

Sophos Endpoint Security and Control 9.7 Schnellstartanleitung

Stand: April 2011



Inhalt

| | | |
|----|--|----|
| 1 | Einleitung..... | 3 |
| 2 | Installierte Software..... | 3 |
| 3 | Vorgehensweise..... | 3 |
| 4 | Systemvoraussetzungen..... | 4 |
| 5 | Installationsvorbereitung..... | 4 |
| 6 | Herunterladen der Installer..... | 5 |
| 7 | Installation von Enterprise Console | 5 |
| 8 | Download von Sicherheitssoftware..... | 6 |
| 9 | Installation von NAC Manager | 6 |
| 10 | Erstellen von Computergruppen..... | 7 |
| 11 | Einrichten von Sicherheitsrichtlinien..... | 7 |
| 12 | Suchen nach Computern..... | 8 |
| 13 | Schützen von Computern..... | 8 |
| 14 | Überprüfen der Netzwerkintegrität..... | 10 |
| 15 | Fehlersuche..... | 10 |
| 16 | Hilfe für gängige Tasks..... | 10 |
| 17 | Technischer Support..... | 11 |
| 18 | Rechtlicher Hinweis..... | 12 |

1 Einleitung

In dieser Anleitung wird beschrieben, wie Sie Ihr Netzwerk mit Sophos Sicherheitssoftware schützen.

Wenn Sie Sophos Software zum ersten Mal installieren, lesen Sie bitte diese Anleitung.

Wenn Sie ein Upgrade durchführen, finden Sie im **Endpoint Security and Control 9.5 Upgrade Center** unter <http://www.sophos.de/support/upgrades/> hilfreiche Tipps.

Hinweis: Bei größeren Netzwerken bieten sich die Installationsoptionen in der *Erweiterten Startup-Anleitung zu Sophos Endpoint Security and Control* an.

2 Installierte Software

Es werden zwei Management-Tools installiert:

- **Sophos Enterprise Console.** Diese Konsole ermöglicht die Installation und Verwaltung von Sicherheitssoftware auf Netzwerkcomputern.
- **Sophos NAC Manager.** Damit können Sie „Network Access Control“ verwenden. Mit Network Access Control können Sie nicht zugelassenen Computern oder Computern, die nicht den Sicherheitsstandards entsprechen, den Netzwerkzugriff verweigern.

Die Installation von NAC Manager ist optional.

Hinweis: Die Tools werden separat über zwei verschiedene Setup-Programme installiert.

Hinweis: Sie können beide Tools auf einem Server installieren. Bei mehr als 1000 Computern sollten Sie die Tools jedoch auf separaten Servern installieren. Die Vorgehensweise ist hierbei jedoch identisch.

3 Vorgehensweise

Das Upgrade umfasst folgende Schritte:

- Überprüfen der Systemvoraussetzungen.
- Vorbereiten der Installation.
- Herunterladen der Installer.
- Installieren von Enterprise Console.
- Download von Sicherheitssoftware.
- Installieren von NAC Manager.
- Erstellen von Computergruppen.
- Einrichten von Sicherheitsrichtlinien.
- Suchen nach Computern.
- Schützen der Computer.
- Überprüfen der Netzwerkintegrität.

4 Systemvoraussetzungen

Überprüfen Sie vor der Installation die Hardware-, Betriebssystems- und Softwarevoraussetzungen.

4.1 Hardware und Betriebssystem

Die System- und Softwarevoraussetzungen finden Sie auf der Sophos Website:
<http://www.sophos.de/products/all-sysreqs.html>.

4.2 Microsoft Systemsoftware

Enterprise Console setzt bestimmte Microsoft Systemsoftware (z.B. Datenbanksoftware) voraus.

Der Enterprise Console-Installer versucht, die Systemsoftware zu installieren, wenn sie nicht bereits auf dem Server vorhanden ist. Wenn die Software jedoch nicht mit dem Server oder Ihren Anforderungen kompatibel ist, muss die Installation manuell durchgeführt werden.

SQL-Serverinstallation

Der Installer versucht, SQL Server 2008 Express zu installieren, sofern Sie nicht bereits SQL Server 2005 Express oder höher nutzen. Hinweis:

- Es wird davon abgeraten, SQL Server auf einem Domänencontroller zu installieren.
- SQL Server 2008 Express ist nicht mit Windows Server 2003 SP1, Windows XP 64-Bit SP1 oder Windows Essential Business Server 2008 kompatibel.
- In Windows Server 2008 R2 Datacenter müssen Sie die Domänenfunktionsebene auf Windows Server 2003 erhöhen. Anweisungen hierzu finden Sie unter:
<http://support.microsoft.com/kb/322692>

.NET Framework-Installation

Der Installer versucht, .NET Framework 3.5 zu installieren, sofern es nicht bereits vorhanden ist. Hinweis:

- Der Installer kann .NET Framework 3.5 nicht auf Computern mit Windows Server 2008 R2 installieren. Sie müssen die Komponente über den Bereich „Funktionen“ im Server Manager hinzufügen.

Hinweis: Nach der Installation der erforderlichen Systemsoftware müssen die Computer eventuell neu gestartet werden. Weitere Informationen finden Sie im Sophos Support-Artikel 65190 (<http://www.sophos.de/support/knowledgebase/article/65190.html>).

5 Installationsvorbereitung

Wählen Sie einen Server aus, der die Systemvoraussetzungen erfüllt und treffen Sie folgende Vorbereitungen:

- Der Server muss mit dem Internet verbunden sein.

- Sie benötigen die Windows-Betriebssystem-CD und Service-Pack-CDs. Sie müssen die CDs möglicherweise im Laufe der Installation einlegen.
- Wenn der Server unter Windows Server 2008 oder höher betrieben wird, deaktivieren Sie die Benutzerkontensteuerung und starten Sie den Server neu.

Hinweis: Nach dem Abschluss der Installation und dem Download der Sicherheitssoftware können Sie die Benutzerkontensteuerung wieder aktivieren.

6 Herunterladen der Installer

Laden Sie die Sophos Installer herunter und platzieren Sie sie auf dem Server, auf dem die Management-Tools installiert werden sollen.

1. Rufen Sie <http://www.sophos.de/support/updates/> auf.
2. Geben Sie Ihre MySophos-Zugangsdaten ein.
3. Verfahren Sie auf der Download-Seite von **Enterprise** wie folgt:
 - Laden Sie den Installer für Enterprise Console herunter.
 - Wenn Sie NAC Manager verwenden, laden Sie den Sophos NAC-Installer herunter.
4. Kopieren Sie die heruntergeladenen Installer bei Bedarf auf den Server, auf dem die Installation durchgeführt werden soll.

Wenn Sie NAC Manager nicht auf dem gleichen Server wie Enterprise Console installieren, sollten Sie den Installer auf den Server kopieren.

7 Installation von Enterprise Console

So installieren Sie Enterprise Console:

1. Melden Sie sich auf dem Computer, auf dem sich Enterprise Console befindet, als Administrator an:
 - Wenn sich der Computer in einer Domäne befindet, melden Sie sich als Domänenadministrator an.
 - Wenn sich der Computer in einer Arbeitsgruppe befindet, melden Sie sich als lokaler Administrator an.
2. Suchen Sie den Enterprise Console-Installer, den Sie im Vorfeld heruntergeladen haben.

Tipp: Der Dateiname des Installers enthält "sec".
3. Doppelklicken Sie auf den Installer.
4. Klicken Sie im Dialogfeld **Sophos Endpoint Security and Control-Netzwerk-Installer** auf **Installieren**.

Die Installationsdateien werden auf den Computer kopiert und ein Installationsassistent öffnet sich.
5. Klicken Sie im Dialogfeld **Sophos Enterprise Console** auf **Weiter**.

6. Es wird ein Assistent gestartet, der Sie durch die Installation leitet. Gehen Sie folgendermaßen vor:
 - a) Übernehmen Sie die Standardwerte, sofern dies möglich ist.
 - b) Wählen Sie ein **vollständiges** Setup.
7. Nach der Installation ist eventuell ein Neustart erforderlich. Klicken Sie auf **Ja** oder **Fertigstellen**.

8 Download von Sicherheitssoftware

Wenn Sie sich nach der Installation zum ersten Mal wieder am System anmelden oder einen Neustart durchführen, wird Enterprise Console automatisch geöffnet und ein Assistent wird ausgeführt.

Hinweis: Wenn Sie über die Remotedesktop-Funktion installiert haben, wird die Konsole nicht automatisch geöffnet. Öffnen Sie die Konsole in diesem Fall über das Start-Menü.

Der Assistent leitet Sie durch die Auswahl und den Download der Sicherheitssoftware. Gehen Sie folgendermaßen vor:

1. Geben Sie auf der Seite **Sophos Download-Konto** Ihren Benutzernamen und Ihr Kennwort (in Ihrer Lizenz enthalten) ein. Wenn Sie über einen Proxyserver auf das Internet zugreifen, aktivieren Sie das Kontrollkästchen **Verbindung zu Sophos über Proxyserver herstellen**.
2. Wählen auf der Seite **Plattformauswahl** die Systeme aus, die jetzt geschützt werden sollen. Klicken Sie auf **Weiter**. Enterprise Console lädt die Software herunter.
3. Der Download-Fortschritt wird auf der Seite **Software wird heruntergeladen** angezeigt. Klicken Sie bei Bedarf auf **Weiter**.
4. Wählen Sie auf der Seite **Computer aus Active Directory importieren** die Option **Gruppen erstellen** aus, wenn Enterprise Console Ihre vorhandenen Computergruppen aus Active Directory nutzen soll.

Wenn die Benutzerkontensteuerung vor der Installation deaktiviert wurde, können Sie sie jetzt wieder aktivieren.

9 Installation von NAC Manager

Sie benötigen die Windows-Betriebssystem-CD und Service-Pack-CDs. Sie müssen die CDs möglicherweise im Laufe der Installation einlegen.

Hinweis: Wenn Sie NAC Manager nicht auf dem gleichen Server wie Enterprise Console installieren, müssen Sie zunächst manuell eine Datenbank von SQL Server 2005 oder höher installieren.

1. Melden Sie sich auf dem Computer, auf dem Sie NAC Manager installieren möchten, als Administrator an:
 - Wenn sich der Computer in einer Domäne befindet, melden Sie sich als Domänenadministrator an.
 - Wenn sich der Computer in einer Arbeitsgruppe befindet, melden Sie sich als lokaler Administrator an.

- Suchen Sie den Sophos NAC-Installer, den Sie im Vorfeld heruntergeladen haben.

Tipp: Der Dateiname des Installers beinhaltet "nac".

- Doppelklicken Sie auf den Installer.
- Klicken Sie im Dialogfeld **Sophos NAC Manager** auf **Installieren**.
- Es wird ein Assistent gestartet, der Sie durch die Installation leitet.

10 Erstellen von Computergruppen

Wenn Sie Ihre Computergruppen mit dem **Download-Assistenten für Sicherheitssoftware** (auf der Basis Ihrer Active Directory-Gruppen) eingerichtet haben, können Sie diesen Abschnitt überspringen. Rufen Sie [Einrichten von Sicherheitsrichtlinien](#) (Seite 7) auf.

Zunächst müssen Gruppen erstellt werden.

- Öffnen Sie Enterprise Console.
- Stellen Sie sicher, dass der Servername oben im Fensterbereich **Gruppen** (links in der Konsole) ausgewählt ist.
- Klicken Sie in der Symbolleiste auf das Symbol **Gruppe erstellen**.
Es wird eine „Neue Gruppe“ zur Liste hinzugefügt, deren Name markiert ist.
- Geben Sie einen Namen für die Gruppe ein.

Weitere Gruppen können im linken Fensterbereich erstellt werden. Wählen Sie den oben angezeigten Server, wenn Sie eine weitere Hauptgruppe einrichten möchten. Wenn Sie in einer Gruppe eine Untergruppe erstellen möchten, wählen Sie die Gruppe. Erstellen Sie dann die Gruppe und benennen Sie sie.

11 Einrichten von Sicherheitsrichtlinien

Enterprise Console übernimmt die Standard-Sicherheitsrichtlinien für Ihre Computergruppen. Sie müssen die Richtlinien nur unter folgenden Voraussetzungen ändern:

- Sie müssen jetzt eine Firewall-Richtlinie einrichten.
- Sie müssen die Network Access Control-, Application Control-, Data Control- oder Device Control-Richtlinien ändern für den Fall, dass Sie diese Funktionen nutzen möchten. Dies können Sie jederzeit tun.

11.1 Einrichten einer Firewall-Richtlinie

Hinweis: Netzwerkadapter sind im Verlauf der Installation vorübergehend nicht verfügbar. Vernetzte Anwendungen, wie Microsoft Remote Desktop, werden unter Umständen abgetrennt.

Standardmäßig blockiert die Firewall alle nicht notwendigen Verbindungen. Sie müssen die Firewall zunächst konfigurieren.

- Doppelklicken Sie im Bereich **Richtlinien** auf **Firewall**.
- Doppelklicken Sie auf die **Standardrichtlinie**, um sie zu ändern. Ein Assistent wird gestartet.

3. Die Auswahl der folgenden Optionen im **Firewall-Richtlinienassistenten** wird empfohlen:
 - a) Wählen Sie auf der Seite **Firewall konfigurieren** die Option **Einseitig** aus, sofern die Firewall-Einstellungen nicht standortabhängig sein sollen.
 - b) Wählen Sie auf der Seite **Arbeitsmodus** die Option **Eingehenden Datenfluss blockieren, ausgehenden Datenfluss erlauben**.
 - c) Wählen Sie auf der Seite **Datei- und Druckerfreigabe** die Option **Datei- und Druckerfreigabe zulassen** aus.

12 Suchen nach Computern

Sie müssen zuerst nach Computern im Netzwerk suchen, bevor sie von Enterprise Console geschützt und verwaltet werden können.

1. Klicken Sie in der Symbolleiste auf das Symbol **Computer suchen**.
2. Wählen Sie die gewünschte Suchmethode aus.
3. Melden Sie sich an und wählen Sie ggf. einen Netzwerkpfad für die Suche aus.

Wenn Sie eine der **Suchoptionen** verwenden, werden die Computer im Ordner **Nicht zugewiesen** abgelegt.

13 Schützen von Computern

Zum Schutz von Computern sind folgende Schritte erforderlich:

- Vorbereiten von Computern.
- Automatisches Schützen von Windows-Systemen
- Manueller Schutz von Windows oder Mac OS X Computern.

13.1 Vorbereitungen

Es sind zunächst einige vorbereitende Schritte erforderlich.

Vorbereiten der Entfernung von Sicherheitssoftware anderer Hersteller

Wenn das Sophos Installationsprogramm andere installierte Sicherheitssoftware entfernen soll, gehen Sie folgendermaßen vor:

- Sollte auf einigen Computern die Virenschutzsoftware anderer Hersteller laufen, schließen Sie die Benutzeroberfläche.
- Sollte auf einigen Computern die Firewall oder das HIPS-Produkt eines anderen Herstellers laufen, deaktivieren Sie diese Software oder stellen Sie sie so ein, dass das Sophos Installationsprogramm ausgeführt werden kann.

Falls auf Computern das Update-Tool anderer Hersteller läuft, sollten Sie es eventuell entfernen. In den Abschnitten „Entfernen von Sicherheitssoftware anderer Hersteller“ und „Schutz von Computern“ der Hilfe zu Enterprise Console finden Sie weitere Hinweise zu diesem Thema.

Prüfen auf ein geeignetes Konto zur Installation von Software

Sie werden zur Eingabe der Daten eines Kontos aufgefordert, das zur Installation von Sicherheitssoftware verwendet werden kann. Dabei handelt es sich meist um ein Administratorkonto. Das Konto muss:

- lokale Administratorrechte auf den Computern haben, die Sie schützen möchten.
- Zugriff auf den Computer haben, auf dem Enterprise Console installiert ist.
- Lesezugriff auf das Update-Verzeichnis haben, von dem die Computer Updates beziehen. Doppelklicken Sie im Bereich **Richtlinien** auf **Update** und dann auf **Standard**, um dies zu überprüfen.

Vorbereiten der Installation von Network Access Control

Vor der Installation von Network Access Control müssen Sie den folgenden Schritt durchführen:

- Geben Sie die URL des Computers an, auf dem NAC Manager installiert wurde. Rufen Sie in Enterprise Console das Menü **Extras** auf und klicken Sie auf **NAC URL konfigurieren**.

13.2 Automatisches Schützen von Windows-Computern

So schützen Sie die Computer:

1. Wählen Sie die Computer, die geschützt werden sollen.
2. Rechtsklicken Sie auf die Auswahl und wählen Sie **Computer schützen**.

Hinweis: Wenn sich Computer in der Gruppe **Nicht zugewiesen** befinden, ziehen Sie sie einfach in die gewünschten Gruppen.

3. Ein Assistent leitet Sie durch die Installation der Sophos Sicherheitssoftware. Gehen Sie folgendermaßen vor:
 - a) Auf der Seite **Funktionsauswahl** können Sie optionale Funktionen installieren. Wählen Sie **Compliance Control**, wenn Sie Network Access Control nutzen können.
 - b) Sehen Sie auf der Seite **Schutz-Übersicht** nach, ob Installationsprobleme aufgeführt werden. Hilfe erhalten Sie unter [Fehlersuche](#) (Seite 10).
 - c) Geben Sie im Dialogfeld **Zugangsdaten** die Daten eines Kontos an, über das Software auf den Computern installiert werden kann.

Die Installation erfolgt gestaffelt. Es kann also einige Minuten dauern, bis der Vorgang auf allen Computern abgeschlossen ist.

Überprüfen Sie nach Abschluss der Installation noch einmal die Computerliste. Wenn in der Spalte **OnAccess Aktiv** angezeigt wird, werden On-Access-Viren-Scans durchgeführt.

13.3 Manueller Schutz von Windows- oder Mac OS X-Computern

Führen Sie zum Schutz von Computern, die nicht automatisch geschützt werden können, ein Setup-Programm in einem zentralen Installationsverzeichnis aus.

Das Verzeichnis des Setup-Programms finden Sie in Enterprise Console unter **Ansicht > Bootstrap-Verzeichnisse**.

1. Melden Sie sich an jedem Computer mit lokalen Administratorrechten an.
2. Doppelklicken Sie im zentralen Installationsverzeichnis auf das Setup-Programm.
 - Das Setup-Programm für Windows-Computer heißt „setup.exe“.
 - Das Setup-Programm für Mac OS X heißt „Sophos Anti-Virus.mpkg“.
3. Es wird ein Assistent gestartet, der Sie durch die Installation leitet.

14 Überprüfen der Netzwerkintegrität

So können Sie in Enterprise Console die Netzwerkintegrität überprüfen:

1. Klicken Sie in der Menüleiste auf das Symbol **Dashboard**, falls das Dashboard nicht bereits angezeigt wird.

Im Dashboard wird angezeigt, wie viele Computer

- Threats erkannt haben.
 - sich nicht auf dem neuesten Stand befinden.
 - nicht mit Richtlinien übereinstimmen.
2. Mit Sophos NAC Manager lassen sich außerdem richtlinienkonforme Computer anzeigen:
 - a) Wählen Sie **Datei > Öffnen > NAC**.
 - b) Klicken Sie in NAC Manager auf **Report > Compliance**.Nun werden die Computer angezeigt, die mit der NAC-Richtlinie übereinstimmen.

15 Fehlersuche

Wenn Sie den Assistenten zum Schutz von Computern starten, kann die Installation von Sicherheitssoftware aus mehreren Gründen nicht durchgeführt werden.

- Auf dem Betriebssystem ist eine automatische Installation nicht möglich. Führen Sie eine manuelle Installation durch. Mehr dazu erfahren Sie unter *Manueller Schutz von Windows- oder Mac OS X-Computern* (Seite 9). Nähere Anweisungen zu anderen Betriebssystemen können Sie der *Erweiterten Startup-Anleitung für Sophos Endpoint Security and Control* entnehmen.
- Das Betriebssystem konnte nicht ermittelt werden. Möglicherweise haben Sie beim Suchen nach Computern Ihren Benutzernamen nicht im Format „Domäne\Benutzername“ eingegeben.
- Die Computer werden von einer Firewall geschützt.

16 Hilfe für gängige Tasks

In der folgenden Tabelle sind Quellen aufgeführt, die weitere Informationen zu häufig vorkommenden Tasks enthalten.

SESC steht für Sophos Endpoint Security and Control

| Schritt | Dokument |
|---|--|
| Schützen von Linux-Systemen | SESC 9.7 Startup-Anleitung für Linux, NetWare und UNIX: „Schützen von Linux-Systemen“ |
| Schützen von Einzelplatzrechnern | SESC 9.7 Erweiterte Statup-Anleitung: „Schützen von Einzelplatzrechnern“ |
| Konfigurieren von Anti-Virus und HIPS | Enterprise Console Hilfe: „Konfigurieren der Antivirus- und HIPS-Richtlinie“ |
| Konfigurieren von Application Control | Enterprise Console Hilfe: „Konfigurieren der Application Control-Richtlinie“ |
| Konfigurieren von Data Control | Enterprise Console Hilfe: „Konfigurieren der Data Control-Richtlinie“ |
| Konfigurieren von Device Control | Enterprise Console Hilfe: „Konfigurieren der Device Control-Richtlinie“ |
| Konfigurieren des Manipulationsschutzes | Enterprise Console Hilfe: „Konfigurieren der Manipulationsschutz-Richtlinie“ |
| Konfigurieren von NAC | NAC Manager Hilfe: „Manage-Bereich im Überblick“ |
| Gewähren von Netzwerkzugriff für Gastbenutzer | Konfigurationsanleitung zu Sophos Compliance Agent: „Dissolvable Agent“ |
| Handhaben von Alerts | Enterprise Console Hilfe: „Benachrichtigungen, Alerts und Fehlermeldungen“ |
| Bereinigen von Computern | Enterprise Console Hilfe: „Bereinigen von Computern“ |
| Erstellen von SEC-Reports | Enterprise Console Hilfe: „Erstellen von Reports“ |
| Erstellen von NAC-Reports | NAC Manager Hilfe: „Report-Bereich im Überblick“ |

17 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.

18 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.

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.de or via the web at <http://www.sophos.de/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.