

# SOPHOS

## Sophos Endpoint Security and Control Anleitung zu Device Control

Sophos Enterprise Console

Dokumentdatum: Juni 2008



# Inhalt

- 1 Voraussetzungen.....3
- 2 Einrichten von Device Control.....4
- 3 Umgang mit Alarmen.....11
- 4 Technischer Support.....13
- 5 Copyright.....14

# 1 Voraussetzungen

## 1.1 Was bedeutet Device Control?

Mit Device Control können Sie verhindern, dass unbekannte Speichergeräte und Drahtlosverbindungen ohne Ihre Genehmigung an Computer im Netzwerk angeschlossen werden.

Device Control ist standardmäßig in Sophos Endpoint Security and Control enthalten.

## 1.2 Einleitung

Diese Anleitung wurde für Systemadministratoren geschrieben, die Device Control (Gerätesteuerung) in ihre Enterprise Console-Richtlinien einbeziehen möchten.

## 1.3 Systemanforderungen an Arbeitsplatzrechner

Sophos Anti-Virus for Windows, version 7.5. Dieses Programm ist eine Komponente von Sophos Endpoint Security and Control.

## 1.4 Abonnieren des richtigen Pakets

Wenn Sie Device Control in Ihre Enterprise Console-Richtlinien integrieren möchten, müssen Sie in EM Library das aktuellste **Windows Endpoint Security and Control 8.0**-Paket abonniert haben.

So überprüfen Sie, ob das richtige Paket abonniert ist:

1. Klicken Sie in Enterprise Console auf **Extras > Verwaltung der Libraries**.
2. Doppelklicken Sie im Konsolenstamm von EM Library auf **EM Library**.
3. Doppelklicken Sie auf **Packages** und klicken Sie dann auf **Subscribed**.
4. Sehen Sie sich im rechten Fensterbereich die Liste der abonnierten Pakete an.

Wenn dort nicht das aktuellste **Windows Endpoint Security and Control 8.0**-Paket aufgeführt ist, müssen Sie es abonnieren.

Unter "Select which software to download" im Abschnitt *How do I change downloading settings?* der EM Library-Hilfe erfahren Sie, wie Sie in EM Library ein Paket abonnieren.

## 2 Einrichten von Device Control

Es empfiehlt sich, die Richtlinien für Device Control wie folgt einzurichten.

**Wichtig:** Sophos Device Control sollte nicht gemeinsam mit ähnlicher Software anderer Anbieter eingesetzt werden.

### 1. Schritt: Auswahl der zu sperrenden Gerätetypen

Normalerweise sind alle Speichergeräte und Drahtlosverbindungen zugelassen. Wählen Sie die zu sperrenden Gerätetypen aus.

- [Unterstützte Gerätetypen](#) auf Seite 4
- [Auswählen von Speichergeräten](#) auf Seite 5
- [Auswählen von Drahtlosverbindungen](#) auf Seite 6

### 2. Schritt: Erkennen von Geräten, ohne sie zu sperren

Überprüfen Sie die Auswirkungen der Richtlinie noch vor dem Einsatz, indem Sie sie dazu konfigurieren, Geräte zu erkennen, ohne sie zu sperren. Weitere Informationen finden Sie unter [Erkennen von Geräten, ohne sie zu sperren](#) auf Seite 6.

**Wichtig:** Dieser Schritt wird *nicht* empfohlen, wenn Application Control-Richtlinien bereits im Einsatz sind, da diese sonst auf den Erkennungsmodus gesetzt werden.

### 3. Schritt: Einrichtung von Alarmen und Benachrichtigungen

Geben Sie Benachrichtigungen an, die bei Erkennung (und späterer Sperrung) nicht zugelassener Geräte gesendet werden sollen. Weitere Informationen finden Sie unter [Einrichten von Alarmen und Benachrichtigungen](#) auf Seite 7.

### 4. Schritt: Erkennen und Sperren von Geräten

Übertragen Sie die Richtlinie auf das gesamte Netzwerk. Unerwünschte und unbekannte Geräte werden von nun an gesperrt. Bei versuchtem Zugriff auf ein gesperrtes Gerät wird eine Benachrichtigung auf dem entsprechenden Computer ausgegeben.

- [Erkennen und Sperren von Geräten](#) auf Seite 7
- [Aktivieren von Desktop-Benachrichtigungen](#) auf Seite 8

## 2.1 Unterstützte Gerätetypen

Mit Device Control können Sie Folgendes sperren: *Speichergeräte* und *Drahtlosverbindungen*.

### Speichergeräte

Folgende Speichergeräte werden erkannt:

- Wechsellaufwerke (z.B. USB-Flashdrives, PC-Kartenlesegeräte und externe Festplatten)
- CD-ROM-/DVD-Laufwerke
- Diskettenlaufwerke

### Drahtlosverbindungen

Die folgenden Drahtlosverbindungen werden erkannt:

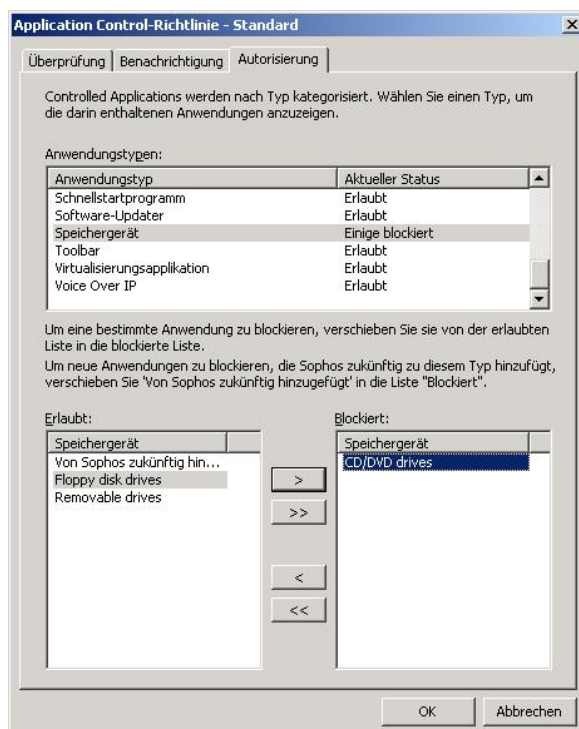
- Wi-Fi-Schnittstellen (802.11-Standard)
- Bluetooth-Schnittstellen
- IrDA-Infrarotschnittstellen

Mit Device Control können sowohl interne als auch externe Geräte und Schnittstellen gesperrt werden. Zum Beispiel sperrt eine Bluetooth-Richtlinie sowohl

- die in einem Computer integrierte Bluetooth-Schnittstelle als auch
- Bluetooth-USB-Stecker, die an diese Schnittstelle angeschlossen werden.

## 2.2 Auswählen von Speichergeräten

1. Doppelklicken Sie im Fenster **Richtlinien** auf **Application Control**. Doppelklicken Sie dann auf die zu ändernde Richtlinie.
2. Klicken Sie im Dialogfeld der **Application Control-Richtlinie** auf die Registerkarte **Autorisierung**.
3. Wählen Sie **Speichergeräte**.
4. Wählen Sie aus der Liste **Erlaubt** den zu sperrenden Speichergerättyp aus und verschieben Sie ihn in die Liste **Blockiert**.

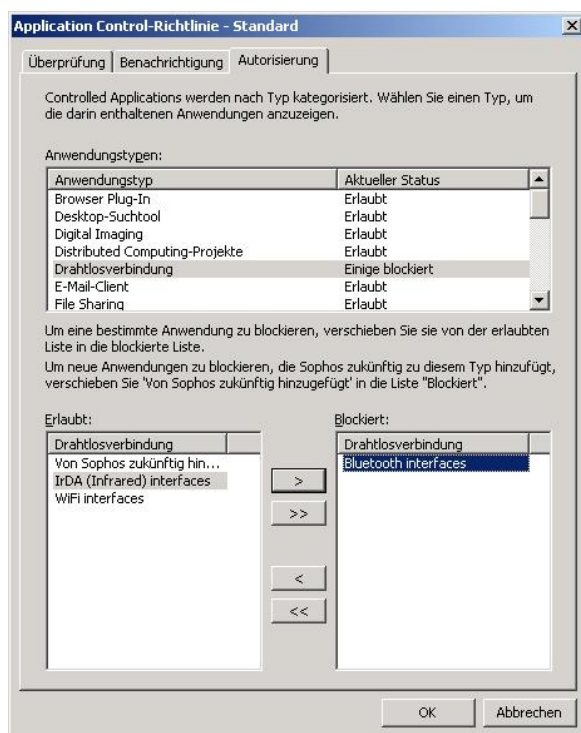


5. Klicken Sie auf **OK**.

## 2.3 Auswählen von Drahtlosverbindungen

**Wichtig:** Sie sollten keine Drahtlosverbindungen auf Computern sperren, auf denen Enterprise Console diese Verbindungsart erfordert.

1. Doppelklicken Sie im Fenster **Richtlinien** auf **Application Control**. Doppelklicken Sie dann auf die zu ändernde Richtlinie.
2. Klicken Sie im Dialogfeld der **Application Control-Richtlinie** auf die Registerkarte **Autorisierung**.
3. Wählen Sie **Drahtlosverbindungen**.
4. Wählen Sie aus der Liste **Erlaubt** die zu sperrende Art von Drahtlosverbindung und verschieben Sie sie in die Liste **Blockiert**.



5. Klicken Sie auf **OK**.

## 2.4 Erkennen von Geräten, ohne sie zu sperren

Sie können die On-Access-Überprüfung für gesperrte Geräte im **Erkennungsmodus** aktivieren, wodurch die Sperrung aufgehoben wird. Sobald Sie jedoch auf diese Geräte zugreifen möchten, wird eine Meldung ausgegeben, dass sie gemäß Ihrer Richtlinie gesperrt sind.

Wenn Sie mehr darüber erfahren möchten, auf welche Weise Enterprise Console gesperrte Geräte meldet, lesen Sie den Abschnitt [Was sind Alarme und Benachrichtigungen?](#) auf Seite 7.

**Wichtig:** Device Control ist eine Komponente von Application Control. Änderungen in diesem Bereich wirken sich auf alle Application Control-Richtlinien aus, die bereits im Einsatz sind.

1. Doppelklicken Sie im Fenster **Richtlinien** auf **Application Control**. Doppelklicken Sie dann auf die zu ändernde Richtlinie.
2. Klicken Sie im Dialogfeld der **Application Control-Richtlinie** auf die Registerkarte **Überprüfung**.
3. Markieren Sie das Kontrollkästchen **On-Access-Überprüfung aktivieren**.
4. Markieren Sie auch das Kontrollkästchen **Erkennen, Ausführung jedoch erlauben**.
5. Klicken Sie auf **OK**.

## 2.5 Erkennen und Sperren von Geräten

**Wichtig:** Device Control ist eine Komponente von Application Control. Änderungen in diesem Bereich wirken sich auf alle Application Control-Richtlinien aus, die bereits im Einsatz sind.

1. Doppelklicken Sie im Fenster **Richtlinien** auf **Application Control**. Doppelklicken Sie dann auf die zu ändernde Richtlinie.
2. Klicken Sie im Dialogfeld der **Application Control-Richtlinie** auf die Registerkarte **Überprüfung**.
3. Markieren Sie das Kontrollkästchen **On-Access-Überprüfung aktivieren**.
4. Deaktivieren Sie das Kontrollkästchen **Erkennen, Ausführung jedoch erlauben**.
5. Klicken Sie auf **OK**.

**Wichtig:** Arbeitsplatzrechner müssen neu gestartet werden, damit die neue Richtlinie zur Gerätespernung wirksam wird.

## 2.6 Einrichten von Alarmen und Benachrichtigungen

### 2.6.1 Was sind Alarme und Benachrichtigungen?

Enterprise Console meldet erkannte bzw. gesperrte Geräte über *Alarme* und *Benachrichtigungen*.

Standardmäßig werden die folgenden **Alarme** angezeigt:

- Alarme werden in Enterprise Console auf der Registerkarte **Status** angezeigt. Weitere Informationen finden Sie unter [Anzeigen der aktuellsten Alarme](#) auf Seite 11.
- Auf einem Arbeitsplatzrechner werden Alarme im **Quarantäne-Manager** von Sophos Anti-Virus angezeigt.

Sie können Enterprise Console so einrichten, dass nur bei der ersten Erkennung oder Sperrung eines Geräts Alarme angezeigt werden. Weitere Informationen finden Sie unter [Anzeigen von Alarmen nur bei erster Erkennung/Sperrung](#) auf Seite 8.

Sie können in Enterprise Console auch folgende **Benachrichtigungen** konfigurieren:

- E-Mail-Benachrichtigungen** Diese Benachrichtigungen werden an die in den Einstellungen Ihrer Antiviren- und HIPS-Richtlinie festgelegten Empfänger gesendet. Weitere Informationen finden Sie unter [Aktivieren von E-Mail-Benachrichtigungen](#) auf Seite 9.
- SNMP-Benachrichtigungen** Diese Benachrichtigungen werden an die in den Einstellungen Ihrer Antiviren- und HIPS-Richtlinie festgelegten Empfänger gesendet. Weitere Informationen finden Sie unter [Aktivieren von SNMP-Benachrichtigungen](#) auf Seite 10.
- Desktop-Benachrichtigungen** Diese Benachrichtigungen werden auf dem Arbeitsplatzrechner angezeigt. Weitere Informationen finden Sie unter [Aktivieren von Desktop-Benachrichtigungen](#) auf Seite 8.

## 2.6.2 Anzeigen von Alarmen nur bei erster Erkennung/Sperrung

Normalerweise wird bei *jeder* Sperrung oder Erkennung eines Geräts auf der Registerkarte **Status** ein Alarm angezeigt.

Durch die folgenden Schritte sorgen Sie dafür, dass nur bei der *ersten* Erkennung bzw. Sperrung ein Alarm angezeigt wird:

1. Doppelklicken Sie im Fenster **Richtlinien** auf **Application Control**. Doppelklicken Sie dann auf die zu ändernde Richtlinie.
2. Klicken Sie im Dialogfeld der **Application Control-Richtlinie** auf die Registerkarte **Benachrichtigung**.
3. Markieren Sie das Kontrollkästchen **Alarm nur bei der ersten Erkennung anzeigen**.
4. Klicken Sie auf **OK**.

## 2.6.3 Aktivieren von Desktop-Benachrichtigungen

Enterprise Console kann so konfiguriert werden, dass eine Desktop-Benachrichtigung auf Arbeitsplatzrechnern angezeigt wird, wenn ein Gerät gesperrt ist.

**Wichtig:** Device Control ist eine Komponente von Application Control. Änderungen in diesem Bereich wirken sich auf alle Application Control-Richtlinien aus, die bereits im Einsatz sind.

1. Doppelklicken Sie im Fenster **Richtlinien** auf **Application Control**. Doppelklicken Sie dann auf die zu ändernde Richtlinie.
2. Klicken Sie im Dialogfeld der **Application Control-Richtlinie** auf die Registerkarte **Benachrichtigung**.
3. Markieren Sie das Kontrollkästchen **Desktop-Benachrichtigung aktivieren**.
4. Geben Sie in das Feld **Benachrichtigungstext** eine Meldung ein, die unter dem Desktop-Benachrichtigungstext angezeigt werden soll.
5. Klicken Sie auf **OK**.



## 2.6.4 Aktivieren von E-Mail-Benachrichtigungen

Sie können Enterprise Console so einrichten, dass bei der Erkennung oder Sperrung eines Geräts eine E-Mail-Benachrichtigung gesendet wird. Die Empfänger von E-Mail-Benachrichtigungen sind in Ihrer Antiviren- und HIPS-Richtlinie festgelegt.

1. Doppelklicken Sie im Fenster **Richtlinien** auf **Application Control**. Doppelklicken Sie dann auf die zu ändernde Richtlinie.
2. Klicken Sie im Dialogfeld der **Application Control-Richtlinie** auf die Registerkarte **Benachrichtigung**.
3. Markieren Sie das Kontrollkästchen **E-Mail-Benachrichtigung aktivieren**.
4. Klicken Sie auf **OK**.

## 2.6.5 Aktivieren von SNMP-Benachrichtigungen


Sie können Enterprise Console so einrichten, dass bei der Erkennung oder Sperrung eines Geräts eine SNMP-Benachrichtigung gesendet wird. Die Empfänger von SNMP-Benachrichtigungen sind in Ihrer Antiviren- und HIPS-Richtlinie festgelegt.

1. Doppelklicken Sie im Fenster **Richtlinien** auf **Application Control**. Doppelklicken Sie dann auf die zu ändernde Richtlinie.
2. Klicken Sie im Dialogfeld der **Application Control-Richtlinie** auf die Registerkarte **Benachrichtigung**.
3. Markieren Sie das Kontrollkästchen **SNMP-Benachrichtigungen aktivieren**.
4. Klicken Sie auf **OK**.

## 3 Umgang mit Alarmen

### 3.1 Anzeigen der aktuellsten Alarme

1. Öffnen Sie die Liste der Computer und wählen Sie den Computer aus, zu dem Sie die neuesten Alarme anzeigen möchten.

Wenn ein Controlled Device erkannt wurde, so wird auf der Registerkarte **Status** neben einem Warnsymbol  die Meldung „Controlled Application erkannt“ angezeigt.

2. Klicken Sie auf die Registerkarte **Alarm- und Fehler-Details**.

Der Name des betreffenden Geräts wird in der Spalte **Objekt erkannt** angezeigt.

### 3.2 Anzeigen aller Alarme

1. Öffnen Sie die Liste der Computer und wählen Sie den betreffenden Computer aus.
2. Öffnen Sie eine beliebige Registerkarte, rechtsklicken Sie auf den Namen des betreffenden Computers und wählen Sie **Computer-Details öffnen**.

### 3.3 Erstellen von Berichten zu Device Control-Alarmen

Zu Device Control-Alarmen in Ihrem Netzwerk lassen sich Berichte (auch Reports genannt) erstellen.

1. Öffnen Sie das Menü **Extras** und wählen Sie **Reports öffnen**.

Das Fenster **Reporting** wird angezeigt.

2. Wählen Sie aus dem Dropdown-Menü die gewünschte Berichtart aus.

Option	Beschreibung
<b>Alarme nach Objektname</b>	In diesem Bericht wird die Anzahl der Alarme nach im Netzwerk erkannten Objekten (z.B. Virus oder PUA) sortiert festgehalten.
<b>Alarme nach Ort</b>	In diesem Bericht wird die Anzahl der Alarme pro Computer und Computergruppe festgehalten.
<b>Alarme nach Zeit</b>	In diesem Bericht wird die Anzahl der Alarme festgehalten, die über einen bestimmten Zeitraum gesendet wurden.
<b>Alarmverlauf</b>	In diesem Bericht wird jeder Alarm ausführlich beschrieben.

3. Klicken Sie auf die Registerkarte **Konfiguration**, um den Bericht anzupassen.
4. Klicken Sie auf die Registerkarte **Tabelle** oder **Diagramm**, wenn Sie den Bericht anzeigen möchten.

### **3.4 Löschen von Device Control-Alarmen aus der Konsole**

1. Öffnen Sie die Registerkarte **Status**, rechtsklicken Sie auf den Namen des Computers, auf dem die Device Control-Alarme gelöscht werden sollen, und wählen Sie **Alarme und Fehler bereinigen**.
2. Klicken Sie im Dialogfeld **Alarme und Fehler bereinigen** auf die Registerkarte **Alarme**.
3. Wählen Sie die zu löschenden Alarme aus.
4. Klicken Sie auf **OK**.

## **4 Technischer Support**

Technischen Support erhalten Sie auf <http://www.sophos.de/support/>.

Wenn Sie sich an den Technischen Support wenden, halten Sie möglichst folgende Informationen bereit:

- Sophos Software-Versionsnummer(n)
- Betriebssystem(e) und Patch-Level(s)
- Die genauen Fehlermeldungen

## **5 Copyright**

Copyright © 2008 Sophos Group. Alle Rechte vorbehalten. Diese Publikation darf weder elektronisch oder mechanisch reproduziert, elektronisch gespeichert oder übertragen, noch fotokopiert oder aufgenommen werden, es sei denn, Sie verfügen entweder über eine gültige Lizenz, gemäß der die Dokumentation in Übereinstimmung mit dem Lizenzvertrag reproduziert werden darf, oder Sie verfügen über eine schriftliche Genehmigung des Urheberrechtsinhabers.

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