 8.2 Update-Zeitpläne

**Wichtig:** Wenn Sophos Endpoint Security and Control über eine Management-Konsole verwaltet wird, werden hier vorgenommene Änderungen eventuell nicht berücksichtigt.

Zeitpunkt und Häufigkeit der Sophos AutoUpdate Updates lassen sich individuell festlegen.

1. Wählen Sie im Menü **Konfigurieren** die Option **Updates**.
2. Klicken Sie auf die Registerkarte **Zeitplan**.
3. Wählen Sie **Automatische Updates aktivieren** und legen Sie die Update-Häufigkeit in Minuten fest.

Wenn die upgedateten Dateien aus dem Unternehmensnetzwerk heruntergeladen werden, werden standardmäßig alle fünf Minuten Updates durchgeführt.

Wenn die Updates vom Sophos Server über das Internet heruntergeladen werden, steht nicht häufiger als alle 60 Minuten ein neues Update für Sophos AutoUpdate zum Abruf bereit.

### 8.3 Auswahl der Update-Quelle

Wenn Sophos AutoUpdate automatisch upgedatet werden soll, müssen Sie eine Update-Quelle angeben.

1. Wählen Sie im Menü **Konfigurieren** die Option **Updates**.
2. Klicken Sie auf die Registerkarte **Primärer Standort**.
3. Geben Sie in der Liste **Adresse** den UNC-Pfad oder die URL des Update-Servers an.

Wählen Sie **Sophos** in der **Adressenliste** aus, um Updates über das Internet direkt von Sophos zu beziehen.

4. Geben Sie in das Feld **Benutzername** den Benutzernamen zur Anmeldung am Update-Server ein.  
Wenn der **Benutzername** die Domäne enthalten muss, verwenden Sie die Form *Domäne\Benutzername*.
5. Geben Sie in das Feld **Kennwort** Ihr Kennwort ein und drücken Sie die Eingabetaste.

## 8.4 Festlegen einer zweiten Update-Quelle

Sie können eine alternative Update-Quelle angeben. Für den Fall, dass ein Update über die gewöhnliche Quelle nicht möglich ist, kann eine alternative Quelle angegeben werden.

1. Wählen Sie im Menü **Konfigurieren** die Option **Updates**.
2. Klicken Sie auf die Registerkarte **Sekundärer Standort**.
3. Geben Sie in der Liste **Adresse** den UNC-Pfad oder die URL des Update-Servers an.  
Wählen Sie **Sophos** in der **Adressenliste** aus, um Updates über das Internet direkt von Sophos zu beziehen.
4. Geben Sie in das Feld **Benutzername** den Benutzernamen zur Anmeldung am Update-Server ein.  
Wenn der **Benutzername** die Domäne enthalten muss, verwenden Sie die Form *Domäne\Benutzername*.
5. Geben Sie in das Feld **Kennwort** Ihr Kennwort ein und drücken Sie die Eingabetaste.

## 8.5 Updates über einen Proxyserver

Wenn Sophos AutoUpdate Updates über das Internet bezieht, müssen Sie die Details eines Proxyservers eingeben, über den die Internetverbindung hergestellt wird.

1. Wählen Sie im Menü **Konfigurieren** die Option **Updates**.
2. Klicken Sie auf die Registerkarte **Primärquelle** oder **Sekundärquelle**.
3. Klicken Sie auf **Proxy-Details**.
4. Aktivieren Sie das Kontrollkästchen **Zugriff über Proxy herstellen**.
5. Geben Sie die **Adresse** und den **Port** des Proxyservers an.
6. Geben Sie die Zugangsdaten ein, d.h. **Benutzername** und **Kennwort**.  
Wenn der Benutzername für eine bestimmte Domäne gilt, verwenden Sie das Format *Domäne\Benutzername*.

## 8.6 Updates über eine Einwahlverbindung

So veranlassen Sie ein Update über eine Einwahlverbindung:

1. Wählen Sie im Menü **Konfigurieren** die Option **Updates**.
2. Klicken Sie auf die Registerkarte **Zeitplan**.
3. Wählen Sie **Bei Einwahl nach Updates suchen**.

Sophos AutoUpdate führt bei der Verbindungsherstellung ein Update durch.

## 8.7 Verringern der Übertragungsrate für Updates

Wenn Sophos AutoUpdate nicht die gesamte Bandbreite auf Updates verwenden soll, verringern Sie die Datenübertragungsrate.

1. Wählen Sie im Menü **Konfigurieren** die Option **Updates**.
2. Klicken Sie auf die Registerkarte **Primärquelle** oder **Sekundärquelle**.
3. Klicken Sie auf **Erweitert**.
4. Wählen Sie die Option **Übertragungsrate verringern** und verschieben Sie den Regler in den gewünschten Bereich.

**Hinweis:** Wird eine zu hohe Rate ausgewählt, nutzt Sophos AutoUpdate die gesamte Bandbreite.

## 8.8 Protokollieren von Updates

Sophos AutoUpdate kann alle Update-Vorgänge in einer Protokolldatei erfassen.

1. Wählen Sie im Menü **Konfigurieren** die Option **Updates**.
2. Öffnen Sie die Registerkarte **Protokollierung**.
3. Aktivieren Sie die Option **Update-Vorgänge protokollieren**.
4. Legen Sie im Feld **Max. Protokollgröße** die gewünschte maximale Protokollgröße in MB fest.
5. Wählen Sie als **Protokollierungsstufe** entweder **Normal** oder **Ausführlich**.

In ausführlichen Protokollen werden mehr Aktivitäten protokolliert als gewöhnlich, was sich auch auf die Protokollgröße auswirkt. Wählen Sie diese Option am besten nur zur Fehlersuche, wenn mehrere Details von Vorteil sein können.

## 8.9 Öffnen des Update-Protokolls

1. Wählen Sie im Menü **Konfigurieren** die Option **Updates**.
2. Öffnen Sie die Registerkarte **Protokollierung**.
3. Klicken Sie auf **Protokolldatei öffnen**.

## 9 Sophos Manipulationsschutz

### 9.1 Allgemeine Informationen

Mit dem Manipulationsschutz können Sie verhindern, dass nicht autorisierte Benutzer (Benutzer ohne hinreichende Fachkenntnisse) sowie bekannte Malware Sophos Sicherheitssoftware deinstallieren bzw. über Sophos Endpoint Security and Control deaktivieren.

**Hinweis:** Der Manipulationsschutz schützt nicht vor Benutzern mit ausgeprägtem Technikverständnis. Auch bietet die Funktion keinen Schutz vor Malware, die eigens dafür konzipiert wurde, das Betriebssystem zu untergraben und die Erkennung zu umgehen. Diese Malware-Art wird ausschließlich von Scans auf Threats und verdächtigem Verhalten erkannt. (Nähere Informationen entnehmen Sie bitte dem Abschnitt „Sophos Anti-Virus“.)

#### Wie wirkt sich der Manipulationsschutz auf die Benutzer auf diesem Computer aus?

##### SophosUsers und SophosPowerUsers

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.

**SophosUsers** oder **SophosPowerUsers** können den Manipulationsschutz nicht deaktivieren.

Nähere Informationen zu den Aufgaben, die die jeweiligen Sophos Gruppen ausführen können, finden Sie unter [Allgemeine Informationen](#) (Seite 5).

##### SophosAdministrators

Mitglieder der Gruppe **SophosAdministrators** können den Manipulationsschutz aktivieren bzw. deaktivieren.

Wenn **Sophos Endpoint Security and Control** auf diesem Computer über eine Management-Konsole verwaltet wird, bestimmt die in der Konsole eingerichtete Manipulationsschutz-Richtlinie die Konfiguration des Manipulationsschutzes sowie das Kennwort. Wenn der Manipulationsschutz über die Konsole aktiviert wird und Sie eine der im Folgenden genannten Aktionen durchführen möchten, lassen Sie sich das Kennwort von Ihrem Konsolen-Administrator geben.

Wenn Sie Mitglied der Gruppe **SophosAdministrators** sind und der Manipulationsschutz aktiviert ist, können Sie die folgenden Aufgaben nur nach Angabe des Manipulationsschutzkennworts durchführen:

- Erneute Konfiguration der Einstellungen von On-Access-Scans bzw. der Erkennung verdächtigen Verhaltens. Weitere Informationen finden Sie unter [Aktivieren des Manipulationsschutz-Kennworts zum Konfigurieren der Software](#) (Seite 81).
- Deaktivieren des Manipulationsschutzes. Weitere Informationen finden Sie unter [Deaktivieren des Manipulationsschutzes](#) (Seite 79).
- Deinstallation von Komponenten von Sophos Endpoint Security and Control (Sophos Anti-Virus, Sophos Client Firewall, Sophos AutoUpdate oder Sophos Remote Management System) über die Systemsteuerung.

- Deinstallation von Sophos SafeGuard Disk Encryption über die Systemsteuerung.

Ein Mitglied der Gruppe **SophosAdministrators**, der das Kennwort nicht kennt, kann nur die oben erwähnten Aufgaben nicht ausführen.

Wenn der Manipulationsschutz nicht aktiviert ist, jedoch zu einem früheren Zeitpunkt ein Kennwort eingerichtet wurde, können Sie den Manipulationsschutz nur wieder aktivieren, indem Sie sich über die Option **Benutzer authentifizieren** authentifizieren. Nach der Deaktivierung des Manipulationsschutzes stehen wieder alle Konfigurationsoptionen der Gruppe **SophosAdministrators** zur Verfügung. Nähere Informationen zum erneuten Aktivieren des Manipulationsschutzes finden Sie unter [Erneute Aktivierung des Manipulationsschutzes](#) (Seite 80).

## 9.2 Aktivieren des Manipulationsschutzes

**Wichtig:** Wenn **Sophos Endpoint Security and Control** über eine Management-Konsole verwaltet wird, werden hier vorgenommene Änderungen eventuell nicht berücksichtigt.

Bei der Erstinstallation von **Sophos Endpoint Security and Control** ist der Manipulationsschutz deaktiviert. Mitglieder der Gruppe **SophosAdministrators** können den Manipulationsschutz aktivieren.

So aktivieren Sie den Manipulationsschutz:

1. Klicken Sie auf der **Startseite** unter **Manipulationsschutz** auf die Option **Manipulationsschutz konfigurieren**.  
Nähere Informationen zur **Startseite** finden Sie unter [Die Startseite](#) (Seite 4).
2. Wählen Sie im Dialogfeld **Manipulationsschutz-Konfiguration** das Kontrollkästchen **Manipulationsschutz aktivieren** aus.
3. Klicken Sie unter dem **Kennwortfeld** auf **Festlegen**. Geben Sie das Kennwort in das Feld **Manipulationsschutz-Kennwort** ein und bestätigen Sie es.

**Tipp:** Das Kennwort muss mindestens 8 Zeichen umfassen und sich aus Groß- und Kleinbuchstaben sowie Zahlen zusammensetzen.

## 9.3 Deaktivieren des Manipulationsschutzes

**Wichtig:** Wenn **Sophos Endpoint Security and Control** über eine Management-Konsole verwaltet wird, werden hier vorgenommene Änderungen eventuell nicht berücksichtigt.

Mitglieder der Gruppe **SophosAdministrators** können den Manipulationsschutz deaktivieren.

So deaktivieren Sie den Manipulationsschutz:

1. Wenn Sie sich noch nicht authentifiziert haben und die Option **Manipulationsschutz konfigurieren** auf der **Startseite** nicht verfügbar ist, befolgen Sie bitte zunächst die Anweisungen im Abschnitt [Aktivieren des Manipulationsschutz-Kennworts zum Konfigurieren der Software](#) (Seite 81), bevor Sie mit Schritt 2 fortfahren.

2. Klicken Sie auf der **Startseite** unter **Manipulationsschutz** auf die Option **Manipulationsschutz konfigurieren**.  
Nähere Informationen zur **Startseite** finden Sie unter [Die Startseite](#) (Seite 4).
3. Deaktivieren Sie im Dialogfeld **Manipulationsschutz-Konfiguration** das Kontrollkästchen **Manipulationsschutz aktivieren** und klicken Sie auf **OK**.

## 9.4 Erneute Aktivierung des Manipulationsschutzes

**Wichtig:** Wenn **Sophos Endpoint Security and Control** über eine Management-Konsole verwaltet wird, werden hier vorgenommene Änderungen eventuell nicht berücksichtigt.

Mitglieder der Gruppe **SophosAdministrators** können den Manipulationsschutz wieder aktivieren.

So aktivieren Sie den Manipulationsschutz erneut:

1. Klicken Sie auf der **Startseite** unter **Manipulationsschutz** auf die Option **Benutzer authentifizieren**.  
Nähere Informationen zur **Startseite** finden Sie unter [Die Startseite](#) (Seite 4).
2. Geben Sie in das Dialogfeld **Manipulationsschutz-Authentifizierung** das Manipulationsschutz-Kennwort ein und klicken Sie auf **OK**.
3. Klicken Sie auf der **Startseite** unter **Manipulationsschutz** auf die Option **Manipulationsschutz konfigurieren**.
4. Wählen Sie im Dialogfeld **Manipulationsschutz-Konfiguration** das Kontrollkästchen **Manipulationsschutz aktivieren** aus.

## 9.5 Informationen zum Manipulationsschutz-Kennwort

Wenn der Manipulationsschutz aktiviert ist, müssen Sie zur Konfiguration von On-Access-Scans und der Erkennung verdächtigen Verhaltens sowie zur Deaktivierung des Manipulationsschutzes das Manipulationsschutz-Kennwort eingeben. Nur Mitglieder der Gruppe „SophosAdministrators“ sind hierzu berechtigt.

Das Manipulationsschutz-Kennwort muss nur einmal nach dem Öffnen von **Sophos Endpoint Security and Control** eingegeben werden. Wenn Sie **Sophos Endpoint Security and Control** jedoch schließen und wieder öffnen, müssen Sie das Kennwort erneut eingeben.

Wenn Sie eine Komponente von **Sophos Endpoint Security and Control** deinstallieren möchten, müssen Sie vor der Deaktivierung des Manipulationsschutzes zur Deinstallation der Software zunächst das Manipulationsschutz-Kennwort eingeben.

Wenn der Manipulationsschutz nicht aktiviert ist, jedoch zu einem früheren Zeitpunkt ein Kennwort eingerichtet wurde, können Sie den Manipulationsschutz nur durch Eingabe des Kennworts wieder aktivieren.

Unter folgenden Voraussetzungen muss zur Aktivierung des Manipulationsschutzes das Manipulationsschutz-Kennwort eingegeben werden:

- Sie haben bereits ein Manipulationsschutz-Kennwort erstellt und den Manipulationsschutz in der Folge deaktiviert.

- In der Management-Konsole wurde ein Manipulationsschutz-Kennwort erstellt, der Manipulationsschutz ist jedoch nicht aktiviert.

## 9.6 Aktivieren des Manipulationsschutz-Kennworts zum Konfigurieren der Software

Mitglieder der Gruppe **SophosAdministrators** können sich durch Eingabe des Manipulationsschutz-Kennworts authentifizieren.

Verfahren Sie hierzu wie folgt:

1. Klicken Sie auf der **Startseite** unter **Manipulationsschutz** auf die Option **Benutzer authentifizieren**.  
Nähere Informationen zur **Startseite** finden Sie unter [Die Startseite](#) (Seite 4).
2. Geben Sie in das Dialogfeld **Manipulationsschutz-Authentifizierung** das Manipulationsschutz-Kennwort ein und klicken Sie auf **OK**.

## 9.7 Ändern des Manipulationsschutz-Kennworts

**Wichtig:** Wenn **Sophos Endpoint Security and Control** über eine Management-Konsole verwaltet wird, werden hier vorgenommene Änderungen eventuell nicht berücksichtigt.

Nur Mitglieder der Gruppe **SophosAdministrators** dürfen das Manipulationsschutz-Kennwort ändern.

So ändern Sie das Manipulationsschutz-Kennwort:

1. Wenn Sie sich noch nicht authentifiziert haben und die Option **Manipulationsschutz konfigurieren** auf der **Startseite** nicht verfügbar ist, befolgen Sie bitte zunächst die Anweisungen im Abschnitt [Aktivieren des Manipulationsschutz-Kennworts zum Konfigurieren der Software](#) (Seite 81), bevor Sie mit Schritt 2 fortfahren.
2. Klicken Sie auf der **Startseite** unter **Manipulationsschutz** auf die Option **Manipulationsschutz konfigurieren**.  
Nähere Informationen zur **Startseite** finden Sie unter [Die Startseite](#) (Seite 4).
3. Klicken Sie im Dialogfeld **Manipulationsschutz-Konfiguration** unter dem **Kennwortfeld** auf **Ändern**.
4. 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.

## 9.8 Deinstallieren von Sophos Sicherheitssoftware

Mitglieder der Gruppe **SophosAdministrators** können Sophos Sicherheitssoftware über die Systemsteuerung deinstallieren:

- Komponenten von Sophos Endpoint Security and Control (Sophos Anti-Virus, Sophos Client Firewall, Sophos AutoUpdate oder Sophos Remote Management System)
- Sophos SafeGuard Disk Encryption

So deinstallieren Sie Sophos Sicherheitssoftware, wenn der Manipulationsschutz aktiviert ist:

1. Klicken Sie auf der **Startseite** unter **Manipulationsschutz** auf die Option **Benutzer authentifizieren**.  
Nähere Informationen zur **Startseite** finden Sie unter [Die Startseite](#) (Seite 4).
2. Geben Sie in das Dialogfeld **Manipulationsschutz-Authentifizierung** das Manipulationsschutz-Kennwort ein und klicken Sie auf **OK**.
3. Klicken Sie auf der **Startseite** unter **Manipulationsschutz** auf die Option **Manipulationsschutz konfigurieren**.
4. Deaktivieren Sie im Dialogfeld **Manipulationsschutz-Konfiguration** das Kontrollkästchen **Manipulationsschutz aktivieren** und klicken Sie auf **OK**.  
Der Manipulationsschutz wurde deaktiviert.
5. Öffnen Sie in der **Systemsteuerung** das Dienstprogramm **Software**, suchen Sie die Software, die Sie entfernen möchten, und klicken Sie auf **Ändern/Entfernen** bzw. **Entfernen**. Befolgen Sie die Anweisungen zur Deinstallation der Software auf dem Bildschirm.

## 9.9 Aufrufen des Protokolls zum Manipulationsschutz

Im Manipulationsschutz-Protokoll werden die beiden folgenden Ereignisarten verzeichnet:

- Erfolgreiche Manipulationsschutz-Authentifizierungsereignisse (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).

Nur Mitglieder der Gruppe **SophosAdministrators** dürfen das Manipulationsschutz-Protokoll aufrufen.

So können Sie das Manipulationsschutz-Protokoll aufrufen:

- ❖ Klicken Sie auf der **Startseite** unter **Manipulationsschutz konfigurieren** auf die Option **Manipulationsschutz-Protokoll anzeigen**.  
Weitere Informationen zur **Startseite** finden Sie unter [Die Startseite](#) (Seite 4).

Aus der Protokollseite können Sie das Protokoll in die Zwischenablage kopieren, es per E-Mail versenden oder ausdrucken.

Wenn Sie im Protokoll bestimmten Text suchen, klicken Sie auf **Suchen** und geben Sie den gewünschten Text in das Suchfeld ein.

## 10 Fehlerbehebung

### 10.1 Update konnte nicht durchgeführt werden

#### 10.1.1 Allgemeine Informationen

Das Update-Protokoll bietet weitere Informationen zu Update-Fehlern. Anweisungen hierzu entnehmen Sie bitte dem Abschnitt [Öffnen des Update-Protokolls](#) (Seite 77).

In den nachfolgenden Abschnitten werden mögliche Ursachen für Update-Fehler dargelegt. Außerdem wird erläutert, wie sich das Problem durch Änderungen an den Update-Einstellungen beheben lässt.

- [Sophos Endpoint Security and Control bezieht Updates aus der falschen Quelle](#) (Seite 84)
- [Sophos Endpoint Security and Control kann den Proxyserver nicht verwenden](#) (Seite 84)
- [Automatische Updates werden nicht nach Zeitplan durchgeführt](#) (Seite 84)
- [Die Update-Quelle wird nicht mehr aktualisiert](#) (Seite 85)

#### 10.1.2 Sophos Endpoint Security and Control bezieht Updates aus der falschen Quelle

1. Wählen Sie im Menü **Konfigurieren** die Option **Updates**.
2. Prüfen Sie, ob auf der Registerkarte **Primärer Standort** die Adresse und Kontodetails angegeben sind, die Sie von Ihrem Administrator erhalten haben.  
(Die Registerkarte **Primärer Standort** wird unter [Auswahl der Update-Quelle](#) (Seite 75) beschrieben.)

#### 10.1.3 Sophos Endpoint Security and Control kann den Proxyserver nicht verwenden

Wenn Sophos Endpoint Security and Control Updates über das Internet bezieht, muss die Verbindung zum Proxyserver (falls vorhanden) intakt sein.

1. Wählen Sie im Menü **Konfigurieren** die Option **Updates**.
2. Klicken Sie auf der Registerkarte **Primärer Standort** auf **Proxy-Details**.
3. Überprüfen Sie die Adresse des Proxyservers, die Portnummer und die Kontodetails auf ihre Richtigkeit.  
Die Proxy-Angaben werden unter [Updates über einen Proxyserver](#) (Seite 76) beschrieben.

#### 10.1.4 Automatische Updates werden nicht nach Zeitplan durchgeführt

1. Wählen Sie im Menü **Konfigurieren** die Option **Updates**.

2. Klicken Sie auf die Registerkarte **Zeitplan**. (Die Registerkarte **Zeitplan** wird unter [Update-Zeitpläne](#) (Seite 75) beschrieben.)
3. Wenn Ihr Computer vernetzt ist oder wenn die Updates über eine Breitband-Internet-Verbindung durchgeführt werden, wählen Sie **Automatische Updates aktivieren** und geben Sie ein Update-Intervall ein. Wenn Sie Updates über eine Einwahlverbindung durchführen, wählen Sie **Bei Internetverbindung auf Updates überprüfen**.

### 10.1.5 Die Update-Quelle wird nicht mehr aktualisiert

Ihr Unternehmen hat das Verzeichnis (im Netzwerk oder auf einem Webserver) verschoben, von dem Sie normalerweise Updates beziehen. Möglicherweise wird das Verzeichnis nicht verwaltet.

Wenn Sie der Meinung sind, dass dies der Fall ist, wenden Sie sich bitte an Ihren Netzwerkadministrator.

## 10.2 Threat nicht beseitigt

Wenn Sophos Anti-Virus einen Threat nicht beseitigt hat, kann dies auf eine der folgenden Ursachen zurückzuführen sein.

### Automatische Bereinigung wurde deaktiviert

Wenn Sophos Anti-Virus keine Bereinigung durchführt, prüfen Sie, ob die automatische Bereinigung aktiviert ist. Anweisungen zum Aktivieren der automatischen Bereinigung entnehmen Sie bitte dem Abschnitt [Allgemeine Informationen](#) (Seite 39) sowie den übrigen Kapiteln zum Thema *Bereinigung*. Die automatische Entfernung von Adware und PUA ist über On-Access-Scans nicht möglich.

### Bereinigung fehlgeschlagen

Wenn eine Bedrohung von Sophos Anti-Virus nicht bereinigt werden konnte („Bereinigung konnte nicht abgeschlossen werden“), ist es möglich, dass dieser Bedrohungstyp nicht bereinigt werden kann oder dass Sie keine ausreichenden Zugriffsrechte haben.

### Vollständige Systemüberprüfung erforderlich

Sie müssen eventuell eine vollständige Systemüberprüfung starten, um alle Komponenten eines Threats oder Adware/PUA zu erkennen, die bisher versteckt waren, bevor Sophos Anti-Virus sie von Ihrem Computer beseitigen kann.

1. Klicken Sie zum Scannen aller Festplattenlaufwerke, einschließlich Bootsektoren, auf dem Computer auf **Computer scannen**. Nähere Informationen hierzu finden Sie unter [Ausführen eines vollständigen Computer-Scans](#) (Seite 17).
2. Sollte der Threat noch immer nicht vollständig erkannt worden sein, haben Sie möglicherweise keine ausreichenden Zugriffsrechte oder einige Laufwerke oder Ordner, die die Komponenten des Threats enthalten, wurden vom Scan ausgeschlossen. Nähere Informationen hierzu finden Sie unter [Ausschließen von Objekten](#) (Seite 10). Sehen Sie in der Scan-Ausschlussliste nach. Wenn die Liste Objekte enthält, entfernen Sie diese und wiederholen Sie den Scan-Vorgang.

### **Wechseldatenträger ist schreibgeschützt**

Stellen Sie sicher, dass Wechseldatenträger (z.B. Diskette, CD) nicht schreibgeschützt sind.

### **NTFS-Volume ist schreibgeschützt**

Stellen Sie bei Dateien auf einem NTFS-Volume (Windows 2000 oder höher) sicher, dass das Volume nicht schreibgeschützt ist.

### **Meldung von einem Viren-/Spyware-Fragment**

Sophos Anti-Virus bereinigt keine Viren-/Spyware-Fragmente, da es keine exakte Übereinstimmung mit Viren/Spyware gefunden hat. Siehe [Viren-/Spyware-Fragment](#) (Seite 86).

## **10.3 Viren-/Spyware-Fragment**

Verfahren Sie wie folgt, wenn ein Viren-/Spyware-Fragment gemeldet wird:

1. Aktualisieren Sie Ihren Schutz umgehend, damit Sophos Anti-Virus mit den aktuellen Virenkennungsdateien ausgestattet ist.
2. Führen Sie eine vollständige Systemüberprüfung durch.

■ [Sofort-Updates](#) (Seite 75)

■ [Ausführen eines vollständigen Computer-Scans](#) (Seite 17)

Wenn Viren-/Spyware-Fragmente immer noch gemeldet werden, wenden Sie sich bitte an den technischen Support von Sophos.

■ [Technischer Support](#) (Seite 98)

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

### **Variante eines bekannten Virus bzw. bekannter Spyware**

Viele neue Viren oder Spywareobjekte basieren auf vorhandenen Mustern, die zum Teil bereits in bekannten Viren bzw. Spywareobjekten aufgetreten sind. Die Meldung eines Viren-/Spyware-Fragments kann durchaus bedeuten, dass Sophos Anti-Virus einen neuen Virus bzw. ein neues Spywareobjekt erkannt hat, der bzw. das freigesetzt werden könnte.

### **Beschädigter Virus**

Viele Viren enthalten Fehler in ihren Replikationsroutinen und die Zieldateien werden nicht wie geplant infiziert. Ein nicht aktiver Teil eines Virus (möglicherweise ein wesentlicher Teil) kann in einer Hostdatei auftauchen und von Sophos Anti-Virus erkannt werden. Ein beschädigter Virus kann sich nicht verbreiten.

### **Datenbank enthält einen Virus/Spyware**

Bei einer vollständigen Systemüberprüfung kann Sophos Anti-Virus ein Viren-/Spyware-Fragment in einer Datenbankdatei melden. Löschen Sie in diesem Falle nicht die Datenbank. Der technische Support kann Ihnen bei der Problembeseitigung behilflich sein.

Im Abschnitt [Technischer Support](#) (Seite 98) wird erläutert, wie Sie Kontakt zum technischen Support aufnehmen können.

## 10.4 Bedrohung teilweise erkannt

Wenn alle Festplattenlaufwerke auf dem Computer, einschließlich Bootsektoren, gescannt werden sollen, führen Sie eine vollständige Systemüberprüfung durch.

- [Ausführen eines vollständigen Computer-Scans](#) (Seite 17)

Sollte der Threat noch immer nicht vollständig erkannt worden sein, wurden möglicherweise Laufwerke oder Ordner, die die Komponenten des Threats enthalten, vom Scan ausgeschlossen. Sollten sich einige dieser Objekte in der Ausschlussliste befinden, entfernen Sie diese und wiederholen Sie den Scan.

- [Ausschließen von Objekten](#) (Seite 15)

Wenn der Threat nicht vollständig erkannt wurde, verfügen Sie möglicherweise nicht über die erforderlichen Zugriffsrechte.

Sophos Anti-Virus kann Threats mit Komponenten, die auf Netzlaufwerken installiert wurden, eventuell nicht vollständig erkennen oder entfernen.

## 10.5 Adware oder PUA aus Quarantäne verschwunden

Verschwindet eine von Sophos Anti-Virus erkannte Adware oder PUA ohne Zutun des Benutzers aus dem Quarantäne-Manager, wurde die Adware oder PUA möglicherweise von der Management-Konsole oder einem anderen Benutzer zugelassen oder bereinigt. Sehen Sie in der Liste zugelassener Adware und PUA nach, ob sie zugelassen wurde. Lesen Sie dazu [Zulassen von Adware und PUA](#) (Seite 26).

## 10.6 Beeinträchtigte Systemleistung

Eine erhebliche Beeinträchtigung der Computerleistung ist unter Umständen auf eine potenziell unerwünschte Anwendung zurückzuführen, die Ihren Computer überwacht. Wenn On-Access-Scans aktiviert sind, werden vermutlich auch zahlreiche Desktop-Benachrichtigungen zu der PUA angezeigt. Dieses Problem lässt sich wie folgt beheben:

1. Führen Sie einen Scan über die Option **Computer scannen** aus, um alle Komponenten der PUA zu ermitteln. Nähere Informationen hierzu finden Sie unter [Ausführen eines vollständigen Computer-Scans](#) (Seite 17).

**Hinweis:** Sollte die PUA nach dem Scan zum Teil erkannt worden sein, lesen Sie den Abschnitt [Bedrohung teilweise erkannt](#) (Seite 87), Schritt 2.

2. Beseitigen Sie die Adware bzw. PUA von Ihrem Computer. Lesen Sie dazu [Adware und PUA in Quarantäne](#) (Seite 30).

## 10.7 Kein Zugriff auf Datenträger mit infiziertem Bootsektor

**Wichtig:** Wenn Sophos Endpoint Security and Control über eine Management-Konsole verwaltet wird, werden hier vorgenommene Änderungen eventuell nicht berücksichtigt.

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

So geben Sie den Zugriff auf einen Datenträger mit infiziertem Bootsektor frei:

1. Klicken Sie auf **Startseite > Anti-virus und HIPS > Anti-virus und HIPS konfigurieren > Konfigurieren > On-Access-Scans** .
2. Aktivieren Sie auf der Registerkarte **Scanning** das Kontrollkästchen **Zugriff auf Laufwerke mit infiziertem Bootsektor erlauben**.

**Wichtig:** Sobald der Zugriff nicht mehr erforderlich ist, deaktivieren Sie das Kontrollkästchen und nehmen den Datenträger aus dem Laufwerk. So verhindern Sie eine Infizierung des Computers beim nächsten Neustart.

## 10.8 Kein Zugriff auf einige Bereiche von Sophos Endpoint Security and Control

Wenn Sie bestimmte Bereiche von Sophos Endpoint Security and Control nicht benutzen oder konfigurieren können, sind diese Bereiche möglicherweise Mitgliedern bestimmter Sophos Benutzergruppen vorbehalten.

Details zu den Sophos Benutzergruppen entnehmen Sie bitte dem Abschnitt [Allgemeine Informationen](#) (Seite 5).

## 10.9 Wiederherstellung nach Folgeerscheinungen von Viren

Das Vorgehen zum Beheben eines virenbedingten Schadens richtet sich danach, auf welche Weise der Computer infiziert wurde.

### Folgeerscheinungen von Viren

Bei einigen Viren treten keine Folgeerscheinungen auf, bei anderen Viren sind diese Erscheinungen jedoch wiederum so gravierend, dass die Festplatte wiederhergestellt werden muss.

Einige Viren nehmen nach und nach geringfügige Änderungen an Daten vor. Diese Art der Schädigung ist besonders schwer zu entdecken.

### Vorgehensweise

Es empfiehlt sich, die zugehörige Threat-Analyse auf der Sophos Website zu Rate zu ziehen und Dokumente nach der Bereinigung sorgfältig zu überprüfen. (Unter [Bereinigungs-Details](#) (Seite 42) erfahren Sie, wo Sie auf der Sophos Website Näheres zu den Folgeerscheinungen der entsprechenden Viren finden können.)

Sicherungskopien sind unerlässlich. Falls Sie vor einer Infizierung noch keine Sicherungskopien angelegt hatten, sollten Sie nach der Bereinigung und Desinfizierung damit anfangen, damit Sie in Zukunft besser vorbereitet sind.

Manchmal lassen sich jedoch noch Daten auf von Viren beschädigten Festplatten retten. Sophos verfügt über Tools zur Behebung bestimmter Virenschäden.

Der technische Support kann Ihnen bei der Problembeseitigung behilflich sein.

Im Abschnitt [Technischer Support](#) (Seite 98) wird erläutert, wie Sie Kontakt zum technischen Support aufnehmen können.

## 10.10 Wiederherstellung nach Folgeerscheinungen von Adware und PUA

Unter Umständen treten bei der Entfernung von PUA und Adware Folgeerscheinungen auf, die bei der Bereinigung nicht beseitigt werden.

### Änderungen am Betriebssystem

Bisweilen werden durch Adware und PUA Änderungen am Betriebssystem (z.B. an den Interneteinstellungen) vorgenommen. Mit Sophos Anti-Virus können Sie Einstellungen wieder auf den Stand vor der Installation der Adware/PUA zurücksetzen. Wenn eine Adware oder PUA beispielsweise die Startseite des Browsers geändert hat, kennt Sophos Anti-Virus die vorherige Startseite nicht.

### Nicht bereinigte Dienstprogramme

Adware/PUA können Dienstprogramme (z.B. *.dll*- oder *.ocx*-Dateien) auf dem Computer installieren. Wenn ein Dienstprogramm harmlos ist, d.h. es hat keine Eigenschaften einer Adware/PUA, z.B. eine Sprachen-Library, und es ist kein wesentlicher Teil der Adware/PUA, wird es möglicherweise von Sophos Anti-Virus nicht als Teil der Adware/PUA erkannt. In diesem Falle wird die Datei nicht von Ihrem Computer entfernt, selbst wenn die Adware oder PUA entfernt wurde, die sie installiert hat.

### Die Adware/PUA ist Teil eines erforderlichen Programms

Adware/PUA können Teil eines absichtlich installierten Programms und für dessen Ausführung erforderlich sein. Wenn Sie die Adware/PUA entfernen, läuft das Programm möglicherweise auf Ihrem Computer nicht mehr.

### Vorgehensweise

Es empfiehlt sich, die zugehörige Threat-Analyse auf der Sophos Website zu Rate zu ziehen. (Unter [Bereinigungs-Details](#) (Seite 42) erfahren Sie, wo Sie auf der Sophos Website Näheres zu den Folgeerscheinungen der entsprechenden Adware/PUA finden können.)

Um Ihr System und dessen Einstellungen auf den vorherigen Stand zurücksetzen zu können, sollten Sie regelmäßige Sicherungskopien von Ihrem System erstellen. Erstellen Sie Sicherungskopien der ausführbaren Dateien der Programme, die Sie verwenden möchten.

Auf Anfrage erhalten Sie beim technischen Support von Sophos weitere Informationen oder Hinweise zur Wiederherstellung nach Folgeerscheinungen durch Adware/PUA.

Im Abschnitt *Technischer Support* (Seite 98) wird erläutert, wie Sie Kontakt zum technischen Support aufnehmen können.

## 10.11 Kennwortfehler gemeldet

Wenn bei der Erstellung eines Zeitplans für einen individuellen Scan eine Kennwort-Fehlermeldung angezeigt wird, stellen Sie Folgendes sicher:

- Das Kennwort für das Benutzerkonto ist korrekt.
- Das Kennwort ist nicht leer.

Überprüfen Sie hierzu ggf. die Benutzerkontoeigenschaften in der **Systemsteuerung** im Bereich **Benutzerkonten**.

## 10.12 Fehlermeldung „Service Failure“ (Fehlerhafter Dienst)

### Symptome

Im Benachrichtigungsbereich wird eine der folgenden Fehlermeldungen angezeigt:

- `Anti-virus and HIPS: service failure`
- `Firewall: service failure`

### Mögliche Ursachen

Ein Dienst von Sophos Endpoint Security and Control ist fehlerhaft und muss neu gestartet werden.

### Problemlösung

1. Öffnen Sie die **Windows-Dienste** (Pfad siehe unten).
2. Führen Sie einen der folgenden Schritte aus:
  - Wenn eine `Anti-Virus und HIPS: service failure`-Meldung angezeigt wird, rechtsklicken Sie auf **Sophos Anti-Virus** und klicken Sie anschließend auf **Neu starten**.
  - Bei Anzeige der Fehlermeldung `Firewall: service failure` rechtsklicken Sie auf **Sophos Client Firewall** und klicken Sie anschließend auf **Neu starten**.

### Hinweise

- Klicken Sie zum Öffnen der Dienste auf **Start, Systemsteuerung**, doppelklicken Sie auf **Verwaltung** und doppelklicken Sie anschließend auf **Dienste**.

## 10.13 Firewall-Protokolldatenbank ist beschädigt

### Symptom

Beim Verwenden der Protokollanzeige der Firewall wird die folgende Fehlermeldung angezeigt: „Die aktuelle Sophos Client Firewall-Protokolldatenbank ist beschädigt.“

### Ursache

Die Firewall-Ereignisprotokolldatenbank wurde beschädigt und muss neu erstellt werden.

### Problemlösung

Nur Mitglieder der Gruppe „Windows Administratoren“ auf diesem Computer können das Problem beheben.

1. Öffnen Sie die **Windows-Dienste** (Pfad siehe unten).
2. Rechtsklicken Sie auf **Sophos Client Firewall** Manager und klicken Sie auf **Anhalten**.
3. Navigieren Sie in Windows Explorer zu C:\Dokumente und Einstellungen\Alle Benutzer\Anwendungsdaten\Sophos\Sophos Client Firewall\logs.

Damit dieser versteckter Ordner angezeigt wird, müssen Sie unter Umständen versteckte Dateien und Ordner in Windows Explorer anzeigen.

4. Löschen Sie op\_data.mdb.
5. Rechtsklicken Sie in den „Diensten“ auf **Sophos Client Firewall** Manager und klicken Sie auf **Neu starten**.

### Hinweise

- Klicken Sie zum Öffnen der Dienste auf **Start, Systemsteuerung**, doppelklicken Sie auf **Verwaltung** und doppelklicken Sie anschließend auf **Dienste**.

## 11 Glossar

<b>Adware und PUA</b>	Unter „Adware“ sind Programme zu verstehen, z.B. Werbung auf dem Bildschirm anzeigen (meist in Popup-Fenstern), wodurch die Arbeitsproduktivität und die Systemleistung beeinträchtigt werden. Unter dem Begriff „potenziell unerwünschte Anwendung“ (kurz <i>PUA</i> ) werden Programme zusammengefasst, die zwar nicht schädlich sind, doch in der Arbeits- bzw. Geschäftsumgebung nicht erwünscht sind.
<b>Anwendungsregel</b>	Regel, die sich auf im Netzwerk übertragene Datenpakete beschränkt, die an eine oder von einer bestimmten Anwendung gesendet werden.
<b>Arbeitsmodus</b>	Je nach Arbeitsmodus ergreift die Firewall Maßnahmen durch Zutun des Benutzers (interaktiver Modus) oder automatisch (nicht interaktiver Modus).
<b>Ausführlicher Scan</b>	Scan einer Datei in allen Einzelheiten.
<b>Authorization Manager</b>	Modul zur Zulassung von Adware und PUA, verdächtigen Dateien, Anwendungen mit verdächtigen Verhaltensmustern und Pufferüberläufen.
<b>automatische Bereinigung</b>	Bereinigung, die nicht durch den Benutzer eingeleitet werden muss.
<b>Benutzerregel</b>	Vom Benutzer erstellte Regeln zur Bestimmung, unter welchen Umständen eine Anwendung ausgeführt werden darf.
<b>Bereinigung</b>	Durch eine Bereinigung werden Threats auf dem Computer entfernt: Viren werden aus Dateien oder dem Bootsektor entfernt, verdächtige Dateien werden verschoben oder gelöscht und Adware/PUA werden gelöscht. Vor der Bereinigung entstandene Schäden werden jedoch nicht behoben. Bedrohungen, die beim Überprüfen von Websites erkannt wurden, werden nicht bereinigt, da diese Bedrohungen nicht auf Ihren Computer heruntergeladen werden. Aus diesem Grund sind keine Maßnahmen erforderlich.
<b>Beschreibungsleiste</b>	Eine Leiste im Protokoll-Viewer oberhalb der Datenansicht, die den Namen des ausgewählten Objekts enthält.
<b>Content Control List (CCL)</b>	Eine Kombination von Bedingungen zur Bestimmung des Inhalts von Dateien (z.B. Kreditkarten- oder Kontodaten oder andere personenbezogenen Daten). Es wird zwischen zwei Arten von „Content Control Lists“ unterschieden: „SophosLabs Content Control Lists“ und „benutzerdefinierte Content Control Lists“.
<b>Controlled Application</b>	Eine Anwendung, deren Ausführung durch die Sicherheitsrichtlinie des Unternehmens unterbunden wird.

---

<b>Data Control</b>	Kontrollfunktion zur Verhinderung, dass ungewollt Daten von Computern übertragen werden. Der Mechanismus greift, wenn ein Benutzer eine Datei versenden oder anderweitig übertragen möchte, die die Kriterien der „Data Control“-Richtlinie und der entsprechenden Regeln erfüllt. Wird beispielsweise eine Tabelle mit Kundendaten auf einen Wechseldatenträger kopiert oder ein vertrauliches Dokument in einem webbasierten E-Mail-Konto hochgeladen, wird die Übertragung bei entsprechender Konfiguration verhindert.
<b>Datenansicht</b>	In dieser Ansicht werden Daten in Bezug auf das in der Strukturansicht ausgewählte Objekt angezeigt.
<b>Device Control</b>	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.
<b>Echter Dateityp</b>	Dateityp, der durch Strukturanalyse und nicht anhand der Dateierweiterung ermittelt wird. Diese Methode liefert bessere Ergebnisse.
<b>Einstellungen zum Löschen des Protokolls</b>	Zeiteinstellungen zum Löschen von Aufzeichnungen im Protokoll.
<b>Erkennung verdächtigen Verhaltens</b>	Dynamische Analyse des Verhaltens aller auf einem System ausgeführten Programme. Bei Erkennung von Schadenspotenzial wird das jeweilige Programm an der Ausführung gehindert.
<b>Firewall-Ereignis</b>	Ein Ereignis findet statt, wenn eine unbekannte Anwendung oder das Betriebssystem auf dem Computer versucht, über eine Netzwerkverbindung mit einem anderen Computer zu kommunizieren.
<b>Firewall-Richtlinie</b>	Von der Management-Konsole für die Firewall festgelegte Einstellungen, die bei der Überwachung der Internet- und Netzwerkverbindungen zu verwenden sind.
<b>Geplanter Scan</b>	Vollständiger oder teilweiser Scan eines Computers zu festen Zeiten.
<b>Gesperrt</b>	Dieser Zustand trifft auf Controlled Applications zu, deren Zugriff von On-Access-Scans gesperrt wurde.
<b>Globale Regel hoher Priorität</b>	Regeln dieser Kategorie sind von höherer Priorität als globale oder Anwendungsregeln und werden daher zuerst zugewiesen.
<b>Globale Regeln</b>	Regeln, die für alle Netzwerkverbindungen und Anwendungen gelten, denen noch keine Regeln zugewiesen wurden. Die auf der LAN-Seite festgelegten Regeln haben Vorrang.

	Anwendungsregeln haben ebenfalls Vorrang (sofern nicht anders vom Benutzer angegeben).
<b>Host Intrusion Prevention System (HIPS)</b>	Unter diesem Begriff ist die Analyse von Verhaltensmustern vor oder während der Ausführung von Programmcode zu verstehen.
<b>ICMP</b>	Kurz für „Internet Control Message Protocol.“ Ein Internetprotokoll der Vermittlungsschicht, das Fehlerbehebungshinweise und andere Informationen zur Verarbeitung von IP-Paketen bietet.
<b>ICMP-Einstellungen</b>	Einstellungen zum Austausch von Informations- und Fehlermeldungen im Netzwerk.
<b>Inhaltsregel</b>	Eine Inhaltsregel umfasst mindestens eine Content Control List. Hierin wird die Maßnahme festgelegt, die bei der Übertragung von Daten, die alle Bedingungen der Content Control Lists der Regel erfüllen, an den festgelegten Zielort ergriffen werden soll.
<b>Instant Messaging</b>	Controlled Application-Kategorie: Instant Messaging Client-Anwendungen (z.B. MSN).
<b>Interaktiver Modus</b>	In diesem Modus zeigt die Firewall einen oder mehrere sog. Lerndialoge in Bezug auf einen Netzwerkzugriff an, für den es noch keine Regel gibt, und speichert die auf diese Weise gesammelten Informationen.
<b>Internet-Telefonie</b>	Controlled Application-Kategorie: Anwendung zur Internet-Telefonie (z.B. Skype)
<b>Laufzeitverhaltensanalyse</b>	Dynamische Analyse bei der Erkennung von verdächtigen Verhaltensmustern und von Pufferüberläufen.
<b>Lerndialog</b>	Im Lerndialog kann der Benutzer angeben, ob Netzwerkaktivitäten zugelassen oder gesperrt werden sollen, wenn eine unbekannte Anwendung Netzwerkzugriff anfordert.
<b>Log Viewer</b>	Ansicht mit Informationen aus der Ereignisdatenbank (z.B. zugelassene und abgelehnte Verbindungen), dem Systemprotokoll und über ausgegebene Alerts.
<b>Manuelle Bereinigung</b>	Eine durch besondere Desinfektionsprogramme oder durch das Löschen von Dateien erzielte Bereinigung.
<b>NetBIOS</b>	Kurz für „Network Basic Input/Output System.“ Schnittstelle zwischen dem Betriebssystem, dem I/O-Bus und dem Netzwerk. Die meisten Windows-LANs basieren auf NetBIOS.

---

<b>Netzwerk-Protokoll</b>	Regeln oder Standards zum Verbinden von Computern im Netzwerk, um einen möglichst reibungslosen Datenaustausch zu gewährleisten.
<b>Nicht interaktiver Modus</b>	In diesem Modus sperrt oder erlaubt die Firewall alle Datenbewegungen, für die keine Regeln vorhanden sind.
<b>Normaler Scan</b>	Scans von Dateien in den Bereichen, die höchstwahrscheinlich infiziert werden können.
<b>On-Access-Scans</b>	Der zentrale Schutz vor Bedrohungen. Beim Versuch, auf eine Datei (d.h. Kopieren, Speichern, Verschieben oder Öffnen der Datei) zuzugreifen, scannt Sophos Anti-Virus die Datei. Der Zugriff wird nur erlaubt, wenn die Datei threatfrei ist bzw. zugelassen wurde.
<b>On-Demand-Scan</b>	Vom Benutzer eingeleiteter Scan. Dabei können einzelne Dateien oder der gesamte Computer gescannt werden.
<b>Primäre Konfiguration</b>	Die Firewall-Konfiguration des Unternehmensnetzwerks, auf das Benutzer am häufigsten zugreifen.
<b>Prozesseinstellungen</b>	In diesen Einstellungen wird festgelegt, ob geänderten oder versteckten Prozessen der Netzwerkzugriff gestattet werden soll.
<b>Prüfsumme</b>	Jede Version einer Anwendung umfasst eine andere Prüfsumme. Mit Hilfe der Prüfsumme kann die Firewall entscheiden, ob eine Anwendung zugelassen oder gesperrt werden soll.
<b>Pufferüberlauf-Erkennung</b>	Erkennung von Pufferüberlauf-Angriffen.
<b>Quarantäne-Manager</b>	Dieses Modul ermöglicht die Verwaltung von isolierten (d.h. in Quarantäne verschobenen) Objekten.
<b>Raw-Socket</b>	Raw-Sockets erlauben Prozessen die Steuerung der Datenbewegungen im Netzwerk und können für illegale Zwecke missbraucht werden.
<b>Rechtsklick-Scan</b>	Ein über das Kontextmenü eingeleiteter Scan von Dateien in Windows-Explorer oder auf dem Desktop.
<b>Rootkit</b>	Trojaner oder Technologie zum Verstecken von Schadobjekten (Prozess, Datei, Registrierungsschlüssel oder Netzwerk-Port) vor Nutzern und Administratoren.
<b>Scan-Fehler</b>	Fehler beim Scannen einer Datei. Beispiel: Der Zugriff wurde verweigert.
<b>Sekundäre Konfiguration</b>	Eingesetzte Firewall-Konfiguration, wenn Benutzer nicht auf das Hauptunternehmensnetzwerk, sondern ein anderes

	Netzwerk (z.B. Wireless-Netzwerk in einem Hotel oder am Flughafen oder ein anderes Unternehmensnetzwerk) zugreifen.
<b>Speichergerät</b>	Wechselmedien (z.B. USB-Flashdrive, PC-Kartenleser, externe Festplatte), CD-/DVD-Laufwerk oder Diskettenlaufwerk und sichere Wechselmedien (z.B. USB-Flash-Laufwerke mit Hardware-Verschlüsselung, wie etwa SanDisk Cruzer Enterprise, Kingston Data Traveller, IronKey Enterprise und IronKey Basic).
<b>Spyware</b>	Ein Programm, das sich hinterlistig und unbemerkt auf dem Computer eines ahnungslosen Benutzers installiert und auf diesem Computer gespeicherte Informationen ohne Erlaubnis oder Benachrichtigung des Benutzers an Dritte weiterleitet.
<b>Stateful Packet Inspection (SPI)</b>	Firewall-Funktion, die die aktiven TCP- und UDP-Netzwerkverbindungen auflistet. Nur Pakete, die einem bekannten Verbindungszustand entsprechen werden von der Firewall zugelassen; andere Pakete werden abgewiesen.
<b>Strukturansicht</b>	In dieser Ansicht lässt sich bestimmen, welche Daten in der Datenansicht des Protokoll-Viewers angezeigt werden sollen.
<b>Systemregel</b>	Systemregeln gelten für alle Anwendungen im Netzwerk und dienen der Zulassung oder Ablehnung untergeordneter Netzwerkaktivitäten.
<b>Threat-Ereignis</b>	Erkennung oder Beseitigung eines Threats.
<b>Unbekannter Datenverkehr</b>	Netzwerkzugriff durch eine Anwendung oder einen Dienst, für den keine Regel vorhanden ist.
<b>Unbekannter Virus</b>	Hierbei handelt es sich um einen Virus, für den noch keine Virenkennung vorhanden ist.
<b>Verdächtige Datei</b>	Datei, die zwar für Viren typische Merkmale aufweist, jedoch nicht schädlich sein muss, da diese Merkmale auch in harmlosen Programmen auftreten können.
<b>Versteckter Prozess</b>	Eine Anwendung kann im Hintergrund einen Prozess starten, der für sie auf das Netzwerk zugreift. Gelegentlich machen sich Schadprogramme diese Technik zunutze, um eine Firewall zu umgehen: Sie starten eine vertrauenswürdige Anwendung, die für sie auf das Netzwerk zugreift, auf das sie selbst keinen Zugriff haben.
<b>Vertrauenswürdige Anwendung</b>	Anwendung mit uneingeschränktem Vollzugriff auf das Netzwerk.
<b>Virenkennung (IDE)</b>	Eine Kennungsdatei, anhand derer Sophos Anti-Virus Viren, Trojaner, Würmer und Spyware erkennt und desinfiziert.

**Übereinstimmung**

Entsprechung zu den in der Content Control List festgelegten Inhalten.

## 12 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](mailto:support@sophos.de) und geben Sie die Versionsnummer(n), Betriebssystem(e) und Patch Level Ihrer Sophos Software sowie ggf. den genauen Wortlaut von Fehlermeldungen an.

## 13 Rechtlicher Hinweis

Copyright © 2010 Sophos Group. Alle Rechte vorbehalten. Kein Teil dieser Publikation darf in jeglicher Form, weder elektronisch oder mechanisch, reproduziert, elektronisch gespeichert oder übertragen werden, noch fotokopiert oder aufgenommen werden, es sei denn, Sie haben entweder eine gültige Lizenz, gemäß der die Dokumentation in Übereinstimmung mit den Lizenzvereinbarungen reproduziert werden darf oder Sie haben eine schriftliche Genehmigung des Copyright-Inhabers.

Sophos und Sophos Anti-Virus sind eingetragene Warenzeichen der Sophos Plc und Sophos Group. Alle anderen erwähnten Produkt- und Unternehmensnamen sind Warenzeichen oder eingetragene Warenzeichen der jeweiligen Inhaber.

### 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](mailto: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>

### ConvertUTF

Copyright 2001–2004 Unicode, Inc.

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

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

## Index

### A

- Adware 87, 89
  - automatische Bereinigung 41
  - Scannen auf 23
  - Zulassen 26
- Adware in Quarantäne 30
- Adware in Quarantäne, Umgang mit 30
- Aktivieren von On-Access-Scans 12
- Aktivieren von Prüfsummenlerndialogen 57
- Alle Dateien, Scannen 23
- Anhalten von Scans 44
- Anti-Virus
  - Konfigurieren der E-Mail-Benachrichtigung 35
  - Konfigurieren des Ereignisprotokolls 37
  - Konfigurieren von
    - Desktop-Benachrichtigungen 34
    - Konfigurieren von SNMP-Benachrichtigungen 37
- Anwendungen
  - Authentifizierung mit Prüfsummen 67
  - Sperren 53
  - Zulassen 52
- Anzeigen
  - Scan-Protokoll 38
  - Scan-Protokoll (individueller Scan) 21
- Arbeitsmodus, Wechsel in den interaktiven Modus 55
- Archivdateien, Scannen 22
- Aufnehmen von Benutzern in eine Sophos Gruppe 6
- Ausführen vollständiger Computer-Scans 17
- Ausführen von individuellen Scans 20
- Ausführen von Rechtsklick-Scans 18
- Ausschließen von Objekten von On-Access-Scans 10
- Ausschließen von Objekten von On-Demand-Scans 15
- Authentifizieren von Anwendungen, Prüfsummen 67
- automatische Bereinigung
  - PUA 41
  - Spyware 39
  - verdächtige Dateien 41
  - Viren 39

### Automatische Bereinigung

- Adware 41

### B

- Bedrohung teilweise erkannt 87
- Benutzergruppen 5, 88
- Benutzerrechte 5, 88
- Benutzerrechte für den Quarantäne-Manager, Konfigurieren 7
- Bereinigung 39
  - Fehlersuche 85
- Bereinigungs-Details 42

### C

- Controlled Applications
  - Scannen auf 13
  - Umgang mit 34
  - Zulassen 34

### D

- Data Control, vorübergehend deaktivieren 46
- Datei- und Druckerfreigabe 51, 52
- Datei- und Druckerfreigabe, Sperren 63
- Datei, freigeben 51, 52
- Dateifreigabe, sperren 63
- Datenverkehr im LAN, Zulassen 51
- Deaktivieren der Firewall 49
- Deaktivieren des Scannens auf Controlled Applications 13
- Deaktivieren von On-Access-Scans 12
- Deaktivieren von Scans 44
- Deinstallieren von Sophos Sicherheitssoftware 82
- Desinfektion/Beseitigung 85
- Device Control 44
  - Controlled Devices 44
  - Sperren von Netzwerkbrücken 44
- Drucker, freigeben 51, 52
- Druckerfreigabe, Sperren 63

### E

- E-Mail-Programm, zulassen 49
- Einrichten globaler Regeln 60, 61, 65
- Erkennen verdächtigen Verhaltens 12
- Erkennen von Pufferüberläufen 12
- Erkennung eines Fragments 87
- Erstellen von individuellen Scans 18

Exportieren von Datensätzen aus dem Firewall Log Viewer 73, 74

Exportieren von Firewall-Konfigurationsdateien 58

## F

Festlegen von Dateierweiterungen für On-Access-Scans 9

Filtern von ICMP-Meldungen 53

Filtern von Protokolldatensätzen 73

Firewall

Deaktivieren 49

Firewall Log Viewer

Exportieren von Einträgen 73, 74

Firewall-Konfigurationsdateien

Exportieren 58

Importieren 58

Firewall-Protokolle

Konfigurieren 71

Folgeerscheinungen 89

Fragment 85

Fragment gemeldet, Fehlerbehebung 86

FTP-Downloads, zulassen 50

## G

Globale Regeln

Einstellung 60, 61, 65

## H

Hinzufügen einer Regel 61, 62

## I

ICMP-Meldungen

Erläuterung 53

Filtern 53

Importieren von Firewall-Konfigurationsdateien 58

In-the-Cloud-Verfahren 24

individuelle Scans

Ausführen 20

Erstellen 18

Konfigurieren 19

Löschen 21

Umbenennen 21

Zeitpläne 20

Infizierter Bootsektor 88

Informationen zur Bereinigung 42

Interaktiver Modus

Anwendungsmeldungen 56

Meldungen versteckter Prozesse 56

Protokoll-Meldungen 56

Prüfsummenlerndialoge 57

Raw-Socket-Meldungen 56

interaktiver Modus, Aktivieren 55

interaktiver Modus, allgemeine Informationen 55

## K

Kennwortfehler 90

Konfigurieren 18

zentrale Reports 68

Benutzerrechte für den Quarantäne-Manager 7

Desktop-Benachrichtigungen 34

E-Mail-Benachrichtigungen 35

Ereignis-Protokollierung 37

Firewall-Protokolle 71

individuelle Scans 19

On-Access-Scans 8

Scan-Protokoll 38

SNMP-Benachrichtigungen 37

## L

langsamer Computer, Fehlerbehebung 87

Laufzeitverhaltensanalyse 12

Log Viewer

Informationen 71

Löschen von individuellen Scans 21

## M

Manipulationsschutz

Aktivieren 79

Ausschalten 79

Benutzerauthentifizierung 81

Deaktivieren 79

Deinstallieren von Sophos Endpoint Security and Control 82

Deinstallieren von Sophos Sicherheitssoftware 82

Einschalten 79

Erneute Aktivierung 80

Kennwort-Eingabe 81

Kennwortänderung 81

Konfigurieren der Software 81

Manipulationsschutz (*Fortsetzung*)

- Protokoll 82
- Überblick 78

**N**

- nicht interaktiver Modus, Wechsel in den 55

**O**

- On-Access-Scans
  - Aktivieren 12
  - Ausschließen von Objekten von 10
  - Deaktivieren 12
  - Festlegen von Dateierweiterungen 9
  - Konfigurieren 8
- On-Access-Scans und On-Demand-Scans, Unterschiede 8
- On-Demand-Scans
  - Ausschließen von Objekten von 15
  - Festlegen von Dateierweiterungen 14
- On-Demand-Scans, Optionen 14
- Optionen für On-Demand-Scans 14

**P**

- Planen von individuellen Scans 20
- Primärserver 75
- Protokolldatensätze
  - Filtern 73
- Protokollieren von Updates 77
- Proxyserver 76
- Prüfsummen gescannter Dateien, Zurücksetzen 9
- Prüfsummen, Authentifizieren von Anwendungen 67
- Prüfsummenlerndialoge
  - Aktivieren 57
  - Interaktiver Modus 57
- PUA 87, 89
  - automatische Bereinigung 41
  - Scannen auf 23
  - Zulassen 26
- PUA in Quarantäne 30
- PUA in Quarantäne, Umgang mit 30
- Pufferüberläufe
  - Erkennen 12
  - Zulassen 26, 33

**Q**

- Quarantäne-Manager 28

**R**

- Raw-Sockets, Zulassen 66
- Rechtsklick-Scans 18
- Rechtsklick-Scans, Ausführen 18
- Rechtsklick-Scans, Konfigurieren 18
- Regel
  - Hinzufügen 61, 62
- Regelpriorität 59
- Rootkits, Scannen 20

**S**

- Scan-Protokoll
  - Anzeigen 38
  - Konfigurieren 38
- Scan-Protokoll (individueller Scan)
  - Anzeigen 21
- Scannen auf Adware und PUA 23
- Scannen auf Controlled Applications 13
- Scannen auf Controlled Applications, Deaktivieren 13
- Scannen auf Macintosh-Viren 22
- Scannen auf Rootkits 20
- Scannen auf verdächtige Dateien 23
- Scannen eines einzelnen Objekts 18
- Scans eines einzelnen Objekts 18
- schädliche Websites
  - Schutz 25
- Sekundärserver 76
- Sicherheitsinformationen 42
- Sofort-Updates 75
- Sophos Endpoint Security and Control 3
- Sophos Gruppen 5
  - Hinzufügen von Benutzern 6
- Sophos Live-Schutz
  - Aktivieren 24
  - Ausschalten 24
  - Deaktivieren 24
  - Einschalten 24
  - In-the-Cloud-Verfahren 24
  - Protokoll 25
  - Überblick 24
- Sperren
  - Anwendungen 53

**Sperren (Fortsetzung)**

- Datei- und Druckerfreigabe 63
- schädliche Websites 25
- zugelassene Adware 26
- zugelassene PUA 26

**Spyware**

- automatische Bereinigung 39

**Spyware in Quarantäne 29****Spyware in Quarantäne, Umgang mit 29****Startseite 4****Support 98****Symbole**

- Scan-Objekte 19

**T****Taskleisten-Symbol 84****Technischer Support 98****Threat-Analysen 42****U****Übertragungsrate für Updates, Verringern 77****Umbenennen von individuellen Scans 21****Umgang mit Controlled Applications 34****Updates 75, 77, 84****Updates über eine Einwahlverbindung 75****V****verdächtige Dateien**

- automatische Bereinigung 41
- Scannen auf 23
- Zulassen 26

**verdächtige Dateien in Quarantäne 31****verdächtige Dateien in Quarantäne, Umgang mit 31****verdächtige Objekte, Zulassen 27****verdächtiges Verhalten**

- Erkennen 12
- Zulassen 26, 33

**verdächtiges Verhalten in Quarantäne 33****verdächtiges Verhalten in Quarantäne, Umgang mit 33****Verringern der Übertragungsrate für Updates 77****Versteckte Prozesse, Zulassen 65****Viren**

- automatische Bereinigung 39
- Wiederherstellung nach Folgeerscheinungen 88

**Viren in Quarantäne 29****Viren in Quarantäne, Umgang mit 29****Vollständige Computer-Scans, Ausführen 17****Vorbereitung**

- Erste Schritte 48

**W****Webbrowser, zulassen 50****Website**

- Zulassen 27

**Wiederherstellung nach Folgeerscheinungen 89****Z****Zeitplan für Scans 90****Zeitplan für Updates 75****zentrale Reports, Konfigurieren 68****zugelassene Adware, Sperren 26****zugelassene PUA, Sperren 26****Zugriff auf Datenträger 88****Zugriffsrechte 5, 88****Zulassen**

- Adware 26
- Anwendungen 52
- Controlled Applications 34
- Datei- und Druckerfreigabe 51, 52
- Datenverkehr im LAN 51
- E-Mail 49
- FTP-Downloads 50
- PUA 26
- Pufferüberläufe 26, 33
- Raw-Sockets 66
- verdächtige Dateien 26
- verdächtiges Verhalten 26, 33
- Versteckte Prozesse 65
- Webbrowser 50
- Website 27

**Zulassen bestimmter Objekte 27****Zurücksetzen der Prüfsummen gescannter Dateien 9**