

Sophos Endpoint Security and Control Einzelplatz-Startup-Anleitung

Sophos Endpoint Security and Control, Version 9.7
Sophos Anti-Virus für Mac OS X, Version 7

Stand: April 2011



Inhalt

- 1 Vorbereitung.....3
- 2 Installation und Konfiguration unter Windows.....4
- 3 Installation und Konfiguration unter Mac OS X.....8
- 4 Technischer Support.....10
- 5 Rechtlicher Hinweis.....11

1 Vorbereitung

1.1 Systemvoraussetzungen

Die Systemvoraussetzungen entnehmen Sie bitte der Sophos Website:

<http://www.sophos.de/products/all-sysreqs.html>.

Außerdem benötigen Sie Internetzugang, um die Software von der Sophos Website herunterladen zu können.

1.2 Voraussetzungen

Für die Installation und Konfiguration sind folgende Informationen erforderlich:

- Internetadresse (URL) und Download-Daten für den Standalone Installer von Sophos Endpoint Security and Control und/oder für Sophos Anti-Virus für Mac OS X.
- Adresse der Update-Quelle, wenn Sie Ihre Updates nicht direkt von Sophos beziehen.
- Die zum Zugriff auf die Update-Quelle erforderlichen Zugangsdaten.
- Daten des Proxyservers, der ggf. die Update-Quelle abrufen (Adresse, Portnummer, Zugangsdaten).

2 Installation und Konfiguration unter Windows

2.1 Installation von Sophos Endpoint Security and Control

Melden Sie sich zur Installation von Sophos Endpoint Security and Control als Administrator an.

Wenn Sie Sicherheitssoftware anderer Hersteller installiert haben, gehen Sie folgendermaßen vor:

- Die Benutzeroberfläche dieser Software darf nicht geöffnet sein.
 - Die Firewall und HIPS-Software anderer Hersteller muss deaktiviert sein oder das Sophos Installationsprogramm zulassen.
1. Laden Sie den Standalone Installer für Ihre Windows-Version von der Sophos Website herunter. Geben Sie bei entsprechender Aufforderung Ihre Zugangsdaten ein.
 2. Öffnen Sie den Ordner, in dem der Installer nach dem Download gespeichert wurde. Doppelklicken Sie auf den Installer. Klicken Sie im Installer-Fenster auf **Installieren**. Der Installationsassistent wird gestartet.
 3. Klicken Sie auf der ersten Seite des **Sophos Endpoint Security and Control Installationsassistenten** auf **Weiter**.
 4. Klicken Sie auf der Seite **Lizenzvereinbarung** auf **Ich akzeptiere die Bedingungen der Lizenzvereinbarung**. Klicken Sie auf **Weiter**.
 5. Wählen Sie auf der Seite **Zielordner** ggf. den Ordner aus, in dem Sophos Endpoint Security and Control installiert werden soll. Klicken Sie auf **Weiter**.
 6. Geben Sie auf der Seite **Quelle aktualisieren** die Angaben zum Standort ein, von dem Sie Ihre Updates beziehen. Erledigen Sie dies am besten sofort.
 - a) Wählen Sie im Feld **Adresse Sophos** aus. Wenn Sie über eine andere Adresse für die Update-Quelle verfügen, geben Sie diese ein.
 - b) Geben Sie in die Felder **Benutzername** und **Kennwort** die für die Anmeldung an der Update-Quelle erforderlichen Zugangsdaten ein.
 - c) Wenn Sie über einen Proxyserver auf das Netzwerk oder Internet zugreifen, aktivieren Sie das Kontrollkästchen **Auf die Update-Quelle über Proxy zugreifen** und klicken Sie auf **Weiter**. Machen Sie die erforderlichen Angaben zum Proxyserver.

Hinweis: Wenn Sie die Angaben zur Update-Quelle später vervollständigen möchten, aktivieren Sie das Kontrollkästchen **Ich gebe diese Zugangsdaten später ein**. Öffnen Sie nach der Installation Sophos Endpoint Security and Control und wählen Sie die Option **AutoUpdate konfigurieren** aus.

Standardmäßig führt Sophos Endpoint Security and Control alle 60 Minuten ein Update durch, sofern die Update-Quelle angegeben wurde und eine Netzwerkverbindung vorhanden ist.

7. Wenn Sie die Firewall installieren möchten, wählen Sie auf der Seite **Wählen Sie weitere Komponenten aus, die Sie installieren möchten** die Option **Sophos Client Firewall installieren** aus und klicken Sie auf **Weiter**.

8. Aktivieren Sie bei Bedarf auf der Seite **Software von Fremdherstellern entfernen** die **gleichnamige Option** und klicken Sie auf **Weiter**.
9. Klicken Sie auf der Seite **Sophos Endpoint Security and Control kann jetzt installiert werden** auf **Weiter**.

Die Software wird nun installiert.

Wichtig: Update-Tools für Fremdsoftware werden hierbei mitunter nicht automatisch entfernt. Sie können diese Tools über die Systemsteuerung entfernen.

10. Geben Sie auf der letzten Seite des Installationsassistenten an, ob ein Neustart durchgeführt werden soll und klicken Sie auf **Fertigstellen**.

Ein Neustart ist erforderlich:



- zum Aktivieren der Firewall
- zur vollständigen Entfernung von Fremdsoftware.

Die Installation von Sophos Endpoint Security and Control ist abgeschlossen, wenn das Symbol von Sophos Endpoint Security and Control in der Taskleiste von Windows angezeigt wird.



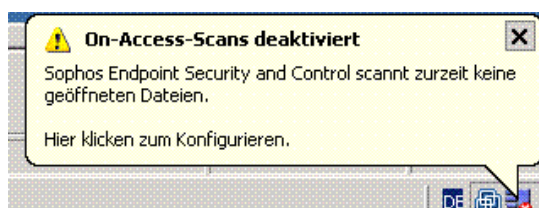
2.1.1 Bedeutung der Taskleisten-Symbole

Das Symbol von Sophos Endpoint Security and Control ändert sich bei ausstehenden Alerts oder Problemen beim Virenschutz. In der folgenden Tabelle werden die Taskleisten-Symbole vorgestellt.

Symbol	Grund
	<ul style="list-style-type: none"> ■ Auf dem Computer werden keine On-Access-Scans durchgeführt. ■ Eine Firewall-Meldung wird angezeigt. ■ Eine Controlled Application wurde erkannt. ■ Ein angeschlossenes Gerät hat eine Device Control-Meldung hervorgerufen. ■ Eine Meldung zur „Data Control“ wird angezeigt. ■ Eine Website wurde gesperrt.
	<ul style="list-style-type: none"> ■ Sophos Endpoint Security and Control konnte kein Update durchführen. ■ Ein Sophos Dienst ist fehlerhaft.

Zudem wird eine Sprechblase mit Hintergrundinformationen angezeigt.

Wenn beispielsweise die On-Access-Scans nicht aktiviert sind, wird folgende **Sprechblasenmeldung** im Statusbereich der Taskleiste angezeigt:



2.2 Konfigurieren der Firewall

Folgende Firewall-Optionen müssen aktiviert werden:

- Verarbeiten von Firewall-Meldungen.
- Gewähren von Netzwerk- oder Internetzugang für Programme.
- Sperren unbekannter Programme.

2.2.1 Verarbeiten von Firewall-Meldungen

Die Firewall befindet sich standardmäßig im „interaktiven“ Modus: Wenn die Firewall einen noch nicht zugelassenen Prozess oder eine noch nicht zugelassen Anwendung erkennt, zeigt sie eine entsprechende Meldung an. Sie können nun entscheiden, ob der Prozess/die Anwendung gesperrt oder zugelassen werden soll.

Es empfiehlt sich, unbekanntem Datenfluss einmalig zu sperren. Wenn die Firewall zum Beispiel eine Meldung über einen versteckten Prozess anzeigt, klicken Sie auf **Diesen Prozess dieses Mal sperren** und dann auf **OK**.

Wenn Sie den Prozess nicht nur einmalig sperren können, konnte die Anwendung/der Prozess, die den Datenfluss auslöst, wahrscheinlich nicht ermittelt werden. Lassen Sie in diesem Fall die Anwendung/den Prozess zu oder sperren Sie sie/ihn. Diese Einstellung können Sie zu einem späteren Zeitpunkt durch Bearbeiten der Firewall-Konfiguration wieder ändern. Details zu diesem Thema entnehmen Sie bitte der Hilfe zu Sophos Endpoint Security and Control.

Einige Prozesse sollten Sie nicht sperren. Darunter fallen Meldungen zu Prüfsummen und Anwendungsregeln in Bezug auf Browser, E-Mail-Programm und andere Programme, die Internet- oder Netzwerkzugriff erhalten sollen.

2.2.2 Einrichten des Netzwerk- oder Internetzugangs für Programme

Die Firewall muss aktiviert sein, um den gewünschten Programmen Netzwerk- oder Internetzugang gewähren zu können.

1. Öffnen Sie das Programm, das auf das Netzwerk oder Internet zugreifen soll (z.B. ein Browser oder E-Mail-Programm).

2. Die Firewall meldet, dass eine neue oder modifizierte Anwendung Netzwerkzugriff angefordert hat. Klicken Sie auf **Prüfsumme zu vorhandenen Prüfsummen für diese Anwendung hinzufügen** und dann auf **OK**.
3. Nun meldet die Firewall eine weitere Anwendung (z.B. Ihr Browser oder Ihr E-Mail-Programm), die Netzwerkzugriff angefordert hat. Klicken Sie auf **Regel für diese Anwendung mit Preset erstellen**. Achten Sie dabei darauf, dass Sie die richtigen Einstellungen für das Programm (z.B. ein **Browser** oder **E-Mail-Client**) im Feld auswählen und klicken Sie auf **OK**.

Sie können die Firewall-Konfiguration auch dahingehend ändern, dass Programmen der Netzwerk- oder Internetzugang in allen Modi gewährt wird. Nähere Informationen finden Sie in der Hilfe zu Sophos Endpoint Security and Control.

2.2.3 Einrichten des Netzwerk- oder Internetzugangs für andere Programme

Es kann sein, dass neben Browser und E-Mail-Programm noch andere Programme Netzwerk- oder Internetzugriff benötigen, z.B. Windows Update. Verwenden Sie hierzu den interaktiven Modus und befolgen Sie die Anweisungen im Abschnitt [Einrichten des Netzwerk- oder Internetzugangs für Programme](#) (Seite 6).

In der Hilfe zu Sophos Endpoint Security and Control wird die Aktivierung von FTP-Downloads beschrieben.

2.2.4 Sperren unbekannter Programme

Versetzen Sie die Firewall nun in den automatischen Modus und aktivieren Sie das Sperren unbekannter Programme.

1. Rechtsklicken Sie im Statusbereich der Taskleiste auf das Sophos Endpoint Security and Control-Symbol. Wählen Sie **Sophos Endpoint Security and Control öffnen**.
2. Klicken Sie im Fenster von **Sophos Endpoint Security and Control** im Bereich **Firewall** auf **Firewall konfigurieren**.

Das Konfigurationsfenster der **Firewall** wird angezeigt.

3. Klicken Sie auf der Registerkarte **Allgemein** unter **Konfiguration** auf **Konfigurieren**.
4. Wählen Sie im Dialogfeld zur Auswahl des Speicherorts unter **Arbeitsmodus** die Option **Standardmäßig sperren. Datenfluss ohne passende Regel wird gesperrt**.

Von nun an zeigt die Firewall keine Meldungen bezüglich unbekannter Prozesse mehr an. Sie werden stattdessen in ein Protokoll geschrieben. Wenn beim Erkennen von nicht zulässigem Datenfluss durch die Firewall eine Sprechblasenmeldung angezeigt werden soll, ändern Sie die Firewall-Konfiguration. Details zu diesem Thema entnehmen Sie bitte der Hilfe zu Sophos Endpoint Security and Control.

Hinweis: In einigen Fällen, z.B. bei Windows-Updates, kann das Umschalten in den interaktiven Modus erforderlich sein. Wenn das ausgewählte Programm ausgeführt wurde, sollten Sie den Modus wieder wechseln.

3 Installation und Konfiguration unter Mac OS X

3.1 Installation von Sophos Anti-Virus

Vor der Installation von Sophos Anti-Virus muss jegliche Sicherheitssoftware anderer Hersteller deinstalliert werden.

Melden Sie sich als Administrator an.

1. Laden Sie den Sophos Anti-Virus-Standalone Installer für Mac OS X von der Sophos Website herunter. Geben Sie bei entsprechender Aufforderung Ihre Zugangsdaten ein.
2. Öffnen Sie den Ordner, in dem der Installer nach dem Download gespeichert wurde. Öffnen Sie das Image. Suchen Sie die Datei Sophos Anti-Virus.mpkg. Doppelklicken Sie darauf, um den Installer zu starten.
3. Klicken Sie auf **Weiter**. Befolgen Sie die Installationsanweisungen.

Die Installation von Sophos Anti-Virus ist abgeschlossen, wenn das Sophos Anti-Virus-Symbol rechts in der Menüleiste schwarz angezeigt wird.



Wenn das Symbol grau ist, bedeutet das, dass der On-Access-Scanner nicht aktiviert ist und das System somit nicht über On-Access-Schutz verfügt. Wenden Sie sich bitte an Ihren Administrator.

3.2 Konfigurieren der Updates von Sophos Anti-Virus

Sie müssen als Administrator angemeldet sein.

1. Klicken Sie auf das Sophos Anti-Virus-Symbol auf der rechten Seite der Menüleiste und wählen Sie anschließend die Option Einstellungen aufrufen aus dem Kurzbefehlmeneü aus.
2. Klicken Sie auf **AutoUpdate**.
3. Wenn bestimmte Einstellungen nicht hervorgehoben sind, klicken Sie auf das Schlosssymbol und geben Sie einen Administratorennamen und ein Kennwort ein.
4. Ändern Sie die Einstellungen wie folgt:
 - Wenn Sophos Anti-Virus Updates direkt von Sophos beziehen soll, wählen Sie im Einblendmenü **Update vom Primärserver** die Option **Sophos** aus. Geben Sie Ihre Sophos Zugangsdaten in die Felder **Benutzername** und **Kennwort** ein.
 - Wenn Sophos Anti-Virus Updates direkt von Ihrem Unternehmens-Webserver beziehen soll, wählen Sie aus dem Einblendmenü **Update vom Primärserver** die Option **Unternehmens-Webserver** aus. Geben Sie in das **Adressfeld** die Internetadresse der Update-Quelle an. Geben Sie die Zugangsdaten des Servers in die Felder **Benutzername** und **Kennwort** ein.

- Wenn Sophos Anti-Virus Updates aus einem Netzwerkvolume beziehen soll, wählen Sie im Einblendmenü **Update vom Primärserver** die Option **Netzwerkvolume** aus. Geben Sie in das **Adressfeld** die Netzwerkadresse der Update-Quelle an. Geben Sie in die Felder **Benutzername** und **Kennwort** die Zugangsdaten des Volumes ein.

Die Adresse lautet etwa wie folgt: Der Text in Klammern muss angepasst werden:

http://<Server>/<Internetfreigabe>/Sophos Anti-Virus/ESCOSX

smb://<Server>/<Samba-Freigabe>/Sophos Anti-Virus/ESCOSX

afp://<Server>/<Apple-Freigabe>/Sophos Anti-Virus/ESCOSX

Anstatt des Domänen- oder Hostnamens können Sie auch die IP-Adresse oder den NetBIOS-Namen angeben. Die Eingabe der IP-Adresse empfiehlt sich insbesondere bei DNS-Problemen.

5. Wenn Sophos Anti-Virus Updates über den in den Systemeinstellungen festgelegten Proxyserver beziehen soll, wählen Sie die Option **Systemeinstellungen des Proxyservers** aus dem Einblendmenü im unteren Bereich des Abschnitts **Primärserver**.
6. Wenn Sophos Anti-Virus Updates von einem benutzerdefinierten Proxyserver beziehen soll, verfahren Sie wie folgt:
 - a) Wählen Sie die Option **Kundenspezifische Proxyeinstellungen** aus dem Einblendmenü im unteren Bereich des Abschnitts **Primärserver** aus.
 - b) Ein Dialog wird geöffnet. Geben Sie die Adresse und Portzahl des Proxyservers in die **Adressfelder** ein. Geben Sie in die Felder **Benutzername** und **Kennwort** die Zugangsdaten des Proxyservers ein.
7. Wählen Sie die Option **Suche nach Updates bei Verbindung zum Netzwerk oder Internet**.

Sophos Anti-Virus lädt nun automatisch Updates von der angegebenen Update-Quelle herunter. Standardmäßig wird alle 60 Minuten ein Update heruntergeladen (sofern eine Netzwerkverbindung besteht). Wenn das Sophos Anti-Virus-Symbol im rechten Bereich der Menüleiste ein weißes X aufweist, wurde die Software nicht aktualisiert. Wenden Sie sich bitte an Ihren Administrator.

4 Technischer Support

Technischen Support zu Sophos Produkten können Sie wie folgt abrufen:

- Rufen Sie das SophosTalk-Forum unter <http://community.sophos.com/> auf und suchen Sie nach Benutzern mit dem gleichen Problem.
- Durchsuchen Sie die Support-Knowledgebase unter <http://www.sophos.de/support/>.
- Laden Sie Dokumentation zu den Produkten unter <http://www.sophos.de/support/docs/> herunter.
- Senden Sie eine E-Mail an den technischen Support support@sophos.de und geben Sie die Versionsnummer(n), Betriebssystem(e) und Patch Level Ihrer Sophos Software sowie ggf. den genauen Wortlaut von Fehlermeldungen an.

5 Rechtlicher Hinweis

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

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

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.

iMatix SFL

This product uses parts of the iMatix SFL, Copyright © 1991-2000 iMatix Corporation <<http://www.imatix.com>>.