

**SOPHOS**

---

simple + secure

# Sophos Enterprise Manager Startup-Anleitung

Produktversion: 4.7  
Stand: August 2011



# Inhalt

1	Einleitung.....	3
2	Vorgehensweise.....	3
3	Systemvoraussetzungen.....	4
4	Installationsvorbereitung.....	5
5	Herunterladen des Installers.....	5
6	Installation von Enterprise Manager .....	5
7	Download von Sicherheitssoftware.....	6
8	Erstellen von Computergruppen.....	6
9	Einrichten von Sicherheitsrichtlinien.....	7
10	Suchen nach Computern.....	8
11	Schützen von Windows-Computern.....	9
12	Schützen von Mac OS X-Systemen.....	13
13	Schützen von Linux-Systemen.....	13
14	Überprüfen der Netzwerkintegrität.....	16
15	Fehlersuche.....	16
16	Hilfe für gängige Tasks.....	16
17	Anhang: Wechsel von Enterprise Console zu Enterprise Manager.....	17
18	Technischer Support.....	20
19	Rechtlicher Hinweis.....	20

# 1 Einleitung

In dieser Anleitung wird beschrieben, wie Sie Sophos Enterprise Manager, Version 4.7, installieren und Ihr Netzwerk mit Sophos Sicherheitssoftware schützen.

Bei Sophos Enterprise Manager handelt es sich um eine eigenständige, automatisierte Konsole, mit der Sophos Sicherheitssoftware unter Windows, Mac und Linux verwaltet und upgedatet wird. Enterprise Manager bietet folgende Funktionen:

- Schutz des Netzwerks vor Viren, Trojanern, Würmern, Spyware, schädlichen Websites, unbekanntem Threats, Adware und sonstigen potenziell unerwünschten Anwendungen.
- Verwalten des Client Firewall-Schutzes auf Endpoints.
- Verhindern, dass Benutzer nicht zugelassene externe Speichermedien und Wireless-Geräte auf Endpoints einsetzen.
- Verhindern, dass Benutzer Sophos Sicherheitssoftware umkonfigurieren, deaktivieren oder deinstallieren.

Der Sophos Support-Artikel 113711

(<http://www.sophos.de/support/knowledgebase/article/113711.html>) bietet eine Übersicht über die im Lizenzumfang von Enterprise Manager und anderer Sicherheitssoftware von Sophos enthaltenen Funktionen.

## Wechsel von Enterprise Console

Zudem wird die Deinstallation von Enterprise Console und Installation von Enterprise Manager ausgeführt.

**Wichtig:** Ein Downgrade von Enterprise Console auf Enterprise Manager ist nicht möglich. Sie müssen Enterprise Console anhand der Anweisungen in der vorliegenden Anleitung deinstallieren und Enterprise Manager installieren und einrichten.

Die Einstellungen von Enterprise Console gehen verloren.

Notieren Sie sich vor der Installation von Enterprise Console Ihre vorhandenen Einstellungen und sichern Sie die Enterprise Console-Datenbank anhand der Anweisungen im Abschnitt *Anhang: Wechsel von Enterprise Console zu Enterprise Manager* (Seite 17).

# 2 Vorgehensweise

Das Upgrade umfasst folgende Schritte:

- Überprüfen der Systemvoraussetzungen.
- Vorbereiten der Installation.
- Herunterladen des Installers.
- Installieren von Enterprise Manager.
- Download von Sicherheitssoftware.
- Erstellen von Computergruppen.

- Einrichten von Sicherheitsrichtlinien.
- Suchen nach Computern.
- Schützen der Computer.
- Überprüfen der Netzwerkintegrität.

## 3 Systemvoraussetzungen

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

### 3.1 Hardware und Betriebssystem

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

### 3.2 Microsoft Systemsoftware

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

Der Enterprise Manager-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. Nähere Informationen entnehmen Sie bitte den Sophos Support-Artikeln 65190 und 111220

(<http://www.sophos.de/support/knowledgebase/article/65190.html> und <http://www.sophos.de/support/knowledgebase/article/111220.html>).

## 4 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.

## 5 Herunterladen des Installers

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

1. Rufen Sie <http://www.sophos.de/support/updates/> auf.
2. Geben Sie Ihre MySophos-Zugangsdaten ein.
3. Laden Sie auf der Seite **Downloads und Updates** den Enterprise Manager-Installer herunter.
4. Kopieren Sie die heruntergeladenen Installer bei Bedarf auf den Server, auf dem die Installation durchgeführt werden soll.

## 6 Installation von Enterprise Manager

So installieren Sie Enterprise Manager:

1. Melden Sie sich auf dem Computer, auf dem Enterprise Manager installiert werden soll, 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 Installer zu Enterprise Manager, den Sie im Vorfeld heruntergeladen haben.
3. Doppelklicken Sie auf den Installer.
4. Klicken Sie im Dialogfeld des Netzwerk-Installers auf **Installieren**.

Die Installationsdateien werden auf den Computer kopiert und ein Installationsassistent öffnet sich.

5. Klicken Sie im Eröffnungsfenster des Installationsassistenten zu Sophos Enterprise Manager auf **Weiter**.
6. Es wird ein Assistent gestartet, der Sie durch die Installation leitet. Übernehmen Sie die Standardwerte, sofern dies möglich ist.
7. Nach der Installation ist eventuell ein Neustart erforderlich. Klicken Sie auf **Ja** oder **Fertigstellen**.

## 7 Download von Sicherheitssoftware

Wenn Sie sich nach der Installation zum ersten Mal wieder am System anmelden oder einen Neustart durchführen, wird Enterprise Manager 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 Sie auf der Seite **Plattform auswählen** die zu schützenden Plattformen aus.

Klicken Sie auf **Weiter**. Enterprise Manager 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 Manager Ihre vorhandenen Computergruppen aus Active Directory nutzen soll.

**Hinweis:** Wenn ein Computer zu mehreren Active Directory-Containern hinzugefügt wird, führt dies zu dem Problem, dass Nachrichten endlos zwischen dem Computer und Enterprise Manager gesendet werden.

Die ausgewählte Software wird in die Freigabe \\*Servername*\SophosUpdate heruntergeladen. Hierbei steht *Servername* für die Bezeichnung des Servers, auf dem Enterprise Manager installiert ist.

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

## 8 Erstellen von Computergruppen

Zunächst müssen Gruppen erstellt werden.

Gruppen bieten die folgenden Vorteile:

- Updaten von Computern in unterschiedlichen Gruppen von verschiedenen Quellen oder über verschiedene Zeitpläne.
- Einsatz unterschiedlicher Antivirus- und HIPS-, Firewall- oder sonstiger Richtlinien für die einzelnen Gruppen.
- Einfachere Computerverwaltung.

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

1. Öffnen Sie Enterprise Manager.
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, deren Name markiert ist.

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.

## 9 Einrichten von Sicherheitsrichtlinien

### Standardrichtlinien

Enterprise Manager übernimmt die Standardrichtlinien für Ihre Computergruppen. Sie müssen die Richtlinien nur unter folgenden Voraussetzungen ändern:

- Sie müssen eine Firewall-Richtlinie einrichten. Mehr dazu erfahren Sie unter [Einrichten einer Firewall-Richtlinie](#) (Seite 8).
- Wenn Sie Device Control oder den Manipulationsschutz nutzen möchten, müssen die entsprechenden Richtlinien manuell geändert werden. Dies können Sie jederzeit tun.

Nähere Informationen zur Aktivierung und Konfiguration von Device Control- und Manipulationsschutz-Richtlinien entnehmen Sie bitte den Abschnitten „*Konfigurieren der Device Control-Richtlinie*“ und „*Konfigurieren der Manipulationsschutzrichtlinie*“ in der *Hilfe* zu *Enterprise Manager*.

### Erstellen von neuen Richtlinien

In Enterprise Manager können Sie bis zu vier Richtlinien von jedem Typ erstellen. Wenn Sie die Höchstanzahl erreicht haben, sind die Optionen **Richtlinie erstellen** und **Richtlinie kopieren** deaktiviert.

So erstellen Sie eine neue Richtlinie:

1. Rechtsklicken Sie in der Ansicht **Endpoints** im Fensterbereich **Richtlinien** auf den Richtlinientyp, den Sie erstellen möchten (z.B. „Update-Richtlinie“), und wählen Sie **Richtlinie erstellen**.

Es wird eine „Neue Richtlinie“ zur Liste hinzugefügt und ihr Name markiert.

2. Geben Sie der Richtlinie einen neuen Namen.
3. Doppelklicken Sie auf die neue Richtlinie. Geben Sie die gewünschten Einstellungen ein.  
Anweisungen zur Auswahl der Einstellungen finden Sie im Abschnitt zum Konfigurieren der entsprechenden Richtlinie.

Die erstellte Richtlinie kann nun Gruppen zugewiesen werden.

### Übertragen von Richtlinien auf Gruppen

1. Markieren Sie im Fensterbereich **Richtlinien** die Richtlinie.
2. Klicken Sie auf die Richtlinie und ziehen Sie sie auf die Gruppe, auf die sie übertragen werden soll. Bestätigen Sie bei entsprechender Aufforderung, dass Sie den Vorgang fortsetzen möchten.

## 9.1 Einrichten einer Firewall-Richtlinie

Die Firewall ist standardmäßig aktiviert und sperrt unnötigen Datenverkehr. Daher sollten regelmäßig genutzte Anwendungen in der Firewall zugelassen werden. Testen Sie die Einstellungen vor der Installation. Weitere Hinweise dazu finden Sie in der *Sophos Enterprise Manager – Richtlinienanleitung*.

Die wichtigsten Firewall-Konfigurationseinstellungen können Sie im **Firewall-Richtlinien-Assistenten** einstellen.

1. Doppelklicken Sie im Bereich **Richtlinien** auf **Firewall**.
2. Doppelklicken Sie auf die **Standardrichtlinie**, um sie zu bearbeiten. 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.

## 10 Suchen nach Computern

Sie müssen zuerst eine Netzwerksuche nach Computern durchführen, bevor sie von Enterprise Manager geschützt und verwaltet werden können.

Wenn die Computergruppen bereits mit dem **Download-Assistenten für Sicherheitssoftware** auf der Grundlage von Active Directory-Gruppen strukturiert haben, können Sie diesen Abschnitt überspringen. Rufen Sie [Schützen von Windows-Computern](#) (Seite 9) auf.

1. Klicken Sie in der Symbolleiste auf das Symbol **Computer suchen**.
2. Wählen Sie die gewünschte Suchmethode aus.
  - Wenn Sie **Import aus Active Directory** auswählen und Computer und Container importieren, werden in Active Directory gefundene Computer in ihrer jeweiligen Gruppe gespeichert.
  - Wenn Sie eine der **Suchoptionen** verwenden, werden die Computer in der Gruppe **Nicht zugewiesen** abgelegt.
3. Melden Sie sich an und wählen Sie ggf. einen Netzwerkpfad für die Suche aus.
4. Wenn Sie eine **Suchoption** verwendet haben, klicken Sie auf die Gruppe **Nicht zugewiesen**, um die gefundenen Computer anzusehen. Um die Computer zu verwalten, ziehen Sie sie in eine Gruppe.

## 11 Schützen von Windows-Computern

Der Abschnitt bietet Anweisungen zum automatischen oder manuellen Schutz von Windows-Computern, wenn Computer nicht automatisch geschützt werden können.

### 11.1 Vorbereiten auf den automatischen Schutz von Windows-Computern

Treffen Sie zunächst folgende Vorbereitungen:

- Vorbereiten der Entfernung von Sicherheitssoftware anderer Hersteller
- Prüfen auf ein geeignetes Konto zur Installation von Software
- Vorbereiten der Installation der Virenschutzsoftware

#### 11.1.1 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 Manager finden Sie weitere Hinweise zu diesem Thema.

## 11.1.2 Prüfen auf ein geeignetes Konto zur Installation von Software

Beim automatischen Schützen von Computern werden Sie vom **Assistenten zum Schutz von Computern** zur Eingabe der Kontodaten für die Installation von Sicherheitssoftware aufgefordert. 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 Manager installiert ist.
- Lesezugriff auf das Update-Verzeichnis haben, von dem die Computer Updates beziehen.

Die Standard-Update-Quelle ist eine einzelne primäre UNC-Freigabe, \\<ComputerName>\SophosUpdate. Enterprise Manager ist dabei der Name des Computers mit Enterprise Manager. Doppelklicken Sie zum Überprüfen des Verzeichnisses im Fensterbereich **Richtlinien** auf **Update**. Doppelklicken Sie nun auf die zu prüfende Richtlinie.

## 11.1.3 Vorbereiten der Installation der Virenschutzsoftware

So bereiten Sie die Computer auf die Installation von Virenschutzsoftware vor: Die Schritte variieren je nach Betriebssystem.

**Hinweis:** Wenn ein Betriebssystem nicht aufgeführt wird, sind keine Vorbereitungen erforderlich.

### 11.1.3.1 Vorbereiten von Windows 7-Computern

So können Sie Windows 7-Computer auf die Installation von Virenschutzsoftware vorbereiten:

Als Alternative können Sie Windows 7-Computer in Active Directory in Windows 2008 und Windows 2008 R2 mit einem Gruppenrichtlinienobjekt (GPO) in vorbereiten. Siehe Support-Artikel 111180 (<http://www.sophos.de/support/knowledgebase/article/111180.html>) auf der Sophos Website.

1. Öffnen Sie in der Systemsteuerung das Netzwerk- und Freigabe-Center. Stellen Sie sicher, dass Sie für den Standort des **Firmennetzwerks** die folgenden Einstellungen vornehmen.

Netzwerkerkennung: Ein

Datei- und Druckerfreigabe: Ein

Dateifreigabeverbindungen: Aktivieren Sie die Dateifreigabe für Geräte mit 40- oder 56-Bit-Verschlüsselung

Kennwortgeschütztes Freigeben: Aus

2. Der Remote-Registrierungsdienst muss gestartet werden und der Starttyp „Automatisch“ lauten.
3. Wählen Sie für die Benutzerkontensteuerung die Option **Nie benachrichtigen** aus. Nach der Installation sollten Sie den **Standard** wiederherstellen.
4. Deaktivieren Sie den Freigabeassistenten.

5. Öffnen Sie die Windows-Firewall mit erweiterter Sicherheit. Öffnen Sie in der Systemsteuerung die **Verwaltung**.
  - a) Stellen Sie sicher, dass **Eingehende Verbindungen** zugelassen werden.
  - b) Lassen Sie unter **Eingehende Regeln** die folgenden Prozesse zu. Deaktivieren Sie nach der Installation die folgenden Prozesse wieder:
    - Remoteverwaltung (NP eingehend) Domäne
    - Remoteverwaltung (NP eingehend) Privat
    - Remoteverwaltung (RPC) Domäne
    - Remoteverwaltung (RPC) Privat
    - Remoteverwaltung (RPC-EPMAP) Domäne
    - Remoteverwaltung (RPC-EPMAP) Privat

### 11.1.3.2 Vorbereiten von Windows Vista-Computern

1. Öffnen Sie in der Systemsteuerung das Netzwerk- und Freigabe-Center. Nehmen Sie die folgenden Einstellungen vor:
  - Netzwerkerkennung: Ein
  - Dateifreigabe: Ein
  - Druckerfreigabe: Ein
  - Kennwortgeschütztes Freigeben: Aus
2. Der Remote-Registrierungsdienst muss gestartet werden und der Starttyp „Automatisch“ lauten.
3. Deaktivieren Sie die Benutzerkontensteuerung. Nach der Installation sollten Sie sie wieder aktivieren.
4. Deaktivieren Sie den Freigabeassistenten.
5. Öffnen Sie die Windows-Firewall mit erweiterter Sicherheit. Öffnen Sie in der Systemsteuerung die **Verwaltung**.
  - a) Stellen Sie sicher, dass **Eingehende Verbindungen** zugelassen werden.
  - b) Lassen Sie unter **Eingehende Regeln** die folgenden Prozesse zu. Deaktivieren Sie nach der Installation die folgenden Prozesse wieder:
    - Remoteverwaltung (NP eingehend) Domäne
    - Remoteverwaltung (NP eingehend) Privat
    - Remoteverwaltung (RPC) Domäne
    - Remoteverwaltung (RPC) Privat
    - Remoteverwaltung (RPC-EPMAP) Domäne
    - Remoteverwaltung (RPC-EPMAP) Privat

### 11.1.3.3 Vorbereiten von Windows 2003-/XP Pro-/2000-Computern:

1. Die Dienste „Remoteregistrierung“, „Server“, „Computerbrowser“ und „Taskplaner“ müssen laufen.
2. Die C\$-Admin-Freigabe muss aktiviert sein.
3. Die „Einfache Dateifreigabe“ muss deaktiviert sein (nur XP Pro).

### 11.1.3.4 Vorbereiten von Windows XP-Computern (SP2 und höher)

**Hinweis:** Anweisungen zu Windows XP Pro finden Sie im Abschnitt [Vorbereiten von Windows 2003-/XP Pro-/2000-Computern](#): (Seite 12).

1. Die Dienste „Remoteregistrierung“, „Server“, „Computerbrowser“ und „Taskplaner“ müssen laufen.
2. Die C\$-Admin-Freigabe muss aktiviert sein.
3. „Einfache Dateifreigabe“ muss deaktiviert sein.
4. Aktivieren Sie die Datei- und Druckerfreigabe für Microsoft-Netzwerke.
5. Die TCP-Ports 8192, 8193 und 8194 müssen geöffnet sein.
6. Die Änderungen werden erst nach einem Neustart des Computers wirksam.

## 11.2 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) Wählen Sie auf der Seite **Funktionsauswahl** die gewünschten optionalen Funktionen aus.

Die Virenschutzkomponente wird immer installiert.

Sophos Client Firewall wird auf Serverbetriebssystemen nicht unterstützt.

**Wichtig:** Stellen Sie sicher, dass die Firewall vor der Installation und Ausführung im Netzwerk alle Daten, Anwendungen und Prozesse zulässt, die nicht blockiert werden sollen. Mehr dazu erfahren Sie unter [Einrichten einer Firewall-Richtlinie](#) (Seite 8).

- b) Sehen Sie auf der Seite **Schutz-Übersicht** nach, ob Installationsprobleme aufgeführt werden. Hilfe erhalten Sie unter [Fehlersuche](#) (Seite 16).
- 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.

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

Wählen Sie zur Überprüfung des Schutzstatus der Computer die Gruppe aus, in der die Computer abgelegt wurden bzw. den Server oben zur Anzeige aller Computer. Wenn nach der Installation in der Computerliste in der Spalte **On-Access Aktiv** angezeigt wird, werden On-Access-Viren-Scans durchgeführt.

### 11.3 Manuelles Schützen von Windows-Systemen

Wenn Sie über Computer verfügen, die nicht automatisch geschützt werden können, schützen Sie sie durch Ausführen des Setups in der Freigabe, in die Sicherheitssoftware heruntergeladen wurde. Bei diesem Ordner handelt es sich um ein so genanntes „Bootstrap-Verzeichnis“.

1. So können Sie das Verzeichnis ermitteln, indem sich das Setup-Programm befindet: Öffnen Sie Enterprise Manager. Klicken Sie im Menü **Ansicht** auf **Bootstrap-Verzeichnisse**.

Im Dialogfeld **Bootstrap-Verzeichnisse** werden in der Spalte **Verzeichnis** die Bootstrap-Verzeichnisse für alle Plattformen angezeigt.

2. Melden Sie sich an jedem Computer mit lokalen Administratorrechten an.
3. Doppelklicken Sie im Bootstrap-Verzeichnis auf das Setup-Programm.  
Das Setup-Programm für Windows-Computer heißt „setup.exe“.
4. Es wird ein Assistent gestartet, der Sie durch die Installation leitet.

## 12 Schützen von Mac OS X-Systemen

Die automatische Installation ist unter Mac nicht möglich. Schützen Sie sie durch Ausführen des Setups in der Freigabe, in die Sicherheitssoftware heruntergeladen wurde. Bei diesem Ordner handelt es sich um ein so genanntes „Bootstrap-Verzeichnis“.

1. So können Sie das Verzeichnis ermitteln, indem sich das Setup-Programm befindet: Öffnen Sie Enterprise Manager. Klicken Sie im Menü **Ansicht** auf **Bootstrap-Verzeichnisse**.

Im Dialogfeld **Bootstrap-Verzeichnisse** werden in der Spalte **Verzeichnis** die Bootstrap-Verzeichnisse für alle Plattformen angezeigt.

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

## 13 Schützen von Linux-Systemen

Zum Schutz von Linux-Systemen sind folgende Schritte erforderlich:

- Erstellen eines Installationspakets.

- Installation von Sophos Anti-Virus auf Linux-Systemen.

## 13.1 Erstellen eines Installationspakets

In diesem Abschnitt wird davon ausgegangen, dass Sie bereits Sophos Anti-Virus anhand der Anweisungen im Abschnitt [Download von Sicherheitssoftware](#) (Seite 6) installiert haben.

Mithilfe des Skripts **mkinstpkg** können Sie ein Distributionspaket für Ihre Benutzer erstellen. Das Skript benötigt Informationen darüber, wie Sophos Anti-Virus auf Ihren Linux-Computern installiert wird. Die Antworten werden in das Installationspaket eingefügt. Wenn die Benutzer eine Installation über dieses Paket vornehmen, müssen Sie keinerlei Informationen bereitstellen, da Update-Speicherort und Zugangsdaten automatisch korrekt eingerichtet werden. Sie können ein Paket in Form eines tar-Archivs oder im RPM-Format erstellen.

**Hinweis:** Das Skript **mkinstpkg** ist nur für den unternehmensinternen Gebrauch bestimmt. Lesen Sie bitte den vom Skript **mkinstpkg** angezeigten Lizenzvertrag und den rechtlichen Hinweis.

So erstellen Sie ein Installationspaket:

1. Den Pfad zur Freigabe, in die Sophos Anti-Virus heruntergeladen wurde („Bootstrap-Verzeichnis“), können Sie wie folgt ermitteln:
  - a) Klicken Sie in Enterprise Manager im Menü **Ansicht** auf **Bootstrap-Verzeichnisse**.  
Im Dialogfeld **Bootstrap-Verzeichnisse** werden in der Spalte **Verzeichnis** die Bootstrap-Verzeichnisse für alle Plattformen angezeigt.
  - b) Notieren Sie sich die entsprechenden Pfade.
2. Melden Sie sich am Linux-Server als Root an.
3. Mounten Sie das Bootstrap-Verzeichnis.  
(Damit dieses Verzeichnis automatisch beim Systemstart gemountet werden kann, verwenden Sie dazu distributionsspezifische Tools oder bearbeiten Sie „fstab“.)
4. Ändern Sie das Bootstrap-Verzeichnis.
5. Um ein Installationspaket in Form eines tar-Archivs namens savinstpkg.tar.gz zu erstellen, geben Sie Folgendes ein:  
**./mkinstpkg.sh**  
Um ein Installationspaket im RPM-Format namens savinstpkg-0.0-1.i586.rpm zu erstellen, geben Sie Folgendes ein:  
**./mkinstpkg.sh -r**  
**Hinweis:** Der Dateiname wird vom RPM-Setup bestimmt und kann daher etwas anders aussehen.
6. Aktivieren Sie bei entsprechender Aufforderung Remote-Management.
7. Als Speicherort geben Sie das Bootstrap-Verzeichnis an (wie es von den Linux-Computern gesehen wird).

Jetzt können Sie Sophos Anti-Virus über das Installationspaket installieren.

## 13.2 Installation von Sophos Anti-Virus für Linux über das Installationspaket

Über das Installationspaket können Sie Sophos Anti-Virus anhand einer der folgenden Methoden installieren:

- Manuelle Installation auf allen Computern. Diese Methode ist über ein RPM-Paket oder ein tar-Archiv möglich.
- Automatische Installation im gesamten Netzwerk. Diese Methode ist nur über ein RPM-Paket möglich.

**Hinweis:** Unter Red Hat Enterprise Linux Version 6, 64-Bit, kann Sophos Anti-Virus nur installiert werden, wenn die folgenden Pakete vorhanden sind:

- glibc-2.11.1-1.i686
- nss-softokn-freebl i686 3.12.4-10.fc12

### 13.2.1 Manuelle Installation von Sophos Anti-Virus für Linux

1. Verwenden Sie Ihre eigenen Tools, um das Installationspaket auf die Computer zu kopieren, auf denen Sie Sophos Anti-Virus installieren möchten.
2. Gehen Sie zu jedem Computer und melden Sie sich als Root an.
3. Legen Sie das Installationspaket in einem temporären Verzeichnis ab und wechseln Sie zu diesem Verzeichnis.
4. Um eine Installation über das tar-Paket durchzuführen, geben Sie Folgendes ein:  
**tar -zxvf savinstpkg.tgz**  
**./sophos-av/install.sh**

Um eine Installation über das RPM-Paket durchzuführen, geben Sie Folgendes ein:

**rpm -i RPM-Paket**

Die erforderlichen Dateien werden vom Server kopiert und Sophos Anti-Virus wird installiert. Sophos Anti-Virus wird von nun an bei jedem Update des Bootstrap-Verzeichnisses automatisch upgedatet.

### 13.2.2 Automatische Installation von Sophos Anti-Virus für Linux

- ❖ Wenn Sophos Anti-Virus automatisch über das Installationspaket installiert werden soll, verwenden Sie ein Betriebssystem-Verwaltungstool, das die Remote-Installation unterstützt. Weitere Informationen entnehmen Sie bitte der entsprechenden Anleitung.

Nach der Installation wird Sophos Anti-Virus gestartet und automatisch bei jedem Update des Bootstrap-Verzeichnisses upgedatet.

## 14 Überprüfen der Netzwerkintegrität

Verfahren Sie wie folgt, um die Netzwerkintegrität von Enterprise Manager aus zu prüfen: 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.

## 15 Fehlersuche

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

- Die automatische Installation mit Enterprise Manager wird von Mac- und Linux-Computern nicht unterstützt. Nähere Informationen zum Schutz dieser Betriebssysteme finden Sie in den Abschnitten [Schützen von Mac OS X-Systemen](#) (Seite 13) und [Schützen von Linux-Systemen](#) (Seite 13).
- 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

Informationen zu häufig vorkommenden Tasks entnehmen Sie bitte den folgenden Abschnitten der *Enterprise Manager Hilfe*:

- *Konfigurieren von Richtlinien*
  - *Konfigurieren der Antivirus- und HIPS-Richtlinie*
  - *Konfigurieren der Firewall-Richtlinie*
  - *Konfigurieren der Device Control-Richtlinie*
  - *Konfigurieren der Manipulationsschutz-Richtlinie*
- *Schützen von Computern*
  - *Benachrichtigungen, Alerts und Fehlermeldungen*
  - *Bereinigen von Computern*
- *Erstellen von Reports*

Praxistipps zur Richtlinienerstellung entnehmen Sie bitte der *Sophos Enterprise Manager Richtlinienanleitung*.

## 17 Anhang: Wechsel von Enterprise Console zu Enterprise Manager

Wenn Sie Enterprise Console deinstallieren und Enterprise Manager installieren, gehen sämtliche Enterprise Console-Einstellungen verloren. Computer werden in die Gruppe **Nicht zugewiesen** verschoben und die Richtlinien werden auf Werkseinstellungen zurückgesetzt.

Notieren Sie sich die vorhandene Konfiguration. Dies kann Ihnen bei der Erstellung von Gruppen und Konfiguration von Richtlinien in Enterprise Manager behilflich sein.

Sie können die Firewall-Konfigurationseinstellungen von Enterprise Console 4.5 oder 4.7 exportieren und in Enterprise Manager importieren. Anweisungen hierzu entnehmen Sie bitte dem nächsten Abschnitt.

Wenn Sie Sophos NAC (Network Access Control) verwenden, müssen Sie es aus dem Netzwerk entfernen. Zudem empfiehlt sich, Data Control und Application Control vor der Deinstallation von Enterprise Console zu deaktivieren.

**Wichtig:** Sichern Sie vor der Deinstallation von Enterprise Console die Enterprise Console-Datenbank. Anweisungen hierzu entnehmen Sie bitte dem Abschnitt [Sichern der Enterprise Console-Datenbank](#) (Seite 19).

### 17.1 Exportieren/Importieren der Firewall-Konfigurationseinstellungen

Verfahren Sie zum Export der Firewall-Konfigurationseinstellungen von Enterprise Console und anschließendem Import in Enterprise Manager wie folgt:

1. Doppelklicken Sie in Enterprise Console im Feld **Richtlinien** auf **Firewall** und doppelklicken Sie anschließend auf die Richtlinie, die Sie exportieren möchten.
2. Klicken Sie auf der **Startseite** des **Firewall-Richtlinienassistenten** auf **Erweiterte Einstellungen**.
3. Klicken Sie im Dialogfeld **Firewall-Richtlinie** auf der Registerkarte **Allgemein** im Bereich **Konfiguration verwalten** auf **Exportieren**, um die Firewall-Einstellungen als Konfigurationsdatei (\*.conf) zu exportieren.
4. Wiederholen Sie die Schritte 1 bis 3 für alle Firewall-Richtlinien in Enterprise Console. (Enterprise Manager unterstützt maximal 5 Firewall-Richtlinien).
5. Doppelklicken Sie zum Import der Einstellungen in Enterprise Manager in Enterprise Manager im Dialogfeld **Richtlinien** auf **Firewall** und doppelklicken Sie dann auf die Richtlinie, für die die exportierte Konfiguration übernommen werden soll.
6. Klicken Sie auf der **Startseite** des **Firewall-Richtlinienassistenten** auf **Erweiterte Einstellungen**.
7. Klicken Sie im Dialogfeld **Firewall-Richtlinie** auf der Registerkarte **Allgemein** im Bereich **Konfiguration verwalten** auf **Importieren**, um die Firewall-Konfigurationseinstellungen zu importieren.

8. Wiederholen Sie die Schritte 5 bis 7 ggf. für weitere Firewall-Richtlinien in Enterprise Manager.

## 17.2 Entfernen von Sophos NAC

Wenn Sie Sophos NAC (Network Access Control) verwenden, müssen Sie es aus dem Netzwerk entfernen.

Sie müssen die Komponenten von Sophos NAC wie folgt entfernen:

- Entfernen von Sophos Compliance Agent von Endpoints.
- Entfernen von NAC Manager auf dem Server.
- Entfernen der NAC-Datenbanken vom Server.

**Hinweis:** Wenn die Komponenten nicht in der genannten Reihenfolge entfernt werden, werden unter Umständen Fehlermeldungen angezeigt.

### 17.2.1 Entfernen von Sophos Compliance Agent

Sie müssen Sophos Compliance Agent von allen Endpoints manuell entfernen.

**Hinweis:** Unter Umständen werden Sie dazu aufgefordert, vor dem Entfernen des Agenten Anwendungen zu schließen.

**Hinweis:** Nach der Entfernung des Agenten ist ein Neustart erforderlich.

1. Gehen Sie zu dem Endpoint.
2. Rufen Sie über das **Startmenü Systemsteuerung > Software** auf.
3. Wählen Sie **Sophos Network Access Control** und klicken Sie auf **Entfernen**.
4. Klicken Sie auf **Ja** zur Bestätigung.

### 17.2.2 Entfernen von NAC Manager

So entfernen Sie NAC Manager:

1. Gehen Sie zu dem Server, auf dem NAC Manager installiert wurde. Hierbei handelt es sich in der Regel um den Server, auf dem sich Enterprise Console befindet.
2. Rufen Sie über das **Startmenü Systemsteuerung > Software** auf.
3. Wählen Sie **Sophos NAC Application Server** und klicken Sie dann auf **Entfernen**.
4. Klicken Sie auf **Ja** zur Bestätigung.

NAC Manager wurde entfernt.

### 17.2.3 Entfernen der NAC-Datenbanken

**Hinweis:** Hierbei werden nur die Server-Dateien entfernt, mit denen die Datenbanken erstellt wurden, nicht jedoch die Datenbanken selbst.

Verfahren Sie auf dem Server, auf dem die NAC-Datenbanken installiert sind, wie folgt:

1. Rufen Sie über das **Startmenü Systemsteuerung > Software** auf.
2. Wählen Sie **Sophos NAC Databases** und klicken Sie dann auf **Entfernen**.
3. Klicken Sie auf **Ja** zur Bestätigung.

### 17.3 Sichern der Enterprise Console-Datenbank

Stellen Sie vor dem Upgrade sicher, dass Sie über ein gültiges, vollständiges Backup Ihrer Enterprise Console-Installation verfügen. Das System muss über dieses Backup wiederhergestellt werden können. Wenn Sie Enterprise Console zu einem späteren Zeitpunkt erneut installieren möchten, können Sie so Ihre Einstellungen wiederherstellen.

**Hinweis:** Das Standardverzeichnis der Datenbank lautet: C:\Programme\Microsoft SQL Server\MSSQL\$SOPHOS.

So legen Sie ein Backup der Enterprise Console-Datenbank an:

1. Gehen Sie zu dem Computer, auf dem der Enterprise Console-Management-Server installiert wurde.
2. Halten Sie die Dienste „Sophos Message Router“ und „Sophos Management Service“ an. Verfahren Sie hierzu wie folgt:
  - a) Klicken Sie auf **Start, Ausführen**, geben Sie **services.msc** ein und klicken Sie auf **OK**.
  - b) Rechtsklicken Sie im **Dienstefenster** auf den Namen des jeweiligen Diensts und klicken Sie auf **Anhalten**.
  - c) Schließen Sie das **Dienstefenster**.

So wird sichergestellt, dass neue Informationen während des Backup-Vorgangs nicht in die Datenbank aufgenommen werden.

3. Erstellen Sie einen Ordner für die Datenbanksicherung (z.B. C:\SophosBackups).
4. Öffnen Sie im Datenbankinstallationsverzeichnis von Enterprise Console eine Befehlszeile.  
Das Standardverzeichnis lautet C:\Programme\Sophos\Enterprise Console\DB.
5. Sichern Sie die Datenbank durch Eingabe eines Befehls in folgendem Format:  
**BackupDB C:\SophosBackups\SOPHOS.bak**

Wenn Ihre SQL Server-Instanz nicht „SOPHOS“ lautet, fügen Sie den Namen der SQL Server-Instanz hinzu, z.B.:

**BackupDB C:\SophosBackups\SOPHOS.bak MySQLServerInstance**

6. Exportieren Sie folgenden Registrierungsschlüssel:
  - 32-Bit-Betriebssysteme: HKLM\SOFTWARE\Sophos\Certification Manager
  - 64-Bit-Betriebssysteme:  
HKEY\_LOCAL\_MACHINE\Software\WOW6432Node\Sophos\Certification Manager

Jetzt kann Enterprise Console deinstalliert werden.

Nähere Informationen zum Wiederherstellen der Enterprise Console-Datenbank finden Sie unter *Fehlersuche* unten.

## 17.4 Fehlersuche

### Wiederherstellen der Enterprise Console-Daten

So können Sie die Installation von Enterprise Console auf den vorherigen Zustand zurücksetzen:

1. Setzen Sie die Datenbank auf die von Ihnen verwendete Instanz zurück. SOPHOS ist die Standardinstanz von SQL Server.
2. Stellen Sie den folgenden Registrierungsschlüssel wieder her:
  - 32-Bit-Betriebssysteme: HKLM\SOFTWARE\Sophos\Certification Manager
  - 64-Bit-Betriebssysteme:  
HKEY\_LOCAL\_MACHINE\Software\WOW6432Node\Sophos\Certification Manager

Bei weiteren Fragen wenden Sie sich bitte an den technischen Support von Sophos.

## 18 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.

## 19 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 Warenzeichen der Sophos Limited. Alle anderen erwähnten Produkt- und Unternehmensnamen sind Marken oder eingetragene Marken der jeweiligen Inhaber.

### ACE™, TAO™, CIAO™, and CoSMIC™

ACE<sup>1</sup>, TAO<sup>2</sup>, CIAO<sup>3</sup>, and CoSMIC<sup>4</sup> (henceforth referred to as “DOC software”) are copyrighted by Douglas C. Schmidt<sup>5</sup> and his research group<sup>6</sup> at Washington University<sup>7</sup>, University of California<sup>8</sup>, Irvine, and Vanderbilt University<sup>9</sup>, Copyright © 1993–2005, all rights reserved.

Since DOC software is open-source<sup>10</sup>, free software, you are free to use, modify, copy, and distribute—perpetually and irrevocably—the DOC software source code and object code produced from the source, as well as copy and distribute modified versions of this software. You must, however, include this copyright statement along with code built using DOC software.

You can use DOC software in commercial and/or binary software releases and are under no obligation to redistribute any of your source code that is built using DOC software. Note, however, that you may not do anything to the DOC software code, such as copyrighting it yourself or claiming authorship of the DOC software code, that will prevent DOC software from being distributed freely using an open-source development model. You needn't inform anyone that you're using DOC software in your software, though we encourage you to let us<sup>10</sup> know so we can promote your project in the DOC software success stories<sup>11</sup>.

DOC software is provided as is with no warranties of any kind, including the warranties of design, merchantability, and fitness for a particular purpose, noninfringement, or arising from a course of dealing, usage or trade practice. Moreover, DOC software is provided with no support and without any obligation on the part of Washington University, UC Irvine, Vanderbilt University, their employees, or students to assist in its use, correction, modification, or enhancement. A number of companies<sup>12</sup> around the world provide commercial support for DOC software, however. DOC software is Y2K-compliant, as long as the underlying OS platform is Y2K-compliant.

Washington University, UC Irvine, Vanderbilt University, their employees, and students shall have no liability with respect to the infringement of copyrights, trade secrets or any patents by DOC software or any part thereof. Moreover, in no event will Washington University, UC Irvine, or Vanderbilt University, their employees, or students be liable for any lost revenue or profits or other special, indirect and consequential damages.

The ACE<sup>13</sup>, TAO<sup>14</sup>, CIAO<sup>15</sup>, and CoSMIC<sup>16</sup> web sites are maintained by the DOC Group<sup>17</sup> at the Institute for Software Integrated Systems (ISIS)<sup>18</sup> and the Center for Distributed Object Computing of Washington University, St. Louis<sup>19</sup> for the development of open-source software as part of the open-source software community<sup>20</sup>. By submitting comments, suggestions, code, code snippets, techniques (including that of usage), and algorithms, submitters acknowledge that they have the right to do so, that any such submissions are given freely and unreservedly, and that they waive any claims to copyright or ownership. In addition, submitters acknowledge that any such submission might become part of the copyright maintained on the overall body of code, which comprises the DOC software. By making a submission, submitter agree to these terms. Furthermore, submitters acknowledge that the incorporation or modification of such submissions is entirely at the discretion of the moderators of the open-source DOC software projects or their designees.

The names ACE, TAO, CIAO, CoSMIC, Washington University, UC Irvine, and Vanderbilt University, may not be used to endorse or promote products or services derived from this source without express written permission from Washington University, UC Irvine, or Vanderbilt University. Further, products or services derived from this source may not be called ACE, TAO, CIAO, or CoSMIC nor may the name Washington University, UC Irvine, or Vanderbilt University appear in their names, without express written permission from Washington University, UC Irvine, and Vanderbilt University.

If you have any suggestions, additions, comments, or questions, please let me<sup>21</sup> know.

Douglas C. Schmidt<sup>22</sup>

## Quellen

1. <http://www.cs.wustl.edu/~schmidt/ACE.html>
2. <http://www.cs.wustl.edu/~schmidt/TAO.html>
3. <http://www.dre.vanderbilt.edu/CIAO/>
4. <http://www.dre.vanderbilt.edu/cosmic/>
5. <http://www.dre.vanderbilt.edu/~schmidt/>
6. <http://www.cs.wustl.edu/~schmidt/ACE-members.html>
7. <http://www.wustl.edu/>
8. <http://www.uci.edu/>
9. <http://www.vanderbilt.edu/>
10. [mailto:doc\\_group@cs.wustl.edu](mailto:doc_group@cs.wustl.edu)
11. <http://www.cs.wustl.edu/~schmidt/ACE-users.html>
12. <http://www.cs.wustl.edu/~schmidt/commercial-support.html>
13. <http://www.cs.wustl.edu/~schmidt/ACE.html>
14. <http://www.cs.wustl.edu/~schmidt/TAO.html>
15. <http://www.dre.vanderbilt.edu/CIAO/>
16. <http://www.dre.vanderbilt.edu/cosmic/>
17. <http://www.dre.vanderbilt.edu/>
18. <http://www.isis.vanderbilt.edu/>
19. <http://www.cs.wustl.edu/~schmidt/doc-center.html>
20. <http://www.opensource.org/>
21. <mailto:d.schmidt@vanderbilt.edu>
22. <http://www.dre.vanderbilt.edu/~schmidt/>

## Apache

The Sophos software that is described in this document may include some software programs that are licensed (or sublicensed) to the user under the Apache License. A copy of the license agreement for any such included software can be found at <http://www.apache.org/licenses/LICENSE-2.0>.

## 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.

### **iMatix SFL**

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

### **OpenSSL cryptographic toolkit**

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact [openssl-core@openssl.org](mailto:openssl-core@openssl.org).

### **OpenSSL license**

Copyright © 1998-2011 The OpenSSL Project. Alle Rechte vorbehalten.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

“This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)”

4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact [openssl-core@openssl.org](mailto:openssl-core@openssl.org).
5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

“This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)”

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,

EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).  
This product includes software written by Tim Hudson (tjh@cryptsoft.com).

### **Original SSLeay license**

Copyright © 1995–1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscape's SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

“This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)”

The word “cryptographic” can be left out if the routines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

“This product includes software written by Tim Hudson (tjh@cryptsoft.com)”

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS

INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License.]