

SOPHOS

Sophos Endpoint Security and Control 9.5 Schnellstartanleitung

Stand: Juni 2010



Inhalt

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

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** zur Installation und Verwaltung von Sicherheitssoftware auf den Computern.
- **Sophos NAC Manager** als Voraussetzung für „Network Access Control“. 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 Installationsschritte

Die Installation besteht aus folgenden Schritten:

- 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 von Computern.
- Überprüfen der Netzwerkintegrität.

4 Systemvoraussetzungen

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

4.1 Hardware und Betriebssystem

Die Systemvoraussetzungen richten sich danach, welche Tools Sie installieren.

Bei den angegebenen Werten handelt es sich um Richtwerte. Es wird davon ausgegangen, dass Management-Tools auf einem Server installiert wurden und das Netzwerk bis zu 1000 Computer umfasst.

Internetzugang ist in jedem Fall erforderlich.

Hinweis: Die folgenden Voraussetzungen gelten nur für Server-Betriebssysteme. Eine ausführlichere Übersicht finden Sie unter <http://www.sophos.de/products/all-sysreqs.html>.

Enterprise Console

Prozessor	Speicherplatz	RAM	Betriebssystem
Pentium 2 GHz oder vergleichbarer Prozessor	Bis zu 2GB für Datenbanken	512 MB	Windows Server 2008 R2 Windows Server 2008 (32- oder 64-Bit) Windows Server 2008 Hyper-V Windows Server 2003 R2 Windows Server 2003 SP1+ (32- oder 64-Bit) VMWare ESX 3.0 oder 3.5 VMWare Workstation 6.5

Enterprise Console und NAC Manager

Prozessor	Speicherplatz	RAM	Betriebssystem
Pentium 2 GHz oder vergleichbarer Prozessor	Bis zu 3 GB für Datenbanken	1 GB	Windows Server 2008 R2 Windows Server 2008 (32- oder 62-Bit) Windows Server 2003 R2 Windows Server 2003 SP1+ (32- oder 64-Bit)

4.2 Microsoft Systemsoftware

Die folgende Microsoft Systemsoftware muss installiert werden, damit Enterprise Console ausgeführt werden kann:

- Microsoft Windows Installer, Version 4.5 mit Patch KB958655
- Sicherheits-Update für Microsoft XML Core Services 6.0
- Microsoft .NET Framework, Version 3.5 SP1
- Microsoft SQL Server 2005 Express

Wenn Sie nicht über diese (oder höhere) Microsoft Systemsoftwareversionen verfügen, sorgt der Enterprise Console-Installer für ihre Installation.

Hinweise

Der Installer installiert SQL Server 2008 Express, sofern Sie nicht bereits SQL Server 2005 Express oder höher nutzen. SQL Server 2008 Express ist nicht mit Windows Server 2003 SP1 oder Windows Essential Business Server 2008 kompatibel.

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.

Nach der Installation der erforderlichen Systemsoftware müssen die Computer eventuell neu gestartet werden. Im Sophos Support-Artikel 65190 (<http://www.sophos.de/support/knowledgebase/article/65190.html>) wird näher beschrieben, wann ein Neustart des Computers erforderlich ist.

5 Installationsvorbereitung

Gehen Sie zu einem Server, 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 Sie Microsoft SQL Server 2000 oder MSDE 2000 nutzen und die Datenbankinstanz nicht "SOPHOS" lautet, führen Sie ein Upgrade auf Microsoft SQL Server 2005 durch.

- 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 auf den Server herunter, auf denen 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 **Endpoint Security and Data Protection** wie folgt:
 - Laden Sie den Enterprise Console-Installer herunter.
 - Wenn Sie NAC Manager verwenden, laden Sie den Sophos NAC-Installer herunter.

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

7 Installieren von Enterprise Console

So installieren Sie Enterprise Console:

1. Melden Sie sich 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 beinhaltet "sec".
3. Doppelklicken Sie auf den Installer.
4. Klicken Sie im Dialogfeld **Sophos Endpoint Security and Control 9.5-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 Installieren 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 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 Sophos NAC-Installer, den Sie im Vorfeld heruntergeladen haben.

Tipp: Der Dateiname des Installers beinhaltet "nac".

3. Doppelklicken Sie auf den Installer.
4. Klicken Sie im Dialogfeld **Sophos NAC Manager** auf **Installieren**.
5. 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 8) auf.

Zunächst müssen Gruppen erstellt werden.

1. Öffnen Sie Enterprise Console.
2. Stellen Sie sicher, dass der Servername oben im Fensterbereich **Gruppen** (links in der Konsole) ausgewählt ist.
3. Klicken Sie in der Symbolleiste auf das Symbol **Gruppe erstellen**.

Es wird eine "Neue Gruppe" zur Liste hinzugefügt und ihr Name markiert.

4. 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. Die Firewall muss also konfiguriert werden, bevor Sie Ihre Computer schützen.

1. Doppelklicken Sie im Bereich **Richtlinien** auf **Firewall**.
2. Doppelklicken Sie auf die **Standardrichtlinie**, um sie zu ändern. Ein Assistent wird geöffnet.

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.
- Automatischer Schutz von Windows Computern.
- 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 **Tools** 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 11).
 - 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 **On-Access 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 zu diesem Thema erfahren Sie unter [Manueller Schutz von Windows- oder Mac OS X-Computern](#) (Seite 11). 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

Task	Dokument
Schützen von Linux-Systemen	SESC 9.5 Startup-Anleitung für Linux, NetWare und UNIX: „Schützen von Linux-Systemen“
Schützen von Einzelplatzrechnern	SESC 9.5 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

Bei Fragen zur Beta-Version können Sie sich an den technischen Support wenden:

1. Rufen Sie Ihr Online-Feedback-Formular auf (in der E-Mail mit den Downloadanweisungen von Sophos enthalten), füllen Sie die relevanten Details aus und senden Sie das Formular direkt an das Sophos Support-Team.
2. Rufen Sie das Sophos Beta-Forum auf (verwenden Sie dazu die Details in der E-Mail mit den Downloadanweisungen von Sophos) und suchen Sie nach anderen Beta-Teilnehmern, die vielleicht die gleichen Probleme haben.
3. Wenn dies nicht möglich ist, senden Sie bitte eine E-Mail an betaprogram@sophos.com und ein Mitarbeiter des Beta-Teams von Sophos wird sich bei Ihnen melden.

18 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.

The Sophos software that is described in this document includes or may include some software programs that are licensed (or sublicensed) to the user under the Common Public License (CPL), which, among other rights, permits the user to have access to the source code. The CPL requires for any software licensed under the terms of the CPL, which is distributed in object code form, that the source code for such software also be made available to the users of the object code form. For any such software covered under the CPL, the source code is available via mail order by submitting a request to Sophos; via email to support@sophos.com or via the web at <http://www.sophos.com/support/queries/enterprise.html>. A copy of the license agreement for any such included software can be found at <http://opensource.org/licenses/cpl1.0.php>