

SOPHOS

Sophos Endpoint Security and Control 9 Erweiterte Startup-Anleitung

Stand: Dezember 2009



Inhalt

1	Einleitung.....	3
2	Planen der Installation.....	4
3	Systemvoraussetzungen.....	9
4	Planen der Installation der Management-Tools.....	10
5	Installieren der Management-Tools – Datenbanken auf separatem Server.....	14
6	Installieren der Management-Tools – zusätzlicher Update Manager auf separatem Server.....	26
7	Freigeben von Sicherheitssoftware in einem Webserver.....	42
8	Erstellen von Computergruppen.....	43
9	Einrichten von Sicherheitsrichtlinien.....	44
10	Suchen nach Computern.....	47
11	Schützen von Windows- und Macintosh-Systemen.....	48
12	Schützen von Linux-Systemen.....	53
13	Schützen von NetWare-Servern.....	55
14	Schutz von UNIX-Systemen.....	57
15	Schützen von UNIX-Systemen mit Sophos Anti-Virus 4.....	58
16	Schützen von UNIX-Systemen mit Sophos Anti-Virus 7.....	60
17	Überprüfen der Netzwerkintegrität.....	64
18	Schützen von Einzelplatzrechnern.....	65
19	Technischer Support.....	66
20	Copyright.....	67

1 Einleitung

In dieser Anleitung wird die Installation von Sophos Endpoint Security and Control in komplexen Netzwerken (oder Netzwerken mit mindestens 1000 Computern) beschrieben. Es werden die Betriebssysteme Windows, Mac OS X, Linux, NetWare und UNIX abgedeckt.

Zur Installation in Netzwerken mit weniger als 1000 PCs und Macintosh-Computern lesen Sie bitte die *Sophos Endpoint Security and Control Schnellstartanleitung*.

Upgrades werden in der *Sophos Endpoint Security and Control Upgrade-Kurzanleitung* und in der *Sophos Endpoint Security and Control Erweiterte Upgrade-Anleitung* beschrieben.

Sophos Begleitmaterial ist auf <http://www.sophos.de/support/docs/> und auf den Sophos CDs erhältlich.

2 Planen der Installation

Zum Schutz Ihrer Computer sind folgende Schritte erforderlich:

1. Installieren der Sophos Management-Tools
2. Bereitstellen von Sicherheitssoftware auf einem Webserver (falls erwünscht)
3. Erstellen von Gruppen für Computer
4. Einrichten von Sicherheitsrichtlinien für diese Gruppen
5. Suchen von Computern im Netzwerk und Einordnen in Gruppen
6. Schützen von Computern
7. Überprüfen der Netzwerkintegrität
8. Schützen von Einzelplatzrechnern

Hinweis: Wenn Sie Active Directory verwenden, können einige Schritte automatisiert werden.

Dieser Abschnitt hilft Ihnen bei den Auswahlmöglichkeiten bei jedem Schritt.

2.1 Planen der Installation von Management-Tools

Die Sophos Management-Tools umfassen:

- **Sophos Enterprise Console** zur Installation und Verwaltung von Sicherheitssoftware auf den Computern.
- **Sophos NAC-Server** 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.

Wichtig: Es wird empfohlen, dass sich die Server, auf denen Enterprise Console installiert wird, in der gleichen Active Directory-Gesamtstruktur befinden wie die Installation von NAC-Server.

2.1.1 Planen der Installation von Sophos Enterprise Console

Sophos Enterprise Console besteht aus vier Komponenten:

Management-Konsole	Schutz und Verwaltung von Computern.
Management-Server	Verwaltung von Updates und Abwicklung des Datenverkehrs.
Datenbank	Verwaltung der Informationen zu allen Computern im Netzwerk.
Update Manager	Automatische Downloads von Sophos Software und Updates von der Sophos Website in ein zentrales Verzeichnis.

Wichtig: Wenn die Komponenten auf unterschiedlichen Servern installiert werden, sollten die Server der gleichen Domäne angehören.

Management-Konsole

Zur einfacheren Verwaltung der Netzwerkcomputer empfiehlt sich ggf. die Installation einer weiteren Management-Konsole auf einem anderen Server. Dies hängt von Ihrer Konfiguration des rollenbasierten Zugriffs auf die Management-Konsole und von der Untergliederung Ihrer IT-Verwaltungseinheit in Teilverwaltungseinheiten ab:

- *Rollenbasierter Zugriff* auf die Management-Konsole setzt das Einrichten von Rollen, Zuweisen von Rechten und Windows-Benutzern und -Gruppen zu den Rollen voraus. Zum Beispiel kann ein Helpdesk-Techniker Computer updaten und bereinigen, jedoch keine Richtlinien konfigurieren, da dies die Aufgabe eines Administrators ist.
- *Teilverwaltungseinheiten* dienen der Einschränkung von Computern und Gruppen, auf denen Benutzer bestimmte Vorgänge ausführen können. Sie können Ihre IT-Verwaltungseinheit in Teilverwaltungseinheiten untergliedern und ihnen Management-Konsolengruppen von Computern zuweisen. Daraufhin lässt sich durch Zuweisung von Windows-Benutzern und -Gruppen der Zugriff auf die Teilverwaltungseinheiten regeln. Die Standardteilverwaltungseinheit enthält alle Management-Konsolengruppen und die Gruppe **Nicht zugewiesen**.

In dieser Anleitung wird die Installation einer zusätzlichen Management-Konsole beschrieben. Anweisungen zum Einrichten von rollenbasiertem Zugang und der Erstellung von Teilverwaltungseinheiten finden Sie unter <http://www.sophos.de/support/bestpractice/esc>.

Datenbank

In folgenden Fällen empfiehlt sich die Installation der Datenbank auf einem anderen Server:

- Es wird mehr Speicherplatz für die Datenbank benötigt.
- Sie verfügen über einen dedizierten SQL Server.
- Die Rechenlast soll auf mehrere Server verteilt werden.

In dieser Anleitung wird die Installation der Enterprise Console-Datenbank entweder auf dem Server mit den anderen Enterprise Console-Komponenten oder auf dem Server mit den NAC-Datenbanken beschrieben.

Update Manager

Ein Update Manager ermöglicht die Erstellung von Freigaben, in denen die Software für die Installation auf anderen Computern bereitsteht. Die in den Schutz eingebundenen Computer beziehen ihre Updates direkt aus diesen Freigaben. Ein Update Manager wird immer zusammen mit Enterprise Console installiert. Sie können jedoch auch weitere Update Manager auf anderen Servern installieren und weitere Freigaben für Software-Downloads einrichten. Dies empfiehlt sich besonders bei komplexen Netzwerken. In dieser Anleitung wird die Installation eines zusätzlichen Update Managers und die Erstellung von Freigaben beschrieben. Anweisungen zur Organisation von Update Managern und Freigaben in größeren Netzwerken finden Sie unter <http://www.sophos.de/support/bestpractice/esc>.

2.1.2 Planen der Installation von Sophos NAC Server

Wenn Sie Sophos Network Access Control (NAC) nutzen möchten, müssen Sie Sophos NAC-Server installieren. Diese Software besteht aus zwei Komponenten:

Sophos NAC Manager	Handhabung und Konfiguration von NAC im Netzwerk.
Sophos NAC Datenbanken	Speicherung von NAC-Netzwerkdaten, die sich über NAC Manager einsehen lassen.

Wichtig: Wenn die Komponenten auf unterschiedlichen Servern installiert werden, müssen die Server der gleichen Domäne angehören.

In folgenden Fällen empfiehlt sich die Installation der Datenbanken auf einem anderen Computer:

- Es wird mehr Speicherplatz für die Datenbanken benötigt.
- Sie verfügen über einen dedizierten SQL Server.
- Die Rechenlast soll auf mehrere Computer verteilt werden.

In der folgenden Tabelle sind die empfohlenen Datenbankgrößen in Relation zur Anzahl der Computer aufgelistet:

Anzahl der Computer	Richtwert für die ReportStore-Datenbankgröße
1500	300 MB
3000	379 MB
5000	485 MB
7500	616 MB
10000	748 MB
15000	1011 MB
20000	1274 MB
25000	1536 MB

Anzahl der Computer	Richtwert für die ReportStore-Protokollgröße
1500	150 MB
3000	206 MB
5000	281 MB
7500	374 MB
10000	467 MB
15000	653 MB
20000	839 MB
25000	1024 MB

In dieser Anleitung wird die Installation der NAC-Datenbanken entweder auf dem Server mit NAC Manager oder auf dem Server mit der Enterprise Console-Datenbank beschrieben.

NAC ermöglicht die Datenübertragung zwischen NAC-Server und Sophos Compliance Agent über HTTPS. Compliance Agent wird auf Computern installiert und unterzieht sie einer Konformitätsprüfung. Der technische Support von Sophos kann Ihnen bei der Aktivierung von HTTPS mit NAC behilflich sein. Im Abschnitt *Technischer Support* (Seite 66) wird erläutert, wie Sie Kontakt zum technischen Support aufnehmen können. Dies muss vor der Installation geschehen.

2.2 Planen der Computergruppen

Überlegen Sie sich, wie die zu schützenden Computer gruppiert werden sollen. Nähere Anweisungen finden Sie unter <http://www.sophos.de/support/bestpractice/esc>.

2.3 Planen der Sicherheitsrichtlinien

Eine *Sicherheitsrichtlinie* besteht aus mehreren Einstellungen, die auf die Computer in einer Gruppe oder Gruppen übertragen werden können.

Bei der Erstellung einer Gruppe werden von Enterprise Console Standardrichtlinien auf sie übertragen. Die Richtlinien lassen sich jederzeit ändern. Sie können auch neue Richtlinien erstellen. Dies wird an anderer Stelle beschrieben. Die Einstellungen werden in der *Richtlinienanleitung zu Sophos Endpoint Security and Control* ausführlich beschrieben.

2.4 Planen der Suche von Computern im Netzwerk

Bevor Sie die Sicherheitssoftware auf Computern im Netzwerk installieren können, müssen die Computer zunächst der Computerliste von Enterprise Console hinzugefügt werden. Näheres zur Computersuche erfahren Sie in der Hilfe zu Enterprise Console.

2.5 Planen der Softwareinstallation

Auf den folgenden Betriebssystemen kann Sicherheitssoftware automatisch über die Konsole auf den folgenden Betriebssystemen installiert werden:

- Windows 2000 und aufwärts
- Windows NT

Hinweis: Sophos Client Firewall oder Sophos Compliance Agent kann nicht auf Computern mit Server-Betriebssystem installiert werden.

Wenn in Ihrem Netzwerk andere Betriebssysteme vorkommen, müssen Sie die Software manuell oder mithilfe von Skripten oder einer anderen Methode installieren (z.B. Active Directory). In dieser Anleitung wird die manuelle Installation auf folgenden Betriebssystemen beschrieben:

- Windows
- Mac OS X

- Linux
- NetWare
- UNIX

3 Systemvoraussetzungen

Die Systemanforderungen entnehmen Sie bitte der Sophos Website:
<http://www.sophos.de/products/all-sysreqs.html>.

Zum Herunterladen der Software von der Sophos Website ist eine Internetverbindung erforderlich.

4 Planen der Installation der Management-Tools

Die Sophos Management-Tools umfassen Sophos Enterprise Console und Sophos NAC-Server.

Sophos Enterprise Console besteht aus vier Komponenten:

Management-Konsole	Schutz und Verwaltung von Computern.
Management-Server	Verwaltung von Updates und Abwicklung des Datenverkehrs.
Datenbank	Verwaltung der Informationen zu allen Computern im Netzwerk.
Update Manager	Automatische Downloads von Sophos Software und Updates von der Sophos Website in ein zentrales Verzeichnis.

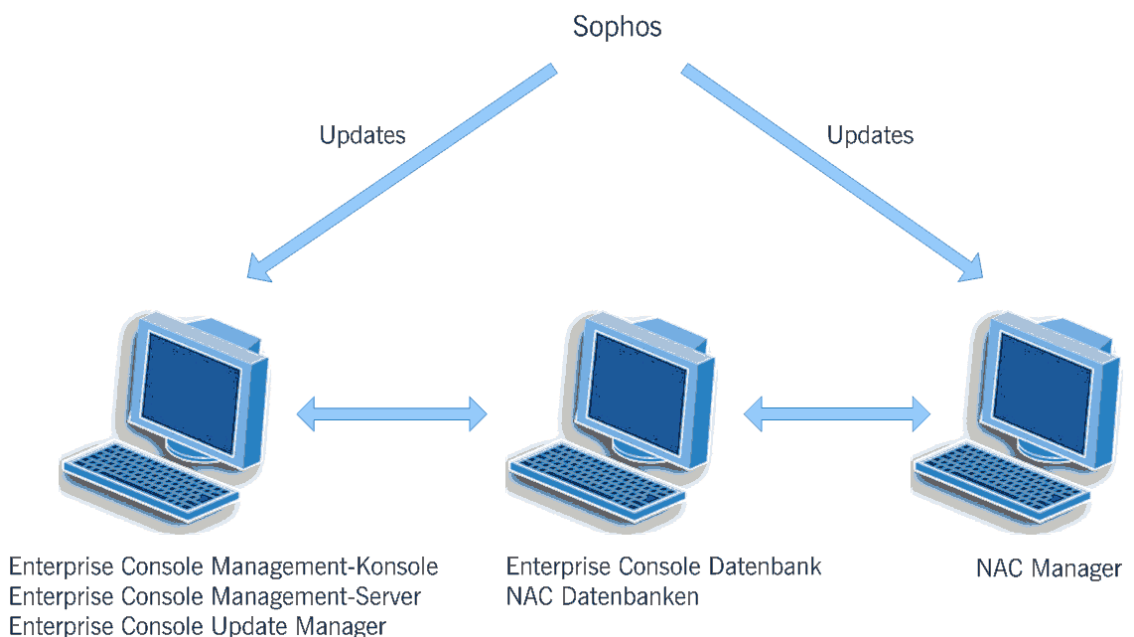
Sophos NAC-Server besteht aus zwei Komponenten:

Sophos NAC Manager	Handhabung und Konfiguration von NAC im Netzwerk.
Sophos NAC Datenbanken	Speicherung von NAC-Netzwerkdaten, die sich über NAC Manager einsehen lassen.

Hinweis: Wenn Sie Network Access Control nicht benötigen, brauchen Sie diese Komponenten nicht zu installieren.

Im Folgenden werden zwei Installationsszenarien beschrieben. In jedem Szenario werden die Komponenten der Management-Tools auf andere Weise im Netzwerk installiert.

Datenbanken auf separatem Server



Hinweis: Die Server, auf denen die NAC-Datenbanken und NAC Manager installiert werden, müssen derselben Domäne angehören.

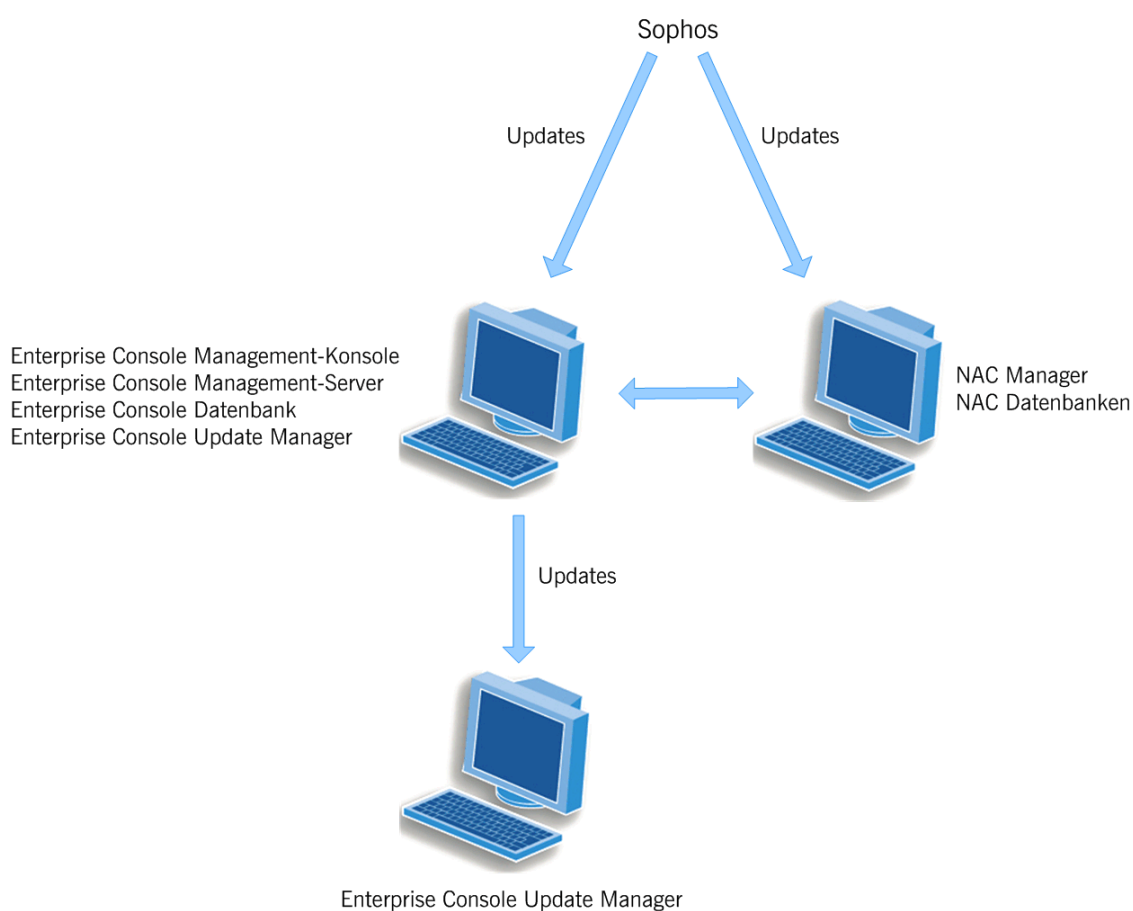
Dieses Szenario wird ausführlich im Abschnitt *Installieren der Management-Tools – Datenbanken auf separatem Server* (Seite 14) beschrieben.

Zusätzlicher Update Manager auf separatem Server

In diesem Szenario lassen sich die Update-Quellen der Update Manager auf zweierlei Weise konfigurieren.

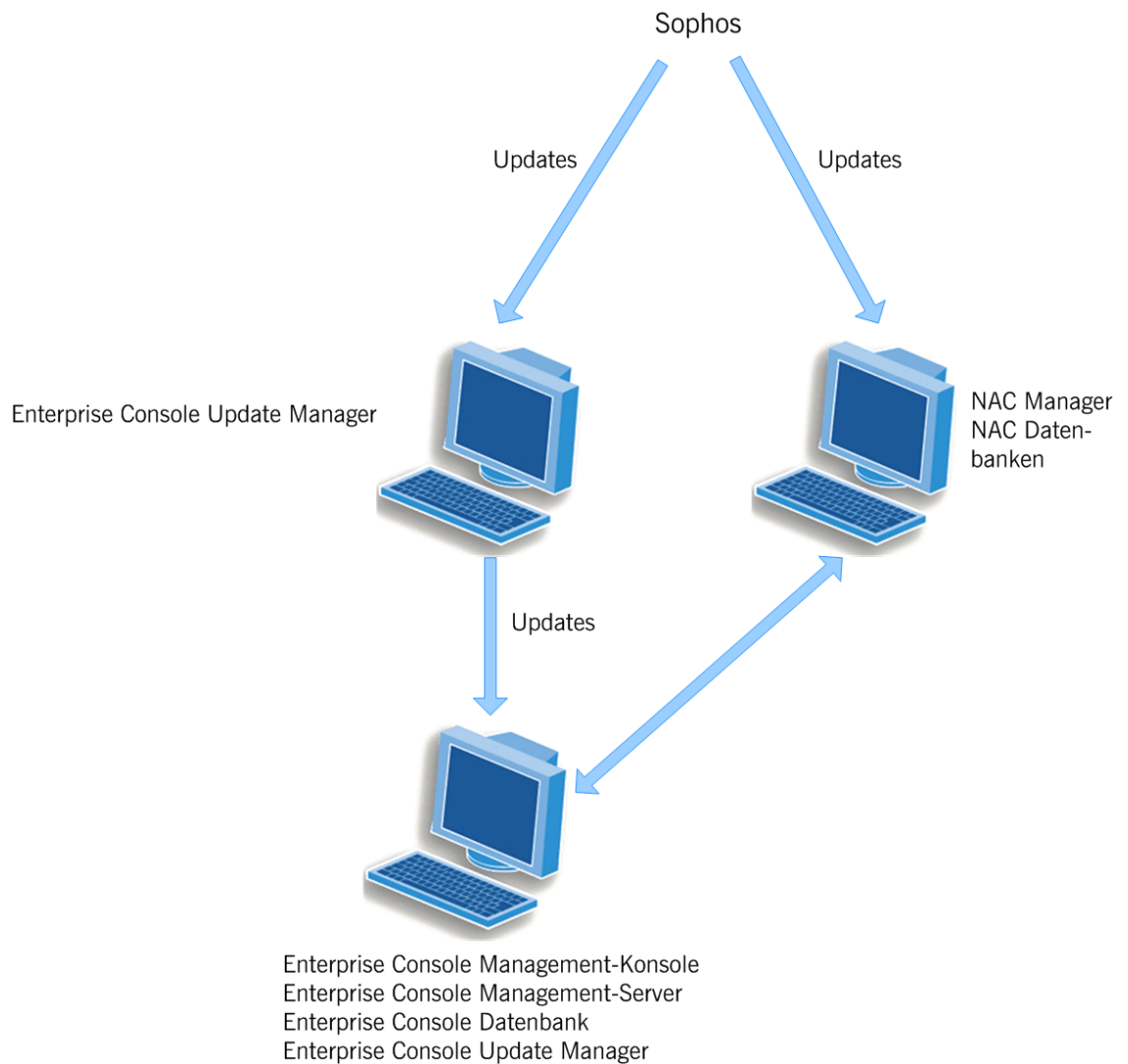
1. Methode:

- Konfigurieren des primären Update Managers, den Sie zusammen mit der Management-Konsole installiert haben, für direkte Updates von der Sophos Website
- Konfigurieren des zusätzlichen Update Managers für Updates vom primären Update Manager



2. Methode:

- Konfigurieren des zusätzlichen Update Managers für direkte Updates von der Sophos Website
- Konfigurieren des Update Managers, den Sie zusammen mit der Management-Konsole installiert haben, für Updates vom zusätzlichen Update Manager



Nähere Anweisungen zu beiden Methoden finden Sie unter [Installieren der Management-Tools – zusätzlicher Update Manager auf separatem Server](#) (Seite 26).

5 Installieren der Management-Tools – Datenbanken auf separatem Server

5.1 Herunterladen der Installer

1. Rufen Sie <http://www.sophos.de/support/updates/> auf.
2. Geben Sie Ihre MySophos-Zugangsdaten ein.
3. Laden Sie von der Website für Endpoint Security and Control-Downloads den Enterprise Console-Installer herunter.
4. Laden Sie den NAC Manager-Installer herunter.
5. Laden Sie den Sophos Compliance Dissolvable Agent-Installer herunter.
6. Stellen Sie sicher, dass die Server, auf denen die Software installiert werden soll, auf das Download-Verzeichnis zugreifen können.
Sie können die Installer auch auf eine CD oder DVD brennen.

5.2 Installieren von Enterprise Console: Datenbank

Gehen Sie zu dem Server, auf dem die Enterprise Console-Datenbank und die NAC-Datenbanken installiert werden sollen.

Wenn der Server unter *Windows Server 2008* betrieben wird, deaktivieren Sie die Benutzerkontensteuerung und starten Sie den Server neu. Nach der Installation von Enterprise Console und der Anmeldung für die Sophos Updates können Sie die Benutzerkontensteuerung wieder einschalten.

Wenn der Server unter *Windows 2000* betrieben wird, muss er nach der Installation neu gestartet werden.

Wenn der Server einer *Domäne* angehört, melden Sie sich als Domänenadministrator an.

Wenn der Server einer *Arbeitsgruppe* angehört, melden Sie sich als lokaler Administrator an.

1. Doppelklicken Sie auf den Enterprise Console-Installer, den Sie vorher heruntergeladen haben.

Ein Installationsassistent wird gestartet.

2. Klicken Sie im Dialogfeld **Sophos Network Installer** auf **Installieren**.

Es wird ein Assistent gestartet, der Sie durch die Installation leitet. Übernehmen Sie unter Beachtung der folgenden Ausnahmen die Voreinstellungen:

Klicken Sie auf der Seite **Setup-Typ** auf **Benutzerdefiniert**.

Wählen Sie auf der Seite **Benutzerdefiniertes Setup** die Option **Datenbank**. Die Optionen **Management-Konsole** und **Management-Server** dürfen nicht ausgewählt sein.

Nach Abschluss der Installation teilt Ihnen der Assistent mit, ob Sie sich abmelden oder den Server neu starten müssen.

5.3 Installieren von Enterprise Console: Management-Konsole, Management-Server, Update Manager

Gehen Sie zu dem Server, auf dem die Management-Konsole, der Management-Server und der Update Manager von Enterprise Console installiert werden sollen. Der Server muss mit dem Internet verbunden sein.

Öffnen Sie zur Ermöglichung der Kommunikation der Management-Konsole mit den verwalteten Arbeitsstationen die Ports 8192 und 8194 auf dem Server. Öffnen Sie Port 80 auf dem Server, damit der Update Manager Sicherheitssoftware von Sophos herunterladen kann.

Wenn der Server unter *Windows Server 2008* betrieben wird, deaktivieren Sie die Benutzerkontensteuerung und starten Sie den Server neu. Nach der Installation von Enterprise Console und der Anmeldung für die Sophos Updates können Sie die Benutzerkontensteuerung wieder einschalten.

Wenn der Server unter *Windows 2000* betrieben wird, muss er nach der Installation neu gestartet werden.

Wenn der Server einer *Domäne* angehört, melden Sie sich als Domänenadministrator an.

Wenn der Server einer *Arbeitsgruppe* angehört, melden Sie sich als lokaler Administrator an.

1. Doppelklicken Sie auf den Enterprise Console-Installer, den Sie vorher heruntergeladen haben.

Ein Installationsassistent wird gestartet.

2. Klicken Sie im Dialogfeld **Sophos Network Installer** auf **Installieren**.

Es wird ein Assistent gestartet, der Sie durch die Installation leitet. Übernehmen Sie unter Beachtung der folgenden Ausnahmen die Voreinstellungen:

Klicken Sie auf der Seite **Setup-Typ** auf **Benutzerdefiniert**.

Wählen Sie auf der Seite **Benutzerdefiniertes Setup** die Option **Management-Konsole** und **Management-Server**. Die Option **Datenbank** darf nicht ausgewählt sein.

Geben Sie auf der Seite **Datenbank-Details** das Verzeichnis und den Namen der Enterprise Console-Datenbank an, die Sie auf dem anderen Server angelegt haben.

Nach der Installation teilt Ihnen der Assistent mit, ob Sie sich abmelden oder den Server neu starten müssen. Wenn Sie sich erneut anmelden, wird Enterprise Console automatisch geöffnet. Der Assistent zum Herunterladen von Sicherheitssoftware wird ausgeführt. Brechen Sie den Assistenten ab. Er wird erst später benötigt.

5.4 Installieren einer zusätzlichen Management-Konsole

Zur einfacheren Verwaltung der Netzwerkcomputer empfiehlt sich ggf. die Installation einer weiteren Management-Konsole auf einem anderen Server. Wenn Sie zu diesem Zeitpunkt keine weitere Management-Konsole installieren möchten, können Sie diesen Abschnitt überspringen.

Wenn der Server unter *Windows Server 2008* betrieben wird, deaktivieren Sie die Benutzerkontensteuerung und starten Sie den Server neu. Nach der Installation der Management-Konsole können Sie die Benutzerkontensteuerung wieder aktivieren.

Wenn der Server unter *Windows 2000* betrieben wird, muss er nach der Installation neu gestartet werden.

Wenn der Server einer *Domäne* angehört, melden Sie sich als Domänenadministrator an.

Wenn der Server einer *Arbeitsgruppe* angehört, melden Sie sich als lokaler Administrator an.

1. Doppelklicken Sie auf den Enterprise Console-Installer, den Sie vorher heruntergeladen haben.

Ein Installationsassistent wird gestartet.

2. Klicken Sie im Dialogfeld **Sophos Network Installer** auf **Installieren**.

Es wird ein Assistent gestartet, der Sie durch die Installation leitet. Übernehmen Sie unter Beachtung der folgenden Ausnahmen die Voreinstellungen:

Klicken Sie auf der Seite **Setup-Typ** auf **Benutzerdefiniert**.

Wählen Sie auf der Seite **Benutzerdefiniertes Setup** die Option **Management-Konsole**. Die Optionen **Management-Server** und **Datenbank** dürfen nicht ausgewählt sein.

Geben Sie auf der Seite **Management-Server** den Namen des Servers ein, auf dem der Management-Server installiert wurde.

Nach der Installation teilt Ihnen der Assistent mit, ob Sie sich abmelden oder den Server neu starten müssen. Bei der nächsten Anmeldung wird Enterprise Console automatisch gestartet. Brechen Sie den Software-Download-Assistenten ggf. ab.

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

So können Sie anderen Benutzern den Zugriff auf eine weitere Management-Konsole gewähren:

- Fügen Sie die Benutzer zu den Gruppen **Sophos Console Administrators** und **Distributed COM-Benutzer** auf dem Server hinzu, auf dem der Management-Server installiert ist.
- Weisen Sie die Benutzer mindestens einer Rolle und Teilverwaltungseinheit in Enterprise Console zu.

Wenn Sie anderen Benutzern die Reporterstellung erlauben möchten, fügen Sie sie zur Gruppe **Sophos DB Users** auf dem Server hinzu, auf dem die Enterprise Console-Datenbank installiert ist.

5.5 Installieren der NAC-Datenbanken

Stellen Sie vor der Installation der NAC-Datenbanken sicher, dass die richtige Version von SQL Server installiert wurde.

- Bei bis zu 1500 Arbeitsstationen werden SQL Server MSDE, SQL Server 2005 Express oder SQL Server 2008 Express empfohlen. SQL Server MSDE-Datenbanken dürfen maximal 2 GB und 2005/2008 Express-Datenbanken maximal 4 GB umfassen.

- Für mehr als 1500 Arbeitsstationen eignen sich besonders SQL Server 2000, 2005 oder 2008.

Der NAC-Installationsassistent leitet Sie durch die Installation der erforderlichen Komponenten. Halten Sie bei der NAC-Installation die CD des Betriebssystems bereit, da sich einige erforderliche Komponenten darauf befinden. Die übrigen Komponenten werden automatisch vom NAC-Installationsassistenten installiert.

1. Sie müssen auf dem Domain Controller manuell ein Standard-Domänenkonto erstellen und festlegen, dass das Kennwort nie abläuft und es nicht durch den Benutzer geändert werden kann.

Der NAC-Installationsassistent fügt dieses Dienstkonto der lokalen Administratorgruppe auf dem NAC Manager-Server hinzu, wodurch NAC Manager Zugriff auf die NAC-Datenbanken erhält.

2. Gehen Sie zu dem Server, auf dem die Enterprise Console-Datenbank installiert wurde.
3. Doppelklicken Sie auf den NAC-Installer, den Sie vorher heruntergeladen haben.

Ein Installationsassistent wird gestartet.

4. Klicken Sie auf **Installieren**.
5. Klicken Sie im Eröffnungsfenster auf **Weiter**.
6. Klicken Sie auf der Seite **Funktionen auswählen** auf **Erweitert**.
7. Deaktivieren Sie alle Optionen und wählen Sie die Option **Sophos NAC-Datenbanken** aus. Klicken Sie auf **Weiter**.

Sie können den Ordner, in dem sich die Skripts zur Erstellung der NAC-Datenbanken befinden, durch Klicken auf **Durchsuchen** ändern. Klicken Sie zum Ändern der SQL Server-Instanz für NAC auf **Auswählen**. Die Schaltfläche **Auswählen** wird nur angezeigt, wenn der NAC-Installer mehrere SQL-Serverinstanzen erkennt.

8. Geben Sie die **Dienstkontoinformationen** auf der entsprechenden Seite in die entsprechenden Felder ein. Klicken Sie auf **Weiter**.

Hierbei handelt es sich um das Standard-Domänenkonto, das von den NAC-Datenbanken und von NAC Manager benötigt wird. Das Dienstkonto wurde in Schritt 1 erstellt.

9. Geben Sie auf der Seite **Geben Sie Ihre Zugangsdaten für den Sophos Download ein** die Sophos Download-Zugangsdaten in die entsprechenden Felder ein. Klicken Sie auf **Weiter**.

Sie erhalten diese Zugangsdaten beim Kauf von Sophos NAC. Sie benötigen die Zugangsdaten zum Herunterladen der aktuellen Erkennungsdaten für Sicherheitsanwendungen. Falsche Angaben können Sie später mit NAC Manager korrigieren. Näheres zu diesem Thema entnehmen Sie bitte der *Hilfe* zu *Sophos Control Center*.

10. Klicken Sie im Dialogfeld **Installationsbereit** auf die Option **Installieren**.

Die NAC-Datenbanken werden konfiguriert. Dabei wird der Installationsfortschritt angezeigt. Ein Teil der Installation nimmt mehrere Minuten in Anspruch, in denen sich die Fortschrittsanzeige nicht ändert. Brechen Sie die Installation nicht ab.

11. Klicken Sie auf **Fertigstellen**.

Wichtig: Bei Installationsfehlern finden Sie im Ereignisprotokoll der Anwendung weitere Informationen. Wenn die Installation der Datenbanken abgebrochen wird, müssen ggf. die folgenden Datenbanken gelöscht werden: AlertStore, AuditStore, GeneralStore, PolicyStore, ReportStore und SecurityStore. Wenn Sie die Datenbanken gelöscht haben, können Sie die Installation wiederholen.

5.6 Anpassen des NAC-Datenbankvolumens

Bei bis zu 1500 Computern wird bei der Installation von NAC die Größe der NAC-Datenbank entsprechend angepasst. In diesem Fall können Sie diesen Abschnitt überspringen.

Bei Installationen in umfangreicheren Netzwerken müssen Sie die Größe der NAC-Datenbanken, der ReportStore-Datenbank und des ReportStore-Protokolls selbst bestimmen. Dieser Abschnitt leistet dabei Hilfestellung.

5.6.1 Richtwert für die ReportStore-Datenbankgröße

Die folgende Tabelle dient als Orientierungshilfe zum Ermitteln der optimalen Größe Ihrer ReportStore-Datenbank.

Anzahl der Computer	Richtwert für die ReportStore-Datenbankgröße
1500	300 MB
3000	379 MB
5000	485 MB
7500	616 MB
10000	748 MB
15000	1011 MB
20000	1274 MB
25000	1536 MB

5.6.2 Richtwert für die ReportStore-Protokollgröße

Die folgende Tabelle dient als Orientierungshilfe zum Ermitteln der optimalen Größe Ihres ReportStore-Protokolls.

Anzahl der Computer	Richtwert für die ReportStore-Protokollgröße
1500	150 MB

Anzahl der Computer	Richtwert für die ReportStore-Protokollgröße
3000	206 MB
5000	281 MB
7500	374 MB
10000	467 MB
15000	653 MB
20000	839 MB
25000	1024 MB

5.6.3 Ändern der NAC-Datenbankgröße – SQL Server 2005/2008

1. Richten Sie im Startmenü von SQL Server den Mauszeiger auf **Microsoft SQL Server 2005** bzw. **Microsoft SQL Server 2008** und klicken Sie auf **SQL Server Management Studio**.
2. Suchen Sie in SQL Server Management Studio die Datenbank ReportStore im Ordner Datenbanken und wählen Sie aus dem Kontextmenü die Option **Eigenschaften**.
3. Wählen Sie im Dialogfeld **Eigenschaften** die Option **Dateien**.
4. Öffnen Sie die Datei ReportStore_Data. Legen Sie im Feld **Anfangsgröße (MB)** die gewünschte Datenbankgröße fest.
5. Öffnen Sie die Datei ReportStore_Log. Legen Sie im Feld **Anfangsgröße (MB)** die gewünschte Protokollgröße fest.
6. Klicken Sie auf **OK**.
7. Schließen Sie SQL Server Management Studio.

5.6.4 Ändern der NAC-Datenbankgröße – SQL Server 2000

1. Richten Sie im Startmenü von SQL Server den Mauszeiger auf **Microsoft SQL Server** und klicken Sie auf **Enterprise Manager**.
2. Suchen Sie in SQL Enterprise Manager die Datenbank ReportStore im Ordner Datenbanken und wählen Sie aus dem Kontextmenü die Option **Eigenschaften**.
3. Klicken Sie im Dialogfeld **ReportStore-Eigenschaften** auf die Registerkarte **Datendateien**.
4. Geben Sie im Feld **Zugeordneter Speicherplatz (MB)** eine angemessene Größe für die Datenbank ein.
5. Klicken Sie auf **In Megabyte** und geben Sie die gewünschte Größe für das Datenbankwachstum an.
6. Klicken Sie auf die Registerkarte **Transaktionsprotokoll**.
7. Geben Sie im Feld **Zugeordneter Speicherplatz (MB)** eine angemessene Größe für das Protokoll ein.
8. Klicken Sie auf **In Megabyte** und geben Sie die gewünschte Größe für das Protokollwachstum an.

9. Klicken Sie auf **OK**.
10. Schließen Sie SQL Enterprise Manager.

5.7 Installieren von NAC Manager

Gehen Sie zu dem Server, auf dem NAC Manager installiert werden soll. Der Server muss mit dem Internet verbunden sein.

Melden Sie als lokaler Administrator an einem Domänenkonto an.

Der NAC-Installationsassistent leitet Sie durch die Installation der erforderlichen Komponenten. Halten Sie bei der NAC-Installation die Betriebssystem-CD bereit, da sich einige erforderliche Komponenten darauf befinden. Die übrigen Komponenten werden automatisch vom NAC-Installationsassistenten installiert.

1. Doppelklicken Sie auf den NAC-Installer, den Sie vorher heruntergeladen haben.
Ein Installationsassistent wird gestartet.
2. Klicken Sie auf **Installieren**.
3. Klicken Sie im Eröffnungsfenster auf **Weiter**.
4. Führen Sie einen der folgenden Schritte durch:
 - Wenn eine Meldung darauf hinweist, dass nur der NAC-Awendungsserver als NAC-Server installiert werden kann, klicken Sie auf **OK**. Klicken Sie auf der Seite **Funktionen auswählen** auf **Weiter**.
 - Wenn sofort die Seite **Funktionen auswählen** angezeigt wird, klicken Sie auf **Erweitert**. Deaktivieren Sie alle Optionen und wählen Sie die Option **Sophos NAC Application Server** aus. Klicken Sie auf **Weiter**.

Klicken Sie zum Ändern des Ordners, in dem sich die NAC Manager-Dateien befinden, auf **Durchsuchen**.

5. Geben Sie die **Dienstkontoinformationen** auf der entsprechenden Seite in die entsprechenden Felder ein. Klicken Sie auf **Weiter**.
Hierbei handelt es sich um das Standard-Domänenkonto, das von den NAC-Datenbanken und von NAC Manager benötigt wird. Das Dienstkonto wurde in Schritt 1 der NAC-Datenbankinstallation erstellt.
6. Geben Sie auf der Seite **Sophos Datenbankserver** den Namen der NAC-Datenbank an. Klicken Sie auf **Weiter**.
Wenn Sie bei der Installation der NAC-Datenbanken die SQL-Serverinstanz für NAC geändert haben, geben Sie den Namen der neuen Serverinstanz im folgenden Format an:
Servername\Instanzname
7. Geben Sie auf der Seite **Proxyserver-Einstellungen** bei Bedarf die Internetproxyeinstellungen des Servers an. Klicken Sie auf **Weiter**.
Die Eingabe der Zugangsdaten ist nur dann erforderlich, wenn NAC Manager einen authentifizierten Proxyserver verwendet.

8. Klicken Sie im Dialogfeld **Das Programm kann jetzt installiert werden** auf die Option **Installieren**.

NAC Manager wird konfiguriert und der Installationsfortschritt wird angezeigt. Ein Teil der Installation nimmt mehrere Minuten in Anspruch, in denen sich die Fortschrittsanzeige nicht ändert. Brechen Sie die Installation nicht ab.

9. Klicken Sie auf **Fertigstellen**.

Hinweis: Bei Installationsfehlern finden Sie im Ereignisprotokoll der Anwendung weitere Informationen.

5.8 Installieren von Compliance Dissolvable Agent auf einem Webserver

Bei Sophos Compliance Dissolvable Agent handelt es sich um eine Client-Komponente von NAC zur Konformitätsprüfung auf Arbeitsstationen. Der Agent ist für Benutzer vorgesehen, auf deren Computern kein Sophos Compliance Agent installiert wurde (z.B. Auftragnehmer oder Gastbenutzer). Compliance Dissolvable Agent muss zunächst auf einem Windows-basierten Webserver installiert werden, der für Benutzer zugänglich ist. Danach kann Compliance Dissolvable Agent über einen Browser heruntergeladen werden.

Hinweis: Es spielt dabei keine Rolle, ob der Agent auf dem Server mit NAC Manager oder den NAC-Datenbanken installiert wird.

1. Doppelklicken Sie auf den Compliance Dissolvable Agent-Installer, den Sie vorher heruntergeladen haben.

Ein Installationsassistent wird gestartet.

2. Klicken Sie im Eröffnungsfenster auf **Weiter**.
3. Behalten Sie im Fenster **Zielordner** den Standardordner bei oder klicken Sie auf **Ändern** und wählen Sie einen anderen Installationsordner. Klicken Sie auf **Weiter**.
4. Geben Sie auf der Seite **Sophos Server** die IP-Adresse oder den DNS-Namen des Servers ein, auf dem Sie NAC Manager installiert haben.

Hinweis: Wenn Sie die Adresse des NAC Manager-Servers später ändern, müssen Sie Compliance Dissolvable Agent auf dem Webserver erneut installieren und die neue Adresse bei der Installation angeben.

5. Wenn NAC über HTTPS kommunizieren soll, aktivieren Sie das Kontrollkästchen **Secure Sophos Server (use HTTPS)**.

Die IP-Adresse oder der DNS-Name des Webzertifikats muss mit dem NAC Manager-Server übereinstimmen.

6. Klicken Sie auf **Weiter**.
7. Klicken Sie im Dialogfeld **Das Programm kann jetzt installiert werden** auf die Option **Installieren**.
8. Klicken Sie auf **Fertigstellen**.

Hinweis: Bei Installationsfehlern finden Sie im Ereignisprotokoll der Anwendung weitere Informationen.

Wenn Sie Compliance Dissolvable Agent im Standardordner installieren, erfolgt der Zugriff darauf über folgende Adresse: `http(s)://IP-Adresse oder DNS-Name/dissolvableagent`. Die IP-Adresse oder der DNS-Name gibt den Webserver an, auf dem Compliance Dissolvable Agent installiert wurde. Beispiel:

`http://www.beispiel.de/dissolvableagenthttps://192.0.2.0/dissolvableagent`

5.9 Anlegen eines Verzeichnisses für Sophos Anti-Virus für NetWare

Wenn auch NetWare-Server geschützt werden sollen, müssen Sie auf jedem zu schützenden Server ein Verzeichnis anlegen, in das der Update Manager die neuesten Versionen von Sophos Anti-Virus für NetWare herunterladen kann.

So legen Sie ein Verzeichnis für Sophos Anti-Virus für NetWare an:

1. Legen Sie auf einem Windows-Computer mit NetWare-Administrator-Software, auf einem der NetWare-Server, die geschützt werden sollen, das Verzeichnis `\\NetWare server\SYS\SWEEP\NLMINST` an. Dabei steht *NetWare server* für den Namen des NetWare-Servers.
2. Geben Sie das Verzeichnis für den Zugriff durch andere Server frei, auf denen ein Update Manager installiert ist.
3. Wiederholen Sie diese Schritte für alle zu schützenden NetWare-Server.

5.10 Herunterladen von Sicherheitssoftware

Zum Herunterladen von Sicherheitssoftware in ein zentrales Verzeichnis, von dem aus sie auf anderen Computern installiert werden kann, muss der installierte Update Manager konfiguriert werden. Hierzu gibt es zwei Methoden:

[Automatisches Konfigurieren des Update Managers](#) (Seite 22). Dies ermöglicht folgende Downloads:

- Nur die neueste Version der Software.
- Nur in Unterverzeichnisse der Freigabe `\\Servername\SophosUpdate`. Hierbei steht *Servername* für die Bezeichnung des Servers, auf dem der Update Manager installiert ist.

[Manuelles Konfigurieren des Update Managers](#) (Seite 23). Dies ermöglicht folgende Downloads:

- Ältere Versionen der Software.
- Downloads in andere Freigaben (z.B. auf anderen Servern).

Hinweis: Sophos Anti-Virus für NetWare müssen Sie anhand dieser Methode herunterladen.

Welche anderen Versionen zum Download bereitstehen, entnehmen Sie bitte dem Abschnitt über das Konfigurieren von Abonnements in der Hilfe zu Enterprise Console.

5.10.1 Automatisches Konfigurieren des Update Managers

1. Wählen Sie in Enterprise Console aus dem Menü **Maßnahmen** die Option **Software-Download-Assistenten starten**.

2. 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**.
3. Wählen Sie auf der Seite **Plattform auswählen** die zu schützenden Plattformen aus.
Klicken Sie auf **Weiter**. Enterprise Console lädt die Software herunter.
4. Der Download-Fortschritt wird auf der Seite **Software-Download** angezeigt. Klicken Sie bei Bedarf auf **Weiter**.
5. Wählen Sie im Dialogfeld **Computer aus Active Directory importieren** die Option **Gruppen für Computer erstellen** aus, wenn Enterprise Console 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 Console gesendet werden.

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

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

Konfigurieren Sie jetzt den Update Manager bei Bedarf manuell. Fahren Sie mit [Freigeben von Sicherheitssoftware in einem Webservice](#) (Seite 42) fort.

5.10.2 Manuelles Konfigurieren des Update Managers

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

1. Klicken Sie in Enterprise Console im Menü **Ansicht** auf **Update Manager**.
2. Wenn der Update Manager *nicht* automatisch konfiguriert wurde, weisen Sie ihm als Update-Quelle die Sophos Website zu:
 - a) Wählen Sie im Fenster **Update Manager** den Update Manager, der auf diesem Server installiert wurde. Rechtsklicken Sie darauf und wählen Sie aus dem Kontextmenü die Option **Konfiguration öffnen/ändern**.
 - b) Klicken Sie im Fenster **Update Manager konfigurieren** auf der Registerkarte **Quellen** auf die Option **Hinzufügen**.
 - c) Wählen Sie im Fenster **Quellen-Details** im Feld **Adresse** die Option **Sophos**. Geben Sie in die Felder **Benutzername** und **Kennwort** die Zugangsdaten für den Download ein, die Sie von Sophos erhalten haben.
 - d) Wenn Sie auf die Update-Quelle über einen Proxyserver zugreifen, aktivieren Sie das Kontrollkästchen **Über Proxyserver verbinden**. Geben Sie die **Adresse** und den **Port** des Proxyservers an. Geben Sie in den Feldern **Benutzername** und **Kennwort** die

entsprechenden Zugangsdaten zum Proxyserver an. Falls der Benutzername auch eine Domäne erfordert, geben Sie ihn im Format Domäne\Benutzername ein.

- e) Klicken Sie auf **OK**, um das Fenster zu schließen.

Sophos wird auf der Registerkarte **Quellen** des Dialogfelds **Update Manager konfigurieren** angeführt.

- f) Klicken Sie auf **OK**, um das Fenster zu schließen.

3. Abonnieren Sie die herunterzuladende Software:

- a) Verfahren Sie im Fensterbereich **Software-Abonnements** wie folgt:

- Doppelklicken Sie auf ein Abonnement, um es zu ändern.
- Klicken Sie zum Hinzufügen eines neuen Abonnements im oberen Fensterbereich auf **Hinzufügen**.

Wichtig: Wenn Sie Sophos Anti-Virus für NetWare abonnieren möchten, müssen Sie zu diesem Zweck ein neues Abonnement hinzufügen. Dieses Abonnement darf keine andere Software enthalten.

- b) Wenn Sie ein neues Abonnement hinzufügen, geben Sie im Fenster **Software-Abonnement** in das Feld **Richtlinie** den Namen ein.
- c) Wählen Sie in der Liste der Plattformen die gewünschte Software aus und doppelklicken Sie auf die gewünschte Version.
- In der Regel bietet sich die Option **Neueste** an, da so sichergestellt wird, dass Software automatisch auf dem neuesten Stand gehalten wird. Welche anderen Versionen zum Download bereitstehen, entnehmen Sie bitte dem Abschnitt über das Konfigurieren von Abonnements in der Hilfe zu Enterprise Console.
- d) Klicken Sie auf **OK**, um das Fenster zu schließen.
- e) Wiederholen Sie diese Schritte für jedes Abonnement, das geändert oder hinzugefügt werden soll.

4. Weisen Sie dem Update Manager diese Abonnements zu:

- a) Wählen Sie im Fenster **Update Manager** den Update Manager, der auf diesem Server installiert wurde. Rechtsklicken Sie darauf und wählen Sie aus dem Kontextmenü die Option **Konfiguration öffnen/ändern**.
- b) Überprüfen Sie im Fenster **Update Manager konfigurieren** auf der Registerkarte **Abonnements**, ob die Abonnements in der Liste **Abonniert für** aufgeführt sind. Ist dies nicht der Fall, wählen Sie in der Liste **Verfügbar** die gewünschten Abonnements aus und klicken Sie auf **>**, um sie in die Liste **Abonniert für** zu verschieben.

5. Wenn Downloads auch auf andere Freigaben als \\Servername\SophosUpdate geschehen sollen, verfahren Sie wie folgt:
 - a) Klicken Sie auf die Registerkarte **Verteilung**.
 - b) Stellen Sie sicher, dass das gewünschte Abonnement auf der Registerkarte oben in der Liste ausgewählt ist.
 - c) Klicken Sie auf **Hinzufügen**.
 - d) Suchen Sie im Fenster **Nach Ordner suchen** eine der Freigaben. Klicken Sie auf **OK**.
 - e) Klicken Sie in der Liste **Verfügbar** auf > und verschieben Sie die Freigabe in die Liste **Update auf**.
 - f) Wählen Sie die Freigabe aus, klicken Sie auf **Konfigurieren** und geben Sie eine Beschreibung ein oder die Zugangsdaten, um darauf zugreifen zu können. Geben Sie im Dialogfeld **Freigaben-Manager** die Beschreibung und die Zugangsdaten ein.
 - g) Wiederholen Sie diese Schritte für jede Freigabe.
6. Klicken Sie auf **OK**, um das Fenster zu schließen.

Die ausgewählte Software wird auf die angegebenen Freigaben heruntergeladen.

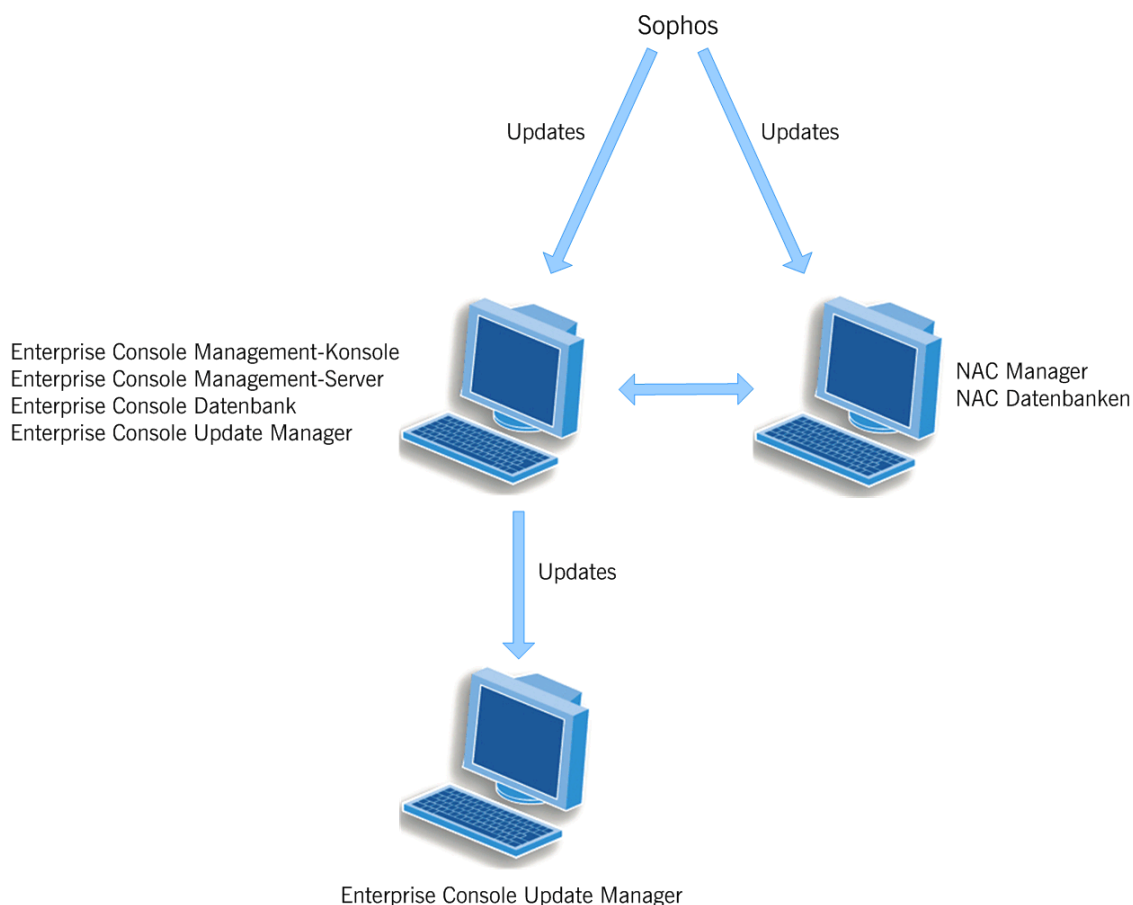
Die Installation der Management-Tools ist hiermit abgeschlossen. Fahren Sie mit [Freigeben von Sicherheitssoftware in einem Webserver](#) (Seite 42) fort.

6 Installieren der Management-Tools – zusätzlicher Update Manager auf separatem Server

In diesem Szenario lassen sich die Update-Quellen der Update Manager auf zweierlei Weise konfigurieren.

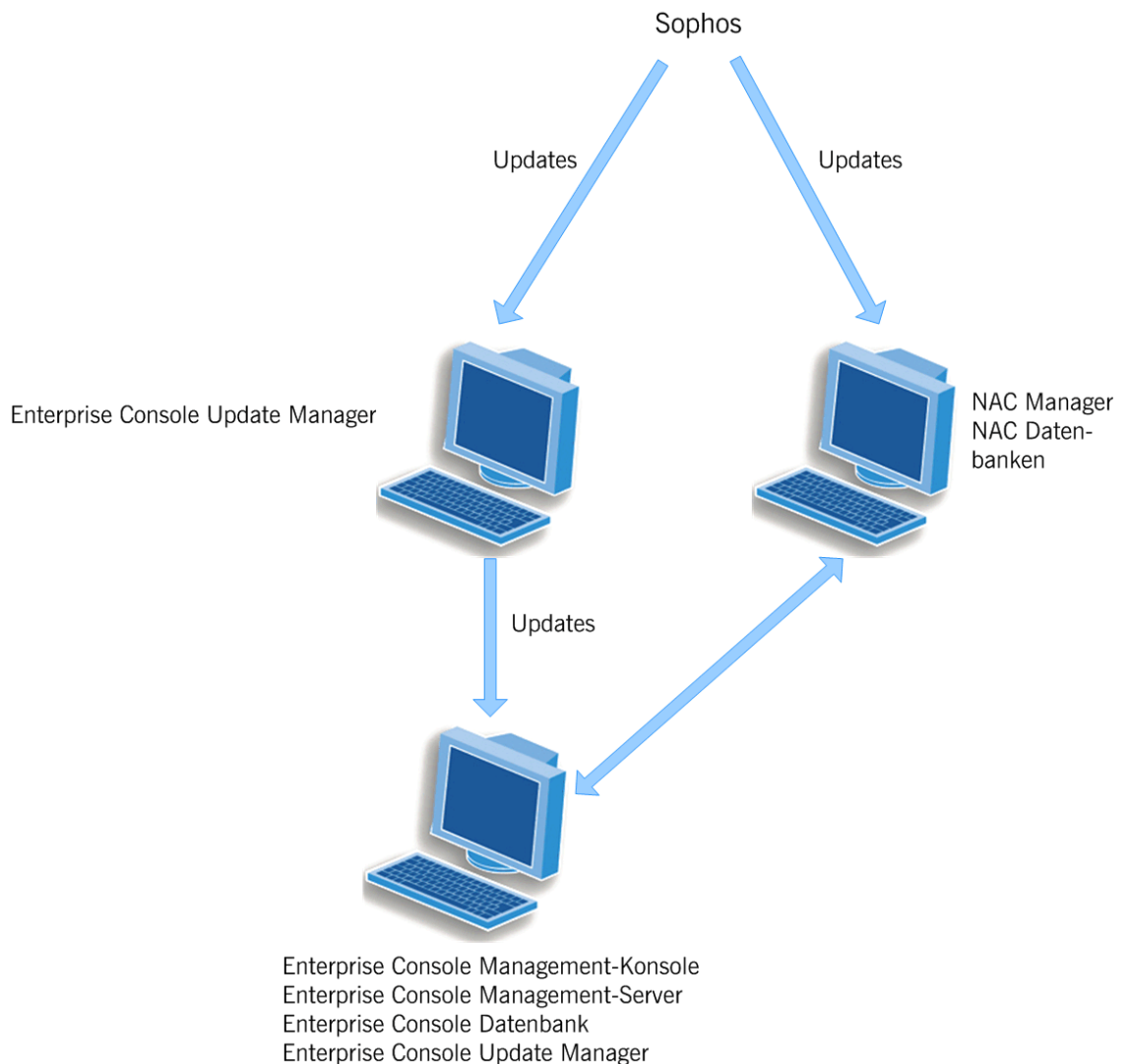
1. Methode:

- Konfigurieren des primären Update Managers, den Sie zusammen mit der Management-Konsole installiert haben, für direkte Updates von der Sophos Website
- Konfigurieren des zusätzlichen Update Managers für Updates vom primären Update Manager



2. Methode:

- Konfigurieren des zusätzlichen Update Managers für direkte Updates von der Sophos Website
- Konfigurieren des Update Managers, den Sie zusammen mit der Management-Konsole installiert haben, für Updates vom zusätzlichen Update Manager



Die zweite Methode empfiehlt sich, wenn der primäre Enterprise Console-Server keine Internetverbindung benötigt.

Die Auswahl einer Methode führt zu folgenden Erwägungen:

- Welche Server müssen an das Internet angeschlossen werden? In den folgenden Installationsabschnitten weisen wir darauf hin, wenn der Installationsserver eine Internetanbindung benötigt.
- Welche Methode soll zum Herunterladen von Sicherheitssoftware in ein zentrales Verzeichnis verwendet werden? Entscheiden Sie sich für eine Methode, wenn Sie so weit sind.

6.1 Herunterladen der Installer

1. Rufen Sie <http://www.sophos.de/support/updates/> auf.
2. Geben Sie Ihre MySophos-Zugangsdaten ein.

3. Laden Sie von der Website für Endpoint Security and Control-Downloads den Enterprise Console-Installer herunter.
4. Laden Sie den NAC Manager-Installer herunter.
5. Laden Sie den Sophos Compliance Dissolvable Agent-Installer herunter.
6. Stellen Sie sicher, dass die Server, auf denen die Software installiert werden soll, auf das Download-Verzeichnis zugreifen können.
Sie können die Installer auch auf eine CD oder DVD brennen.

6.2 Installieren von Enterprise Console: alle Komponenten

Gehen Sie zu dem Server, auf dem alle Komponenten von Enterprise Console installiert werden sollen. Wenn der zusätzliche Update Manager direkt von der Sophos Website updaten soll, muss der Server über Internetzugang verfügen.

Öffnen Sie zur Ermöglichung der Kommunikation der Management-Konsole mit den verwalteten Arbeitsstationen die Ports 8192 und 8194 auf dem Server. Öffnen Sie Port 80 auf dem Server, damit der Update Manager Sicherheitssoftware von Sophos oder einem anderen Update Manager über HTTP herunterladen kann. Öffnen Sie die Ports 137, 138, 139 und 445 auf dem Server, damit der Update Manager Sicherheitssoftware von einem anderen Update Manager über einen UNC-Pfad herunterladen kann.

Wenn der Server unter *Windows Server 2008* betrieben wird, deaktivieren Sie die Benutzerkontensteuerung und starten Sie den Server neu. Nach der Installation von Enterprise Console und der Anmeldung für die Sophos Updates können Sie die Benutzerkontensteuerung wieder einschalten.

Wenn der Server unter *Windows 2000* betrieben wird, muss er nach der Installation neu gestartet werden.

Wenn der Server einer *Domäne* angehört, melden Sie sich als Domänenadministrator an.

Wenn der Server einer *Arbeitsgruppe* angehört, melden Sie sich als lokaler Administrator an.

1. Doppelklicken Sie auf den Enterprise Console-Installer, den Sie vorher heruntergeladen haben.

Ein Installationsassistent wird gestartet.

2. Klicken Sie im Dialogfeld **Sophos Network Installer** auf **Installieren**.

Es wird ein Assistent gestartet, der Sie durch die Installation leitet. Übernehmen Sie die Voreinstellungen und wählen Sie ein **vollständiges** Setup.

Nach der Installation teilt Ihnen der Assistent mit, ob Sie sich abmelden oder den Server neu starten müssen. Wenn Sie sich erneut anmelden, wird Enterprise Console automatisch geöffnet. Der Assistent zum Herunterladen von Sicherheitssoftware wird ausgeführt. Brechen Sie den Assistenten ab. Er wird erst später benötigt.

6.3 Installieren einer zusätzlichen Management-Konsole

Zur einfacheren Verwaltung der Netzwerkcomputer empfiehlt sich ggf. die Installation einer weiteren Management-Konsole auf einem anderen Server. Wenn Sie zu diesem Zeitpunkt keine weitere Management-Konsole installieren möchten, können Sie diesen Abschnitt überspringen.

Wenn der Server unter *Windows Server 2008* betrieben wird, deaktivieren Sie die Benutzerkontensteuerung und starten Sie den Server neu. Nach der Installation der Management-Konsole können Sie die Benutzerkontensteuerung wieder aktivieren.

Wenn der Server unter *Windows 2000* betrieben wird, muss er nach der Installation neu gestartet werden.

Wenn der Server einer *Domäne* angehört, melden Sie sich als Domänenadministrator an.

Wenn der Server einer *Arbeitsgruppe* angehört, melden Sie sich als lokaler Administrator an.

1. Doppelklicken Sie auf den Enterprise Console-Installer, den Sie vorher heruntergeladen haben.

Ein Installationsassistent wird gestartet.

2. Klicken Sie im Dialogfeld **Sophos Network Installer** auf **Installieren**.

Es wird ein Assistent gestartet, der Sie durch die Installation leitet. Übernehmen Sie unter Beachtung der folgenden Ausnahmen die Voreinstellungen:

Klicken Sie auf der Seite **Setup-Typ** auf **Benutzerdefiniert**.

Wählen Sie auf der Seite **Benutzerdefiniertes Setup** die Option **Management-Konsole**. Die Optionen **Management-Server** und **Datenbank** dürfen nicht ausgewählt sein.

Geben Sie auf der Seite **Management-Server** den Namen des Servers ein, auf dem der Management-Server installiert wurde.

Nach der Installation teilt Ihnen der Assistent mit, ob Sie sich abmelden oder den Server neu starten müssen. Bei der nächsten Anmeldung wird Enterprise Console automatisch gestartet. Brechen Sie den Software-Download-Assistenten ggf. ab.

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

So können Sie anderen Benutzern den Zugriff auf eine weitere Management-Konsole gewähren:

- Fügen Sie die Benutzer zu den Gruppen **Sophos Console Administrators** und **Distributed COM-Benutzer** auf dem Server hinzu, auf dem der Management-Server installiert ist.
- Weisen Sie die Benutzer mindestens einer Rolle und Teilverwaltungseinheit in Enterprise Console zu.

Wenn Sie anderen Benutzern die Reporterstellung erlauben möchten, fügen Sie sie zur Gruppe **Sophos DB Users** auf dem Server hinzu, auf dem die Enterprise Console-Datenbank installiert ist.

6.4 Installieren von NAC Manager und den NAC-Datenbanken

Gehen Sie zu dem Server, auf dem NAC Manager und die NAC-Datenbanken installiert werden sollen. Der Server muss mit dem Internet verbunden sein.

Stellen Sie vor der Installation der NAC-Datenbanken sicher, dass die richtige Version von SQL Server installiert wurde.

- Bei bis zu 1500 Arbeitsstationen wird SQL Server MSDE, SQL Server 2005 Express oder SQL Server 2008 Express empfohlen. SQL Server MSDE-Datenbanken dürfen maximal 2 GB und 2005/2008 Express-Datenbanken maximal 4 GB umfassen.
- Für mehr als 1500 Arbeitsstationen eignet sich besonders SQL Server 2000, 2005 oder 2008.

Für die Installation von NAC melden Sie sich bitte wie folgt an:

- Wenn sich der Server in einer Domäne befindet, melden Sie sich als Domänenadministrator an.
- Wenn sich der Server in einer Arbeitsgruppe befindet, melden Sie sich als lokaler Administrator an.

Der NAC-Installationsassistent leitet Sie durch die Installation der erforderlichen Komponenten. Halten Sie bei der NAC-Installation die Betriebssystem-CD bereit, da sich einige erforderliche Komponenten darauf befinden. Die übrigen Komponenten werden automatisch vom NAC-Installationsassistenten installiert.

1. Doppelklicken Sie auf den NAC-Installer, den Sie vorher heruntergeladen haben.
Ein Installationsassistent wird gestartet.
2. Klicken Sie auf **Installieren**.
3. Klicken Sie im Eröffnungsfenster auf **Weiter**.
4. Klicken Sie auf der Seite **Funktionen auswählen** auf **Weiter**.
5. Geben Sie auf der Seite **Geben Sie Ihre Zugangsdaten für den Sophos Download ein** die Sophos Download-Zugangsdaten in die entsprechenden Felder ein. Klicken Sie auf **Weiter**.
Sie erhalten diese Zugangsdaten beim Kauf von Sophos NAC. Sie benötigen die Zugangsdaten zum Herunterladen der aktuellen Erkennungsdaten für Sicherheitsanwendungen. Falsche Angaben können Sie zu einem späteren Zeitpunkt mit NAC Manager korrigieren. Näheres zu diesem Thema entnehmen Sie bitte der *Hilfe* zu *Sophos Control Center*.
6. Geben Sie auf der Seite **Proxyserver-Einstellungen** bei Bedarf die Internetproxyeinstellungen des Servers an. Klicken Sie auf **Weiter**.
Die Eingabe der Zugangsdaten ist nur dann erforderlich, wenn NAC Manager einen authentifizierten Proxyserver verwendet.
7. Klicken Sie im Dialogfeld **Installationsbereit** auf die Option **Installieren**.
NAC wird konfiguriert und der Installationsfortschritt wird angezeigt. Ein Teil der Installation nimmt mehrere Minuten in Anspruch, in denen sich die Fortschrittsanzeige nicht ändert. Brechen Sie die Installation nicht ab.

8. Klicken Sie auf **Fertigstellen**.

Wichtig: Bei Installationsfehlern finden Sie im Ereignisprotokoll der Anwendung weitere Informationen. Wenn die Installation der Datenbanken abgebrochen wird, müssen ggf. die folgenden Datenbanken gelöscht werden: AlertStore, AuditStore, GeneralStore, PolicyStore, ReportStore und SecurityStore. Wenn Sie die Datenbanken gelöscht haben, können Sie die Installation wiederholen.

6.5 Anpassen des NAC-Datenbankvolumens

Bei bis zu 1500 Computern wird bei der Installation von NAC die Größe der NAC-Datenbank entsprechend angepasst. In diesem Fall können Sie diesen Abschnitt überspringen.

Bei Installationen in umfangreicheren Netzwerken müssen Sie die Größe der NAC-Datenbanken, der ReportStore-Datenbank und des ReportStore-Protokolls selbst bestimmen. Dieser Abschnitt leistet dabei Hilfestellung.

6.5.1 Richtwert für die ReportStore-Datenbankgröße

Die folgende Tabelle dient als Orientierungshilfe zum Ermitteln der optimalen Größe Ihrer ReportStore-Datenbank.

Anzahl der Computer	Richtwert für die ReportStore-Datenbankgröße
1500	300 MB
3000	379 MB
5000	485 MB
7500	616 MB
10000	748 MB
15000	1011 MB
20000	1274 MB
25000	1536 MB

6.5.2 Richtwert für die ReportStore-Protokollgröße

Die folgende Tabelle dient als Orientierungshilfe zum Ermitteln der optimalen Größe Ihres ReportStore-Protokolls.

Anzahl der Computer	Richtwert für die ReportStore-Protokollgröße
1500	150 MB

Anzahl der Computer	Richtwert für die ReportStore-Protokollgröße
3000	206 MB
5000	281 MB
7500	374 MB
10000	467 MB
15000	653 MB
20000	839 MB
25000	1024 MB

6.5.3 Ändern der NAC-Datenbankgröße – SQL Server 2005/2008

1. Richten Sie im Startmenü von SQL Server den Mauszeiger auf **Microsoft SQL Server 2005** bzw. **Microsoft SQL Server 2008** und klicken Sie auf **SQL Server Management Studio**.
2. Suchen Sie in SQL Server Management Studio die Datenbank ReportStore im Ordner Datenbanken und wählen Sie aus dem Kontextmenü die Option **Eigenschaften**.
3. Wählen Sie im Dialogfeld **Eigenschaften** die Option **Dateien**.
4. Öffnen Sie die Datei ReportStore_Data. Legen Sie im Feld **Anfangsgröße (MB)** die gewünschte Datenbankgröße fest.
5. Öffnen Sie die Datei ReportStore_Log. Legen Sie im Feld **Anfangsgröße (MB)** die gewünschte Protokollgröße fest.
6. Klicken Sie auf **OK**.
7. Schließen Sie SQL Server Management Studio.

6.5.4 Ändern der NAC-Datenbankgröße – SQL Server 2000

1. Richten Sie im Startmenü von SQL Server den Mauszeiger auf **Microsoft SQL Server** und klicken Sie auf **Enterprise Manager**.
2. Suchen Sie in SQL Enterprise Manager die Datenbank ReportStore im Ordner Datenbanken und wählen Sie aus dem Kontextmenü die Option **Eigenschaften**.
3. Klicken Sie im Dialogfeld **ReportStore-Eigenschaften** auf die Registerkarte **Datendateien**.
4. Geben Sie im Feld **Zugeordneter Speicherplatz (MB)** eine angemessene Größe für die Datenbank ein.
5. Klicken Sie auf **In Megabyte** und geben Sie die gewünschte Größe für das Datenbankwachstum an.
6. Klicken Sie auf die Registerkarte **Transaktionsprotokoll**.
7. Geben Sie im Feld **Zugeordneter Speicherplatz (MB)** eine angemessene Größe für das Protokoll ein.
8. Klicken Sie auf **In Megabyte** und geben Sie die gewünschte Größe für das Protokollwachstum an.

9. Klicken Sie auf **OK**.
10. Schließen Sie SQL Enterprise Manager.

6.6 Installieren eines zusätzlichen Update Managers

Begeben Sie sich zum Server, auf dem ein zusätzlicher Update Manager installiert werden soll. Wenn der zusätzliche Update Manager direkt von der Sophos Website updaten soll, muss der Server über Internetzugang verfügen.

Öffnen Sie Port 80 auf dem Server, damit der Update Manager Sicherheitssoftware von Sophos oder einem anderen Update Manager über HTTP herunterladen kann. Öffnen Sie die Ports 137, 138, 139 und 445 auf dem Server, damit der Update Manager Sicherheitssoftware von einem anderen Update Manager über einen UNC-Pfad herunterladen kann.

Wenn die Windows-Version des Servers über integrierte Netzwerkerkennung verfügt, diese Funktion jedoch deaktiviert ist, aktivieren Sie sie und starten Sie den Server neu.

Wenn der Server unter *Windows Server 2008* betrieben wird, deaktivieren Sie die Benutzerkontensteuerung und starten Sie den Server neu. Nach der Installation des Update Managers und der Anmeldung für die Sophos Updates können Sie die Benutzerkontensteuerung wieder aktivieren.

Wenn der Server unter *Windows 2000* betrieben wird, muss er nach der Installation neu gestartet werden.

Wenn der Server einer *Domäne* angehört, melden Sie sich als Domänenadministrator an.

Wenn der Server einer *Arbeitsgruppe* angehört, melden Sie sich als lokaler Administrator an.

1. Suchen Sie auf dem Enterprise Console-Server die Ordnerfreigabe SumInstallSet.
2. Doppelklicken Sie auf Setup.exe, um den Installer zu starten.
3. Klicken Sie im Fenster **Sophos Update Manager** auf **Weiter**.

Es wird ein Assistent gestartet, der Sie durch die Installation leitet. Übernehmen Sie die Voreinstellungen.

Der installierte Update Manager wird nun von Enterprise Console verwaltet.

6.7 Installieren von Compliance Dissolvable Agent auf einem Webserver

Bei Sophos Compliance Dissolvable Agent handelt es sich um eine Client-Komponente von NAC zur Konformitätsprüfung auf Arbeitsstationen. Der Agent ist für Benutzer vorgesehen, auf deren Computern kein Sophos Compliance Agent installiert wurde (z.B. Auftragnehmer oder Gastbenutzer). Compliance Dissolvable Agent muss zunächst auf einem Windows-basierten Webserver installiert werden, der für Benutzer zugänglich ist. Danach kann Compliance Dissolvable Agent über einen Browser heruntergeladen werden.

Hinweis: Es spielt dabei keine Rolle, ob der Agent auf dem Server mit NAC Manager oder den NAC-Datenbanken installiert wird.

1. Doppelklicken Sie auf den Compliance Dissolvable Agent-Installer, den Sie vorher heruntergeladen haben.

Ein Installationsassistent wird gestartet.

2. Klicken Sie im Eröffnungsfenster auf **Weiter**.
3. Behalten Sie im Fenster **Zielordner** den Standardordner bei oder klicken Sie auf **Ändern** und wählen Sie einen anderen Installationsordner. Klicken Sie auf **Weiter**.
4. Geben Sie auf der Seite **Sophos Server** die IP-Adresse oder den DNS-Namen des Servers ein, auf dem Sie NAC Manager installiert haben.

Hinweis: Wenn Sie die Adresse des NAC Manager-Servers später ändern, müssen Sie Compliance Dissolvable Agent auf dem Webserver erneut installieren und die neue Adresse bei der Installation angeben.

5. Wenn NAC über HTTPS kommunizieren soll, aktivieren Sie das Kontrollkästchen **Secure Sophos Server (use HTTPS)**.

Die IP-Adresse oder der DNS-Name des Webzertifikats muss mit dem NAC Manager-Server übereinstimmen.

6. Klicken Sie auf **Weiter**.
7. Klicken Sie im Dialogfeld **Das Programm kann jetzt installiert werden** auf die Option **Installieren**.
8. Klicken Sie auf **Fertigstellen**.

Hinweis: Bei Installationsfehlern finden Sie im Ereignisprotokoll der Anwendung weitere Informationen.

Wenn Sie Compliance Dissolvable Agent im Standardordner installieren, erfolgt der Zugriff darauf über folgende Adresse: `http(s)://IP-Adresse oder DNS-Name/dissolvableagent`. Die IP-Adresse oder der DNS-Name gibt den Webserver an, auf dem Compliance Dissolvable Agent installiert wurde. Beispiel:

`http://www.beispiel.de/dissolvableagenthttps://192.0.2.0/dissolvableagent`

6.8 Anlegen eines Verzeichnisses für Sophos Anti-Virus für NetWare

Wenn auch NetWare-Server geschützt werden sollen, müssen Sie auf jedem zu schützenden Server ein Verzeichnis anlegen, in das der Update Manager die neuesten Versionen von Sophos Anti-Virus für NetWare herunterladen kann.

So legen Sie ein Verzeichnis für Sophos Anti-Virus für NetWare an:

1. Legen Sie auf einem Windows-Computer mit NetWare-Administrator-Software, auf einem der NetWare-Server, die geschützt werden sollen, das Verzeichnis `\\NetWare server\SYS\SWEET\NLMINST` an. Dabei steht *NetWare server* für den Namen des NetWare-Servers.
2. Geben Sie das Verzeichnis für den Zugriff durch andere Server frei, auf denen ein Update Manager installiert ist.

3. Wiederholen Sie diese Schritte für alle zu schützenden NetWare-Server.

6.9 Herunterladen von Sicherheitssoftware

Wie bereits erläutert, lassen sich die Update-Quellen der Update Manager in diesem Szenario auf zweierlei Weise konfigurieren. Wählen Sie die passende Methode aus:

- [Primärer Update Manager bezieht Updates von Sophos](#) (Seite 35)
- [Weiterer Update Manager bezieht Updates von Sophos](#) (Seite 39)

6.9.1 Primärer Update Manager bezieht Updates von Sophos

Konfigurieren des primären Update Managers für Updates von Sophos

Der primäre Update Manager, den Sie zusammen mit der Management-Konsole installiert haben, muss für direkte Updates von der Sophos Website konfiguriert werden. Hierzu gibt es zwei Methoden:

[Automatisches Konfigurieren des primären Update Managers](#) (Seite 35). Dies ermöglicht folgende Downloads:

- Nur die neueste Version der Software.
- Nur in Unterverzeichnisse der Freigabe `\\Servername\SophosUpdate`. Hierbei steht `Servername` für die Bezeichnung des Servers, auf dem der primäre Update Manager installiert ist.

[Manuelles Konfigurieren des primären Update Managers](#) (Seite 36). Dies ermöglicht folgende Downloads:

- Ältere Versionen der Software.
- Downloads in andere Freigaben (z.B. auf anderen Servern).

Hinweis: To download Sophos Anti-Virus for NetWare, you must use this method.

Welche anderen Versionen zum Download bereitstehen, entnehmen Sie bitte dem Abschnitt über das Konfigurieren von Abonnements in der Hilfe zu Enterprise Console.

Konfigurieren des zusätzlichen Update Managers für Updates vom primären Update Manager

Dies wird im Abschnitt [Konfigurieren eines zusätzlichen Update Managers](#) (Seite 37) ausführlich beschrieben.

6.9.1.1 Automatisches Konfigurieren des primären Update Managers

1. Wählen Sie in Enterprise Console aus dem Menü **Maßnahmen** die Option **Software-Download-Assistenten starten**.
2. 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**.

3. Wählen Sie auf der Seite **Plattform auswählen** die zu schützenden Plattformen aus.
Klicken Sie auf **Weiter**. Enterprise Console lädt die Software herunter.
4. Der Download-Fortschritt wird auf der Seite **Software-Download** angezeigt. Klicken Sie bei Bedarf auf **Weiter**.
5. Wählen Sie im Dialogfeld **Computer aus Active Directory importieren** die Option **Gruppen für Computer erstellen** aus, wenn Enterprise Console 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 Console gesendet werden.

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

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

Konfigurieren Sie jetzt den Update Manager bei Bedarf manuell. Fahren Sie mit [Konfigurieren eines zusätzlichen Update Managers](#) (Seite 37) fort.

6.9.1.2 Manuelles Konfigurieren des primären Update Managers

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

1. Klicken Sie in Enterprise Console im Menü **Ansicht** auf **Update Manager**.
2. Wenn der Update Manager *nicht* automatisch konfiguriert wurde, weisen Sie ihm als Update-Quelle die Sophos Website zu:
 - a) Wählen Sie im Fenster **Update Manager** den Update Manager, der auf diesem Server installiert wurde. Rechtsklicken Sie darauf und wählen Sie aus dem Kontextmenü die Option **Konfiguration öffnen/ändern**.
 - b) Klicken Sie im Fenster **Update Manager konfigurieren** auf der Registerkarte **Quellen** auf die Option **Hinzufügen**.
 - c) Wählen Sie im Fenster **Quellen-Details** im Feld **Adresse** die Option **Sophos**. Geben Sie in die Felder **Benutzername** und **Kennwort** die Zugangsdaten für den Download ein, die Sie von Sophos erhalten haben.
 - d) Wenn Sie auf die Update-Quelle über einen Proxyserver zugreifen, aktivieren Sie das Kontrollkästchen **Über Proxyserver verbinden**. Geben Sie die **Adresse** und den **Port** des Proxyservers an. Geben Sie in den Feldern **Benutzername** und **Kennwort** die entsprechenden Zugangsdaten zum Proxyserver an. Falls der Benutzername auch eine Domäne erfordert, geben Sie ihn im Format Domäne\Benutzername ein.
 - e) Klicken Sie auf **OK**, um das Fenster zu schließen.

Sophos wird auf der Registerkarte **Quellen** des Dialogfelds **Update Manager konfigurieren** angeführt.

f) Klicken Sie auf **OK**, um das Fenster zu schließen.

3. Abonnieren Sie die herunterzuladende Software:

a) Verfahren Sie im Fensterbereich **Software-Abonnements** wie folgt:

- Doppelklicken Sie auf ein Abonnement, um es zu ändern.
- Klicken Sie zum Hinzufügen eines neuen Abonnements im oberen Fensterbereich auf **Hinzufügen**.

Wichtig: Wenn Sie Sophos Anti-Virus für NetWare abonnieren möchten, müssen Sie zu diesem Zweck ein neues Abonnement hinzufügen. Dieses Abonnement darf keine andere Software enthalten.

b) Wenn Sie ein neues Abonnement hinzufügen, geben Sie im Fenster **Software-Abonnement** in das Feld **Richtlinie** den Namen ein.

c) Wählen Sie in der Liste der Plattformen die gewünschte Software aus und doppelklicken Sie auf die gewünschte Version.

In der Regel bietet sich die Option **Neueste** an, da so sichergestellt wird, dass Software automatisch auf dem neuesten Stand gehalten wird. Welche anderen Versionen zum Download bereitstehen, entnehmen Sie bitte dem Abschnitt über das Konfigurieren von Abonnements in der Hilfe zu Enterprise Console.

d) Klicken Sie auf **OK**, um das Fenster zu schließen.

e) Wiederholen Sie diese Schritte für jedes Abonnement, das geändert oder hinzugefügt werden soll.

4. Weisen Sie dem Update Manager diese Abonnements zu:

a) Wählen Sie im Fenster **Update Manager** den Update Manager, der auf diesem Server installiert wurde. Rechtsklicken Sie darauf und wählen Sie aus dem Kontextmenü die Option **Konfiguration öffnen/ändern**.

b) Überprüfen Sie im Fenster **Update Manager konfigurieren** auf der Registerkarte **Abonnements**, ob die Abonnements in der Liste **Abonniert für** aufgeführt sind. Ist dies nicht der Fall, wählen Sie in der Liste **Verfügbar** die gewünschten Abonnements aus und klicken Sie auf **>**, um sie in die Liste **Abonniert für** zu verschieben.

5. Klicken Sie auf **OK**, um das Fenster zu schließen.

Die ausgewählte Software wird auf den auf diesem Server installierten Update Manager heruntergeladen.

6.9.1.3 Konfigurieren eines zusätzlichen Update Managers

1. Klicken Sie in Enterprise Console im Menü **Ansicht** auf **Update Manager**.

2. Weisen Sie dem zusätzlichen Update Manager als Update-Quelle den primären Update Manager zu:
 - a) Wählen Sie im Bereich **Update Manager** den zusätzlichen Update Manager. Rechtsklicken Sie darauf und wählen Sie aus dem Kontextmenü die Option **Konfiguration öffnen/ändern**.
 - b) Klicken Sie im Fenster **Update Manager konfigurieren** auf der Registerkarte **Quellen** auf die Option **Hinzufügen**.
 - c) Wählen Sie im Fenster **Quellenangaben** im Feld **Adresse** die Freigabe, in die der primäre Update Manager die Software herunterladen soll.

Die Felder **Benutzername** und **Kennwort** werden automatisch mit den entsprechenden Zugangsdaten ausgefüllt.
 - d) Wenn Sie auf die Update-Quelle über einen Proxyserver zugreifen, aktivieren Sie das Kontrollkästchen **Über Proxyserver verbinden**. Geben Sie die **Adresse** und den **Port** des Proxyservers an. Geben Sie in den Feldern **Benutzername** und **Kennwort** die entsprechenden Zugangsdaten zum Proxyserver an. Falls der Benutzername auch eine Domäne erfordert, geben Sie ihn im Format Domäne\Benutzername ein.
 - e) Klicken Sie auf **OK**, um das Fenster zu schließen.

Die Freigabe, in die der primäre Update Manager die Software herunterlädt, wird im Fenster **Update Manager konfigurieren** auf der Registerkarte **Quellen** angezeigt.
3. So legen Sie die zuvor eingerichteten Abonnements für den Update Manager fest:
 - Überprüfen Sie auf der Registerkarte **Abonnements**, ob sich die Abonnements in der Liste **Abonniert für** befinden. Ist dies nicht der Fall, wählen Sie in der Liste **Verfügbar** die gewünschten Abonnements aus und klicken Sie auf >, um sie in die Liste **Abonniert für** zu verschieben.
4. Wenn Downloads auch auf andere Freigaben als \\Servername\SophosUpdate geschehen sollen, verfahren Sie wie folgt:
 - a) Klicken Sie auf die Registerkarte **Verteilung**.
 - b) Stellen Sie sicher, dass das gewünschte Abonnement auf der Registerkarte oben in der Liste ausgewählt ist.
 - c) Klicken Sie auf **Hinzufügen**.
 - d) Suchen Sie im Fenster **Nach Ordner suchen** eine der Freigaben. Klicken Sie auf **OK**.
 - e) Klicken Sie in der Liste **Verfügbar** auf > und verschieben Sie die Freigabe in die Liste **Update auf**.
 - f) Wählen Sie die Freigabe aus, klicken Sie auf **Konfigurieren** und geben Sie eine Beschreibung ein oder die Zugangsdaten, um darauf zugreifen zu können. Geben Sie im Dialogfeld **Freigaben-Manager** die Beschreibung und die Zugangsdaten ein.
 - g) Wiederholen Sie diese Schritte für jede Freigabe.

5. Klicken Sie auf **OK**, um das Fenster zu schließen.

Die ausgewählte Software wird in die Freigaben heruntergeladen, die beim nächsten geplanten Update angegeben werden.

Die Installation der Management-Tools ist hiermit abgeschlossen. Fahren Sie mit *Freigeben von Sicherheitssoftware in einem Webserven* (Seite 42) fort.

6.9.2 Weiterer Update Manager bezieht Updates von Sophos

Die Konfiguration eines zusätzlichen Update Managers wird im Abschnitt *Konfigurieren eines zusätzlichen Update Managers* (Seite 39) ausführlich beschrieben.

Im Abschnitt *Konfigurieren des primären Update Managers* (Seite 40) wird beschrieben, wie Sie den primären Update Manager, der zusammen mit der Management-Konsole installiert wurde, für Updates vom zusätzlichen Update Manager konfiguriert wird.

6.9.2.1 Konfigurieren eines zusätzlichen Update Managers

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

1. Klicken Sie in Enterprise Console im Menü **Ansicht** auf **Update Manager**.
2. Weisen Sie dem zusätzlichen Update Manager als Update-Quelle die Sophos Website zu:
 - a) Wählen Sie im Bereich **Update Manager** den zusätzlichen Update Manager. Rechtsklicken Sie darauf und wählen Sie aus dem Kontextmenü die Option **Konfiguration öffnen/ändern**.
 - b) Klicken Sie im Fenster **Update Manager konfigurieren** auf der Registerkarte **Quellen** auf die Option **Hinzufügen**.
 - c) Wählen Sie im Fenster **Quellen-Details** im Feld **Adresse** die Option **Sophos**. Geben Sie in die Felder **Benutzername** und **Kennwort** die Zugangsdaten für den Download ein, die Sie von Sophos erhalten haben.
 - d) Wenn Sie auf die Update-Quelle über einen Proxyserver zugreifen, aktivieren Sie das Kontrollkästchen **Über Proxyserver verbinden**. Geben Sie die **Adresse** und den **Port** des Proxyservers an. Geben Sie in den Feldern **Benutzername** und **Kennwort** die entsprechenden Zugangsdaten zum Proxyserver an. Falls der Benutzername auch eine Domäne erfordert, geben Sie ihn im Format Domäne\Benutzername ein.
 - e) Klicken Sie auf **OK**, um das Fenster zu schließen.
Sophos wird auf der Registerkarte **Quellen** des Dialogfelds **Update Manager konfigurieren** angeführt.
 - f) Klicken Sie auf **OK**, um das Fenster zu schließen.
3. Abonnieren Sie die herunterzuladende Software:
 - a) Verfahren Sie im Fensterbereich **Software-Abonnements** wie folgt:
 - Doppelklicken Sie auf ein Abonnement, um es zu ändern.

- Klicken Sie zum Hinzufügen eines neuen Abonnements im oberen Fensterbereich auf **Hinzufügen**.

Wichtig: Wenn Sie Sophos Anti-Virus für NetWare abonnieren möchten, müssen Sie zu diesem Zweck ein neues Abonnement hinzufügen. Dieses Abonnement darf keine andere Software enthalten.

- b) Wenn Sie ein neues Abonnement hinzufügen, geben Sie im Fenster **Software-Abonnement** in das Feld **Richtlinie** den Namen ein.
 - c) Wählen Sie in der Liste der Plattformen die gewünschte Software aus und doppelklicken Sie auf die gewünschte Version.
In der Regel bietet sich die Option **Neueste** an, da so sichergestellt wird, dass Software automatisch auf dem neuesten Stand gehalten wird. Welche anderen Versionen zum Download bereitstehen, entnehmen Sie bitte dem Abschnitt über das Konfigurieren von Abonnements in der Hilfe zu Enterprise Console.
 - d) Klicken Sie auf **OK**, um das Fenster zu schließen.
 - e) Wiederholen Sie diese Schritte für jedes Abonnement, das geändert oder hinzugefügt werden soll.
4. Weisen Sie dem Update Manager diese Abonnements zu:
- a) Wählen Sie im Bereich **Update Manager** den zusätzlichen Update Manager. Rechtsklicken Sie darauf und wählen Sie aus dem Kontextmenü die Option **Konfiguration öffnen/ändern**.
 - b) Überprüfen Sie im Fenster **Update Manager konfigurieren** auf der Registerkarte **Abonnements**, ob die Abonnements in der Liste **Abonniert für** aufgeführt sind. Ist dies nicht der Fall, wählen Sie in der Liste **Verfügbar** die gewünschten Abonnements aus und klicken Sie auf >, um sie in die Liste **Abonniert für** zu verschieben.
5. Klicken Sie auf **OK**, um das Fenster zu schließen.
- Die ausgewählte Software wird in den zusätzlichen Update Manager heruntergeladen.

6.9.2.2 Konfigurieren des primären Update Managers

1. Klicken Sie in Enterprise Console im Menü **Ansicht** auf **Update Manager**.
2. Weisen Sie dem primären Update Manager als Update-Quelle einen anderen (zusätzlich eingerichteten) Update Manager zu:
 - a) Wählen Sie im Fenster **Update Manager** den Update Manager, der auf diesem Server installiert wurde. Rechtsklicken Sie darauf und wählen Sie aus dem Kontextmenü die Option **Konfiguration öffnen/ändern**.
 - b) Klicken Sie im Fenster **Update Manager konfigurieren** auf der Registerkarte **Quellen** auf die Option **Hinzufügen**.
 - c) Wählen Sie im Fenster **Quellen-Details** im Feld **Adresse** die Freigabe, in die der zusätzliche Update Manager die Software herunterladen soll.

Die Felder **Benutzername** und **Kennwort** werden automatisch mit den entsprechenden Zugangsdaten ausgefüllt.

- d) Wenn Sie auf die Update-Quelle über einen Proxyserver zugreifen, aktivieren Sie das Kontrollkästchen **Über Proxyserver verbinden**. Geben Sie die **Adresse** und den **Port** des Proxyservers an. Geben Sie in den Feldern **Benutzername** und **Kennwort** die entsprechenden Zugangsdaten zum Proxyserver an. Falls der Benutzername auch eine Domäne erfordert, geben Sie ihn im Format Domäne\Benutzername ein.
- e) Klicken Sie auf **OK**, um das Fenster zu schließen.

Die Freigabe, in die der zusätzliche Update Manager die Software herunterlädt, wird im Fenster **Update Manager konfigurieren** auf der Registerkarte **Quellen** angezeigt.

- 3. So legen Sie die zuvor eingerichteten Abonnements für den Update Manager fest:
 - Überprüfen Sie auf der Registerkarte **Abonnements**, ob sich die Abonnements in der Liste **Abonniert für** befinden. Ist dies nicht der Fall, wählen Sie in der Liste **Verfügbar** die gewünschten Abonnements aus und klicken Sie auf >, um sie in die Liste **Abonniert für** zu verschieben.
- 4. Wenn Downloads auch auf andere Freigaben als \\Servername\SophosUpdate geschehen sollen, verfahren Sie wie folgt:
 - a) Klicken Sie auf die Registerkarte **Verteilung**.
 - b) Stellen Sie sicher, dass das gewünschte Abonnement auf der Registerkarte oben in der Liste ausgewählt ist.
 - c) Klicken Sie auf **Hinzufügen**.
 - d) Suchen Sie im Fenster **Nach Ordner suchen** eine der Freigaben. Klicken Sie auf **OK**.
 - e) Klicken Sie in der Liste **Verfügbar** auf > und verschieben Sie die Freigabe in die Liste **Update auf**.
 - f) Wählen Sie die Freigabe aus, klicken Sie auf **Konfigurieren** und geben Sie eine Beschreibung ein oder die Zugangsdaten, um darauf zugreifen zu können. Geben Sie im Dialogfeld **Freigaben-Manager** die Beschreibung und die Zugangsdaten ein.
 - g) Wiederholen Sie diese Schritte für jede Freigabe.
- 5. Klicken Sie auf **OK**, um das Fenster zu schließen.

Die ausgewählte Software wird in die Freigaben heruntergeladen, die beim nächsten geplanten Update angegeben werden.

Die Installation der Management-Tools ist hiermit abgeschlossen. Fahren Sie mit [Freigeben von Sicherheitssoftware in einem Webservice](#) (Seite 42) fort.

7 Freigeben von Sicherheitssoftware in einem Webserver

Bisweilen empfiehlt sich, Sophos Sicherheitssoftware in einem Webserver freizugeben, damit Computer über HTTP darauf zugreifen können. Bei der Installation von Sophos Anti-Virus für UNIX, Version 4, *muss* dieser Schritt durchgeführt werden, kann jedoch auf Wunsch auch erst nach dem Download von Sophos Anti-Virus für UNIX, Version 4, erfolgen.

So geben Sie Sicherheitssoftware in einem Webserver frei:

1. Den Pfad zur Freigabe, in die die Sicherheitssoftware heruntergeladen wurde („Bootstrap-Verzeichnis“), können Sie wie folgt ermitteln:
 - a) Klicken Sie in Enterprise Console 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 den Pfad bis ausschließlich des Ordners des zentralen Installationsverzeichnisses. Beispiel:
`\\server name\SophosUpdate`
2. Stellen Sie das Bootstrap-Verzeichnis, einschließlich der Unterordner, auf dem Webserver bereit.
3. Legen Sie Benutzernamen und Kennwörter zum Schutz vor unerlaubtem Zugriff auf den Ordner im Webserver fest.

Hinweis: Anweisungen zur Freigabe von Ordnern im Internet und zum Einrichten von Zugangsdaten entnehmen Sie bitte dem Begleitmaterial des Webservers. Wenden Sie sich bei weiteren Fragen bitte an Ihren Webserver-Betreiber.

8 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. Fahren Sie mit den Anweisungen im Abschnitt [Einrichten von Sicherheitsrichtlinien](#) (Seite 44) fort.

Zunächst müssen Gruppen erstellt werden.

1. Wenn der Bereich **Gruppen** nicht links unten im Fenster angezeigt wird, wählen Sie aus dem Menü **Ansicht** die Option **Endpoints**.
2. Klicken Sie in den Bereich **Gruppen**.
3. Wählen Sie aus dem Menü **Gruppen** die Option **Gruppe erstellen**.

Im linken Fensterbereich wird eine **Neue Gruppe** hinzugefügt, deren Name hervorgehoben ist.

4. Geben Sie der Gruppe einen Namen.
5. Zum Erstellen weiterer Hauptgruppen wählen Sie den oben im Bereich **Gruppen** angezeigten Server und wiederholen die Schritte 3 und 4.

Um in einer Gruppe eine Untergruppe zu erstellen, wählen Sie die entsprechende Gruppe aus und wiederholen die Schritte 3 und 4.

9 Einrichten von Sicherheitsrichtlinien

Eine *Sicherheitsrichtlinie* besteht aus mehreren Einstellungen, die auf die Computer in einer Gruppe oder Gruppen übertragen werden können.

Enterprise Console übernimmt die Standardrichtlinien für Ihre Computergruppen. In diesem Abschnitt wird Folgendes beschrieben:

- Die Standardrichtlinien und ob sie geändert werden müssen
- Erstellen und Ändern von Richtlinien
- Übertragen von Richtlinien auf Computergruppen

9.1 Standardrichtlinien

In diesem Abschnitt werden die Standardrichtlinien und empfohlene Anpassungen beschrieben. Empfohlene Richtlinieneinstellungen werden in der *Richtlinienanleitung zu Sophos Endpoint Security and Control* beschrieben.

9.1.1 Update-Richtlinie

Standardmäßig beziehen Computer ihre Updates von der Standardfreigabe, die auf dem Server erstellt wurde, auf dem der entsprechende Update Manager installiert ist.

Dies lässt sich jedoch auch anpassen:

- Sie können eine sekundäre Update-Quelle für Computer angeben, die nicht dauerhaft mit dem Unternehmensnetzwerk verbunden sind. Dies ist z.B. bei Laptops der Fall.
- Geben Sie die Adresse der Software an, die auf einem Webserver bereitgestellt wurde.

Wenn die Quelle für Software-Updates geändert werden soll, muss die Update-Richtlinie entsprechend angepasst werden. Dies können Sie jederzeit tun.

9.1.2 Antivirus- und HIPS-Richtlinie

Sophos Endpoint Security and Control verhält sich standardmäßig wie folgt:

- Der Zugriff auf Dateien, die mit Viren/Spyware infiziert sind, wird verweigert.
- Laufende Prozesse werden auf verdächtige Verhaltensmuster analysiert.
- Bei Erkennung eines Threats wird eine Benachrichtigung an Enterprise Console gesendet.

Dies lässt sich jedoch auch anpassen:

- On-Access-Scans für Exchange Server oder andere Server, deren Leistung beeinträchtigt werden könnte, lassen sich deaktivieren. Näheres hierzu entnehmen Sie bitte dem Support-Artikel 12421 (<http://www.sophos.de/support/knowledgebase/article/12421.html>) auf der Sophos Website.
- Verdächtiges Verhalten kann blockiert werden.
- Die Erkennung verdächtiger Dateien lässt sich aktivieren.

- Die Erkennung von Adware und potenziell unerwünschten Anwendungen lässt sich aktivieren.
- Die Erkennung von Threats in Webseiten kann aktiviert werden.

Diese Einstellungen müssen Sie in der Antivirus- und HIPS-Richtlinie manuell ändern. Dies können Sie jederzeit tun.

9.1.3 Application Control-Richtlinie

Application Control ist standardmäßig deaktiviert. Wenn Sie diese Funktion nutzen möchten, so muss die Application Control-Richtlinie manuell geändert werden. Dies können Sie jederzeit tun.

9.1.4 Firewall-Richtlinie

Standardmäßig blockiert Sophos Client Firewall alle unwichtigen Verbindungen. Um Netzwerkverbindungsprobleme zu verhindern, müssen Sie die Firewall-Richtlinie vor dem Schutz von Computern entsprechend anpassen.

9.1.5 NAC-Richtlinie

Standardmäßig wird Computern der Netzwerkzugriff gewährt. Wenn Sie diese Funktion nutzen möchten, so muss eine der NAC-Richtlinien manuell geändert und übertragen werden. Dies können Sie jederzeit tun.

9.1.6 Data Control-Richtlinie

Standardmäßig ist Data Control deaktiviert und es sind keine Regeln zur Überwachung oder Einschränkung der Übertragung von Dateien auf das Internet oder auf Speichermedien festgelegt. Wenn Sie diese Funktion nutzen möchten, so muss die Data Control-Richtlinie manuell geändert werden. Dies können Sie jederzeit tun.

9.1.7 Device Control-Richtlinie

Standardmäßig ist Device Control deaktiviert. Alle Geräte sind zugelassen. Wenn Sie diese Funktion nutzen möchten, so muss die Device Control-Richtlinie manuell geändert werden. Dies können Sie jederzeit tun.

9.2 Erstellen/Ändern einer Richtlinie

1. Wenn der Bereich **Richtlinien** nicht links unten im Fenster angezeigt wird, wählen Sie aus dem Menü **Ansicht** die Option **Endpoints**.
2. Führen Sie im Fenster **Richtlinien** einen der folgenden Schritte durch:
 - Um eine neue Richtlinie zu erstellen, rechtsklicken Sie auf den gewünschten Richtlinientyp (z.B. Update-Richtlinie) und wählen Sie **Richtlinie erstellen**.

- Um eine Standardrichtlinie zu ändern, doppelklicken Sie auf den gewünschten Richtlinientyp. Wählen Sie **Standard**.

Wenn Sie eine neue Richtlinie erstellt haben, wird der Liste eine **Neue Richtlinie** hinzugefügt und der Name hervorgehoben. Geben Sie der Richtlinie einen Namen.

3. Doppelklicken Sie auf die Richtlinie. Nehmen Sie nun die gewünschten Einstellungen vor.

Wenn Sie eine Richtlinie erstellt haben, muss sie auf eine Computergruppe übertragen werden.

9.3 Ändern einer NAC-Richtlinie

NAC-Richtlinien können nur über den browserbasierten NAC Manager geändert werden. Bis jetzt wird von Sophos nur der Internet Explorer unterstützt. Wenn Sie NAC Manager zum ersten Mal einsetzen, sind zunächst folgende Schritte erforderlich:

- Wenn es sich bei Ihrem Browser nicht um Internet Explorer 7.x handelt, nehmen Sie die Adresse des Servers mit NAC Manager in die Liste vertrauenswürdiger Websites auf.

- Deaktivieren Sie den Pop-up-Blocker.

1. Wenn der Bereich **Richtlinien** nicht links unten im Fenster angezeigt wird, wählen Sie aus dem Menü **Ansicht** die Option **Endpoints**.
2. Doppelklicken Sie im Bereich **Richtlinien** auf NAC. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.

Hinweis: Wenn die Adresse des Servers mit NAC Manager noch nicht erkannt oder angegeben wurde, werden Sie jetzt dazu aufgefordert.

NAC Manager wird in Ihrem Standard-Webbrowser geöffnet.

3. Sie können sich über ein beliebiges Konto anmelden.

Wenn Sie NAC Manager zum ersten Mal starten, geben Sie folgende Zugangsdaten ein:

- Account Name = admin
- Password = beliebiges Kennwort

Hinweis: Notieren Sie sich das Kennwort, denn bis Sie andere Benutzerkonten angelegt haben, können Sie NAC Manager nur über dieses Kennwort aufrufen.

4. Nehmen Sie auf der NAC Manager-Seite der zu ändernden Richtlinie die gewünschten Einstellungen vor.

Übertragen Sie die Richtlinie anschließend auf eine Computergruppe.

9.4 Übertragen einer Richtlinie

- ❖ Ziehen Sie eine Richtlinie aus dem Bereich **Richtlinien** auf die gewünschte Gruppe.

10 Suchen nach Computern

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

1. Wenn der Bereich **Gruppen** nicht links unten im Fenster angezeigt wird, wählen Sie aus dem Menü **Ansicht** die Option **Endpoints**.
2. Klicken Sie im Menü **Maßnahmen** auf die Option **Computer suchen**.
3. Wählen Sie die gewünschte Suchmethode aus.
4. Melden Sie sich an und wählen Sie ggf. einen Netzwerkpfad für die Suche aus.

Wenn Sie eine der **Suchoptionen** verwenden, werden die Computer in der Gruppe **Nicht zugewiesen** abgelegt.

11 Schützen von Windows- und Macintosh-Systemen

Folgende Schritte sind involviert:

- Vorbereitung
- Automatisches Schützen von Windows-Systemen
- Manuelles Schützen von Windows- oder Macintosh-Systemen

11.1 Vorbereitung

11.1.1 Entfernen von Fremdsoftware

Wenn der Sophos Installer andere installierte Sicherheitssoftware entfernen soll, gehen Sie folgendermaßen vor:

1. Wenn auf dem Computer Antivirensoftware von einem anderen Anbieter installiert ist, stellen Sie sicher, dass die Benutzeroberfläche der Virenschutzsoftware geschlossen ist.
2. Wenn auf Computern eine Firewall oder ein HIPS-Produkt anderer Hersteller ausgeführt wird, muss es deaktiviert oder dazu konfiguriert sein, dass das Sophos Installationsprogramm ausgeführt werden kann.

Falls auf Computern das Update-Tool anderer Hersteller läuft, sollten Sie es eventuell entfernen. Details zu diesem Thema entnehmen Sie bitte der *Hilfe* zu *Sophos Control Center*.

11.1.2 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 sollte folgende Voraussetzungen erfüllen:

- Lokale Administratorrechte für die zu schützenden Computer
- Anmeldung am Computer, auf dem Enterprise Console installiert wurde.
- Lesezugriff auf das Update-Verzeichnis, von dem die Computer ihre Updates beziehen. Doppelklicken Sie im Bereich **Richtlinien** auf **Update** und dann auf **Standard**, um dies zu überprüfen.

Hinweis: Wenn der Bereich **Richtlinien** nicht links unten im Fenster angezeigt wird, wählen Sie aus dem Menü **Ansicht** die Option **Endpoints**.

11.1.3 Vorbereiten der Installation der Virenschutzsoftware

Sie müssen nicht nur dafür sorgen, dass die allgemeinen Systemanforderungen erfüllt werden, es sind außerdem noch weitere Schritte notwendig, bevor auf den Computern Software automatisch installiert werden kann.

Bereiten Sie die Installation der Virenschutzsoftware vor:

1. Unter Windows 7/Vista:

- a) Öffnen Sie in Windows 7 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

- b) Öffnen Sie in Windows Vista in der Systemsteuerung das Netzwerk- und Freigabe-Center. Nehmen Sie die folgenden Einstellungen vor:

Netzwerkerkennung: Ein

Dateifreigabe: Ein

Druckerfreigabe: Ein

Kennwortgeschütztes Freigeben: Aus

- c) Der Remote-Registrierungsdienst muss gestartet werden und der Starttyp „Automatisch“ lauten. Dieser Dienst ist unter Windows 7/Vista standardmäßig nicht aktiv.

- d) Wählen Sie in Windows 7 für die Benutzerkontensteuerung die Option **Nie benachrichtigen** aus. Nach der Installation sollten Sie den **Standard** wiederherstellen.

- e) Schalten Sie in Windows Vista die Benutzerkontensteuerung ab. Nach der Installation sollten Sie sie wieder aktivieren.

- f) Deaktivieren Sie den Freigabeassistenten.

- g) Öffnen Sie die Windows-Firewall mit erweiterter Sicherheit. Öffnen Sie in der Systemsteuerung die **Verwaltung**. Stellen Sie sicher, dass **Eingehende Verbindungen** zugelassen werden.

- h) 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

2. Unter Windows 2003/XP Pro/2000/NT:
 - a) Die Dienste „Remoteregistrierung“, „Server“, „Computerbrowser“ und „Taskplaner“ müssen laufen.
 - b) Die C\$-Admin-Freigabe muss aktiviert sein.
 - c) „Einfache Dateifreigabe“ muss deaktiviert sein (nur XP).
3. Unter Windows XP SP2 und höher:
 - a) Die Dienste „Remoteregistrierung“, „Server“, „Computerbrowser“ und „Taskplaner“ müssen laufen.
 - b) Die C\$-Admin-Freigabe muss aktiviert sein.
 - c) „Einfache Dateifreigabe“ muss deaktiviert sein.
 - d) Aktivieren Sie die Datei- und Druckerfreigabe für Microsoft-Netzwerke.
 - e) Die TCP-Ports 8192, 8193 und 8194 müssen geöffnet sein.
 - f) Die Änderungen werden erst nach einem Neustart des Computers wirksam.

11.1.4 Vorbereiten der Installation von Compliance Agent

Bei Sophos Compliance Agent handelt es sich um eine Client-Komponente von NAC zur Konformitätsprüfung auf Arbeitsstationen. Compliance Agent wird installiert, wenn Windows-Computer geschützt werden.

Vor der Installation von Compliance Agent sind folgende Schritte erforderlich:

- ❖ Geben Sie die URL des Computers an, auf dem NAC Manager installiert wurde. Klicken Sie in Enterprise Console im Menü **Extras** auf **NAC URL konfigurieren**.

11.2 Automatisches Schützen von Windows-Computern

1. Wählen Sie die Computer aus, 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.

Ein Assistent leitet Sie durch die Installation der Sophos Sicherheitssoftware. Übernehmen Sie unter Beachtung der folgenden Ausnahmen die Voreinstellungen:

Aktivieren Sie auf der Seite **Funktionen auswählen** das Kontrollkästchen **Sophos Compliance Agent**, wenn Sie NAC nutzen möchten.

Im Abschnitt *Fehlersuche* (Seite 51) wird erläutert, wie in der **Schutz-Übersicht** angezeigte Fehler behoben werden können.

Geben Sie im Dialogfeld **Zugangsdaten** die Daten eines Kontos an, über das Software auf den Computern installiert werden kann.

Die gewählten Computer werden durch Sicherheitssoftware geschützt. 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, wird bei Zugriff auf Threats gescannt.

11.2.1 Fehlersuche

Wenn Sie Windows-Systeme automatisch schützen lassen, 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 [Manuelles Schützen von Windows- oder Macintosh-Computern](#) (Seite 51). Probleme mit anderen Betriebssystemen werden an anderer Stelle in diesem Handbuch behandelt.
- 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.
- Die „Einfache Dateifreigabe“ wurde auf Windows XP-Computern nicht deaktiviert.
- Der Freigabe-Assistent wurde auf Windows Vista-Computern nicht deaktiviert.
- Sie haben bei der Installation eine Funktion ausgewählt, die nicht auf diesem Betriebssystem unterstützt wird.

Wenn die Installation von Compliance Agent nicht durchgeführt werden kann oder ein Fehler auftritt, können Sie das Compliance Agent-Installationsprotokoll aufrufen. Das Protokoll befindet sich im Ordner %tmp%.

11.3 Manuelles Schützen von Windows- oder Macintosh-Computern

Wenn Sie über Computer verfügen, die nicht automatisch geschützt werden können, schützen Sie sie durch Ausführen des Installers in der Freigabe, in die Sicherheitssoftware heruntergeladen wurde („Bootstrap-Verzeichnis“).

Hierzu müssen Sie auf den zu schützenden Computern als Administrator angemeldet sein.

So können Sie Windows- oder Macintosh-Computer manuell schützen:

1. Das Bootstrap-Verzeichnis können Sie wie folgt ermitteln:
 - a) Klicken Sie in Enterprise Console 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 notwendigen Pfade.
2. Erstellen Sie auf dem Computer, auf dem das Bootstrap-Verzeichnis gehostet wird, ein Benutzerkonto mit Lesezugriff.

3. Suchen Sie auf allen Computern, die Sie schützen möchten, den Installer im Bootstrap-Verzeichnis und doppelklicken Sie darauf.

- Bei Windows-Computern heißt der Installer setup.exe.
- Bei Macintosh-Computern heißt der Installer Sophos Anti-Virus.mpkg.

Ein Assistent leitet Sie durch die Installation der Sophos Sicherheitssoftware. Übernehmen Sie unter Beachtung der folgenden Ausnahmen die Voreinstellungen:

Erstellen Sie auf der Seite mit den **Benutzerkonten-Details** die Daten des in Schritt 2 erstellten Kontos ein.

4. Führen Sie nach der Installation ein Update durch:
 - Rechtsklicken Sie auf Windows-Computern auf das Sophos-Symbol in der Symbolleiste und klicken Sie auf **Jetzt updaten**.
 - Klicken Sie bei einem Mac auf das Sophos Anti-Virus Symbol auf der rechten Seite der Menüleiste und wählen Sie anschließend die Option **Jetzt aktualisieren** aus dem Kurzbefehlmnü aus.

12 Schützen von Linux-Systemen

Zum Schutz von Linux-Systemen sind folgende Schritte erforderlich:

- Erstellen eines Installationspakets
- Installation von Sophos Anti-Virus auf Linux-Systemen

12.1 Erstellen eines Installationspakets

In diesem Abschnitt wird davon ausgegangen, dass Sie Sophos Anti-Virus heruntergeladen haben, wie weiter oben beschrieben.

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 die rechtliche Anmerkung.

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 Console 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.tgz 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. Wählen Sie die Verwaltung von Computern über Enterprise Console.
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.

12.2 Installieren von Sophos Anti-Virus über das Installationspaket

Über das Installationspaket können Sie Sophos Anti-Virus auf eine der folgenden Methoden installieren:

- Manuelle Installation auf jedem Computer. 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.

12.2.1 Manuelles Installieren von Sophos Anti-Virus

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.

12.2.2 Automatisches Installieren von Sophos Anti-Virus

- ❖ 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.

13 Schützen von NetWare-Servern

Führen Sie auf jedem NetWare-Server folgende Schritte aus:

- Installieren Sie Sophos Anti-Virus.
- Laden Sie Sophos Anti-Virus.

13.1 Installieren von Sophos Anti-Virus

In diesem Abschnitt wird davon ausgegangen, dass Sie auf jedem NetWare-Server ein zu schützendes Verzeichnis angelegt und Sophos Anti-Virus darin abgespeichert haben, wie weiter oben beschrieben.

Zur Installation von Sophos Anti-Virus führen Sie auf jedem NetWare-Server folgende Schritte durch:

1. Den Pfad zur Freigabe, in die Sophos Anti-Virus heruntergeladen wurde („Bootstrap-Verzeichnis“), können Sie wie folgt ermitteln:
 - a) Klicken Sie in Enterprise Console 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 auf einem Windows-Computer mit NetWare-Administratorsoftware mit Administratorenrechten auf dem NetWare-Server an.
3. Wechseln Sie in das Bootstrap-Verzeichnis.
4. Kopieren Sie alle Dateien aus diesem Verzeichnis nach `\\NetWare-Server\SYS\SWEET`

13.2 Laden von Sophos Anti-Virus

Führen Sie zum Laden von Sophos Anti-Virus die folgenden Schritte für alle NetWare-Server durch:

1. Führen Sie auf einem Windows-Computer, auf dem die NetWare-Administratorsoftware ausgeführt, folgende Schritte aus:
 - a) Fügen Sie das Standard-Installationsverzeichnis zum Suchpfad hinzu:
SEARCH
Die Anzahl der Zeichenketten im Suchpfad wird angezeigt. Geben Sie folgenden Befehl ein:
SEARCH ADD *nächste Zeichenkettensnummer* SYS:\SWEET\
Dabei ist die *nächste Zeichenkettensnummer* die Anzahl der Zeichenketten + 1.
 - b) Laden Sie Sophos Anti-Virus:
LOAD SWEET

Es empfiehlt sich, die genannten Befehle in der gleichen Reihenfolge in die Datei AUTOEXEC.NCF aufzunehmen. Auf diese Weise wird Sophos Anti-Virus beim jedem Server-Neustart neu gestartet.

Wenn Sie Sophos Anti-Virus zum ersten Mal laden, werden Sie zur Eingabe von Administratordaten aufgefordert.

2. Drücken Sie eine Taste.
3. Geben Sie den vollständigen Namen (fully qualified distinguished name) eines Administrators ein und drücken Sie die Eingabetaste.
4. Geben Sie das Administrator-Kennwort ein und drücken Sie die Eingabetaste.
Notieren Sie sich den vollständigen Namen des Administrators und das Kennwort (an einem sicheren Ort). Sophos Anti-Virus meldet sich nun bei jedem Start als Administrator an und kann so die vollständige eDirectory-Struktur sehen.

Das **Sophos Anti-Virus**-Fenster wird geöffnet.

Das Laden von Sophos Anti-Virus ist abgeschlossen. Sophos Anti-Virus wird ab jetzt bei jedem Update des Bootstrap-Verzeichnisses automatisch aktualisiert.

14 Schutz von UNIX-Systemen

Für UNIX-Systeme gibt es zwei Versionen von Sophos Anti-Virus für UNIX.

Sophos Anti-Virus Version 4

Diese Version weist folgende Merkmale auf:

- Unterstützung einer Vielzahl von Plattformen (siehe <http://www.sophos.de/products/all-sysreqs.html>).
- Die Verwaltung über Enterprise Console ist nicht möglich.
- Automatische Updates sind nicht möglich.
- Geplante Scans sind (abgesehen von der Verwendung des Befehls crontab) nicht möglich.

Der Schutz von UNIX-Systemen mit Version 4 wird im Abschnitt *Schützen von UNIX-Systemen mit Sophos Anti-Virus 4* (Seite 58) beschrieben.

Sophos Anti-Virus Version 7

Diese Version weist folgende Merkmale auf:

- Unterstützung einer kleinen Anzahl von Plattformen (siehe <http://www.sophos.de/products/all-sysreqs.html>).
- Die Verwaltung über Enterprise Console ist möglich.
- Automatische Updates sind möglich.
- Geplante Scans sind möglich.

Der Schutz von UNIX-Systemen mit Version 7 wird im Abschnitt *Schützen von UNIX-Systemen mit Sophos Anti-Virus 7* (Seite 60) beschrieben.

15 Schützen von UNIX-Systemen mit Sophos Anti-Virus 4

Folgende Schritte sind erforderlich:

- Bereitstellen von Sophos Anti-Virus für UNIX auf einem Webserver
- Installieren von Sophos Anti-Virus auf UNIX-Systemen

15.1 Freigeben von Sophos Anti-Virus in einem Webserver

In diesem Abschnitt wird davon ausgegangen, dass Sie Sophos Anti-Virus heruntergeladen haben, wie weiter oben beschrieben.

Sie müssen Sophos Anti-Virus in einem Webserver freigeben, damit Computer über HTTP darauf zugreifen können. Wenn Sie Sophos Anti-Virus bereits freigegeben haben, können Sie diesen Abschnitt überspringen.

So geben Sie Sophos Anti-Virus in einem Webserver frei:

1. Den Pfad zur Freigabe, in die Sophos Anti-Virus heruntergeladen wurde („Bootstrap-Verzeichnis“), können Sie wie folgt ermitteln:
 - a) Klicken Sie in Enterprise Console 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. Stellen Sie das Bootstrap-Verzeichnis, einschließlich der Unterordner, auf dem Webserver bereit.
3. Legen Sie Benutzernamen und Kennwörter zum Schutz vor unerlaubtem Zugriff auf den Ordner im Webserver fest.

Hinweis: Anweisungen zur Freigabe von Ordnern im Internet und zum Einrichten von Zugangsdaten entnehmen Sie bitte dem Begleitmaterial des Webservers. Wenden Sie sich bei weiteren Fragen bitte an Ihren Webserver-Betreiber.

Installieren Sie jetzt Sophos Anti-Virus.

15.2 Installieren von Sophos Anti-Virus

Zur Installation von Sophos Anti-Virus sind auf jedem UNIX-System folgende Schritte erforderlich:

1. Öffnen Sie das Stammverzeichnis (Root) des Bootstrap-Verzeichnisses des Webservers.
2. Kopieren Sie die Datei `emininstall.sh` in einen Pfad für ausführbare Dateien, z.B. `/etc`.
Im Folgenden wird dieses Verzeichnis als *Pfad* bezeichnet.

3. Geben Sie folgenden Befehl ein:

```
cd Pfad
```

4. Geben Sie folgenden Befehl ein:

```
chmod +x emininstall.sh
```

5. Erstellen Sie im Verzeichnis */etc* eine Datei namens *emininstall.conf*.

6. Öffnen Sie diese Datei in einem Editor und geben Sie folgende Zeilen ein:

```
EM install CID=Bootstrap-Verzeichnis  
EM cache dir=Cache-Pfad  
SAV install dir=Installationspfad
```

Hierbei gilt:

- *Bootstrap-Verzeichnis* ist das auf dem Webserver freigegebene Bootstrap-Verzeichnis.
- *Cache-Pfad* ist das Cache-Verzeichnis, in das beim Update-Vorgang die Installationsdateien kopiert werden.
- *Installationspfad* ist das Verzeichnis, in das Sophos Anti-Virus installiert wird.

Hinweis: Die Dateien im *Cache-Pfad* dürfen nicht gelöscht werden, da sie sonst erneut heruntergeladen werden. Aus diesem Grund sollten Sie die Dateien nicht im */tmp*-Verzeichnis ablegen, das gelegentlich vom UNIX-System gelöscht wird.

7. Starten Sie

```
emininstall.sh
```

Die Installation von Sophos Anti-Virus ist hiermit abgeschlossen.

8. Erstellen Sie einen Cron-Job, um *emininstall.sh* in regelmäßigen Abständen auszuführen. Daraufhin sucht die Datei nach Updates und installiert sie automatisch. Näheres zur Erstellung eines Cron-Jobs entnehmen Sie bitte dem Support-Artikel 12176 (<http://www.sophos.de/support/knowledgebase/article/12176.html>) auf der Sophos Website.

16 Schützen von UNIX-Systemen mit Sophos Anti-Virus 7

Die Installation ist auf eine der folgenden Methoden möglich:

- Installationspaket
- Tarball

16.1 Schützen von UNIX-Systemen über ein Installationspaket

Zum Schützen von UNIX-Systemen über ein Installationspaket sind folgende Schritte erforderlich:

- Erstmalige manuelle Installation von Sophos Anti-Virus auf einem UNIX-Server
- Erstellen eines Installationspakets
- Installieren von Sophos Anti-Virus auf den restlichen UNIX-Systemen

16.1.1 Manuelle Erstinstallation von Sophos Anti-Virus

In diesem Abschnitt wird davon ausgegangen, dass Sie Sophos Anti-Virus heruntergeladen haben, wie weiter oben beschrieben.

Wenn Sophos Anti-Virus, Version 4, auf dem UNIX-Server installiert wurde und Sie ein Upgrade auf Version 7 durchführen möchten, muss Version 4 zunächst deinstalliert werden. Entsprechende Anweisungen entnehmen Sie bitte der *Startup-Anleitung zu Sophos Anti-Virus für UNIX*, Version 4.

1. Den Pfad zur Freigabe, in die Sophos Anti-Virus heruntergeladen wurde („Bootstrap-Verzeichnis“), können Sie wie folgt ermitteln:
 - a) Klicken Sie in Enterprise Console 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 UNIX-Server als „root“ an.
3. Mounten Sie das Bootstrap-Verzeichnis.
4. Ändern Sie das Bootstrap-Verzeichnis.
5. Führen Sie das Installationsskript aus:

```
./install.sh
```

Aktivieren Sie Remote-Management.
Nach dem Update wird der UNIX-Server in Enterprise Console in der Gruppe **Nicht zugewiesen** aufgeführt.
6. Erstellen Sie in Enterprise Console ggf. eine neue Gruppe für den UNIX-Server.

7. Ziehen Sie den Server aus der Gruppe **Nicht zugewiesen** in diese Gruppe.
8. Standardmäßig ist der Gruppe bereits die Standard-Update-Richtlinie zugewiesen. Anweisungen zum Ändern der Richtlinie können Sie bei Bedarf der *Hilfe zu Enterprise Console* entnehmen.
9. Geben Sie auf dem UNIX-Server folgenden Befehl ein, um das erste Update durchzuführen:

```
/opt/sophos-av/bin/savupdate
```

Der nächste Schritt ist die Erstellung eines Installationspakets.

16.1.2 Erstellen eines Installationspakets

Mithilfe des Skripts **mkinstpkg** können Sie ein Distributionspaket für Ihre Benutzer erstellen. Das Skript benötigt Informationen darüber, wie Sophos Anti-Virus auf Ihren UNIX-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 erstellen.

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

So erstellen Sie ein Installationspaket:

1. Wechseln Sie auf dem UNIX-Server mit Sophos Anti-Virus in das Verzeichnis

```
/opt/sophosav/update/cache/Primary-unpacked.
```
2. Um ein Installationspaket in Form eines tar-Archivs namens `savinstpkg.tar` zu erstellen, geben Sie Folgendes ein:

```
./mkinstpkg.sh
```
3. Wählen Sie die Verwaltung von Computern über Enterprise Console.
4. Geben Sie als Speicherort den freigegebenen Ordner an (aus Sicht eines UNIX-Systems).

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

16.1.3 Installieren von Sophos Anti-Virus über das Installationspaket

Über das Installationspaket können Sie Sophos Anti-Virus auf eine der folgenden Methoden installieren:

- Manuelle Installation auf jedem Computer.
- Automatische Installation im gesamten Netzwerk.

16.1.3.1 Manuelles Installieren von Sophos Anti-Virus

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 -xvf savinstpkg.tar
./sophos-av/install.sh
```

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.

16.1.3.2 Automatisches Installieren von Sophos Anti-Virus

- ❖ 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.

16.2 Schützen von UNIX-Systemen über Tarball

16.2.1 Herunterladen des Sophos Anti-Virus-Tarballs

1. Fahren Sie mit den Anweisungen im Abschnitt <http://www.sophos.de/support/updates/> fort.
2. Geben Sie Ihre MySophos-Zugangsdaten ein.
3. Rufen Sie die Webseite für Sophos Anti-Virus für UNIX-Downloads auf und laden Sie den Sophos Anti-Virus für UNIX-Tarball herunter.
4. Der Tarball muss in einem Verzeichnis gespeichert werden, auf das die zu schützenden UNIX-Computer zugreifen können.
Sie können den Installer auch auf eine CD oder DVD brennen.

16.2.2 Installieren von Sophos Anti-Virus über Tarball

Es wird davon ausgegangen, dass Sie den Tarball und Sophos Anti-Virus in eine Freigabe heruntergeladen haben (Anweisungen siehe oben).

Wenn Sophos Anti-Virus, Version 4, auf dem UNIX-Computer installiert wurde und Sie ein Upgrade auf Version 7 durchführen möchten, muss Version 4 zunächst deinstalliert werden. Entsprechende Anweisungen entnehmen Sie bitte der *Startup-Anleitung zu Sophos Anti-Virus für UNIX*, Version 4.

1. Den Pfad zur Freigabe, in die Sophos Anti-Virus heruntergeladen wurde („Bootstrap-Verzeichnis“), können Sie wie folgt ermitteln:
 - a) Klicken Sie in Enterprise Console 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 UNIX-Computer als „root“ an.
3. Entpacken Sie den im Vorfeld heruntergeladenen Tarball:

```
tar -xvf tarball
```

4. Führen Sie das Installationsskript aus:

```
./sophos-av/install.sh
```

Wenn Sie zur Angabe eines Update-Verzeichnisses aufgefordert werden, geben Sie die Adresse des Bootstrap-Verzeichnisses an.

5. Leiten Sie das erste Update folgendermaßen ein:

```
/opt/sophos-av/bin/savupdate
```

Nach dem Update befindet sich der UNIX-Computer in Enterprise Console in der Gruppe **Nicht zugewiesen**.

6. Erstellen Sie in Enterprise Console ggf. eine neue Gruppe für den UNIX-Computer.
7. Ziehen Sie den Computer aus der Gruppe **Nicht zugewiesen** in diese Gruppe.
8. Standardmäßig wurde der Gruppe die Standard-Update-Richtlinie zugewiesen. Anweisungen zum Ändern der Richtlinie können Sie bei Bedarf der *Hilfe zu Enterprise Console* entnehmen.

Der UNIX-Computer ist nun geschützt. Sophos Anti-Virus wird ab jetzt bei jedem Update des Bootstrap-Verzeichnisses automatisch aktualisiert. Wiederholen Sie die Schritte 2 bis 8 für alle UNIX-Computer, die geschützt werden sollen.

17 Überprüfen der Netzwerkintegrität

So überprüfen Sie die Netzwerkintegrität über Enterprise Console:

1. Öffnen Sie das Dashboard.

Wenn es nicht angezeigt wird, wählen Sie aus dem Menü **Ansicht** die Option **Dashboard**.

Im Dashboard wird angezeigt, wie viele Computer

- Bedrohungen erkannt haben.
- nicht auf dem neuesten Stand sind
- nicht mit Richtlinien übereinstimmen.

2. Mit NAC können Sie außerdem überprüfen, ob Computer mit der NAC-Richtlinie übereinstimmen:

a) Wählen Sie aus dem Menü **Extras** die Option **NAC-Verwaltung**.

b) Klicken Sie in NAC Manager im Menü **Report** auf **Compliance**.

18 Schützen von Einzelplatzrechnern

Einige Computer sind nicht in ein Netzwerk integriert und der Zugriff auf sie ist nicht einfach. Es kann sich z.B. um Computer handeln, die von Mitarbeitern zu Hause verwendet werden. Um diese Computer zu schützen, muss jeder Benutzer die Sophos Sicherheitssoftware manuell mithilfe des Installationsprogramms für Einzelplatzrechner auf seinem Computer installieren. Die Software wird dann über Updates aus dem Internet stets auf dem neuesten Stand gehalten. Es gibt drei mögliche Vorgehensweisen:

- Der Benutzer kann die Software von Sophos herunterladen. Danach wird sie automatisch von dort aus aktualisiert. Siehe Support-Artikel 41141 (<http://www.sophos.de/support/knowledgebase/article/41141.html>) auf der Sophos Website.
- Sie können die Software und alle nachfolgenden Updates auf Ihrer eigenen Website bereitstellen. Der Benutzer lädt die Software und Updates von dort herunter. Weitere Informationen zur Bereitstellung von Sophos Updates auf Ihrer Website finden Sie im Support-Artikel 12134 (<http://www.sophos.de/support/knowledgebase/article/12134.html>).
- Sie können die Software auf eine CD brennen und an Ihre Benutzer senden. Der Benutzer kann nun die Software installieren und sie so einrichten, dass sie Updates von dem von Ihnen gewünschten Standort bezieht. Siehe Support-Artikel 13093 (<http://www.sophos.de/support/knowledgebase/article/13093.html>) auf der Sophos Website.

18.1 Informationen für Einzelplatzbenutzer

Senden Sie allen Benutzern, die nicht mit dem Netzwerk verbunden sind, Folgendes:

- Das Verzeichnis, von dem aus Sicherheitssoftware heruntergeladen werden kann (wenn nicht auf der CD bereitgestellt).
- Die *Sophos Endpoint Security and Control Einzelplatz-Startup-Anleitung*.
- Den erforderlichen Benutzernamen und das Kennwort (sowohl für den Download direkt von Sophos als auch für den Download von Ihrer Website).

Beachten Sie beim Übermitteln der Zugangsdaten bitte die folgenden Hinweise:

- Senden Sie die Zugangsdaten nicht per E-Mail an einen infizierten Computer, da sie gestohlen werden könnten.
- Falls notwendig, senden Sie die Zugangsdaten per Fax oder Post.

19 Technischer Support

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

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

- Die Versionsnummer(n) Ihrer Sophos Software
- Betriebssystem(e) und Patch Level
- Den genauen Wortlaut von Fehlermeldungen (falls zutreffend)

20 Copyright

Copyright © 2009 Sophos Group. Alle Rechte vorbehalten. Diese Publikation darf weder elektronisch oder mechanisch reproduziert, elektronisch gespeichert oder übertragen, noch fotokopiert oder aufgenommen werden, es sei denn, Sie verfügen entweder über eine gültige Lizenz, gemäß der die Dokumentation in Übereinstimmung mit dem Lizenzvertrag reproduziert werden darf, oder Sie verfügen über eine schriftliche Genehmigung des Urheberrechtsinhabers.

Sophos und Sophos Anti-Virus sind eingetragene Marken von Sophos Plc und der Sophos Group. 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.com 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>

ACE™, TAO™, CIAO™, and CoSMIC™

ACE¹, TAO², CIAO³, and CoSMIC⁴ (henceforth referred to as “DOC software”) are copyrighted by Douglas C. Schmidt⁵ and his research group⁶ at Washington University⁷, University of California⁸, Irvine, and Vanderbilt University⁹, Copyright © 1993–2005, all rights reserved.

Since DOC software is open-source¹⁰, 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 us¹¹ know so we can promote your project in the DOC software success stories¹².

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 companies¹³ 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 ACE¹⁴, TAO¹⁵, CIAO¹⁶, and CoSMIC¹⁷ web sites are maintained by the DOC Group¹⁸ at the Institute for Software Integrated Systems (ISIS)¹⁹ and the Center for Distributed Object Computing of Washington University, St. Louis²⁰ for the development of open-source software as part of the open-source software community²¹. 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 me²² know.

Douglas C. Schmidt²³

The ACE home page is <http://www.cs.wustl.edu/ACE.html>

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. <http://www.the-it-resource.com/Open-Source/Licenses.html>
11. mailto:doc_group@cs.wustl.edu
12. <http://www.cs.wustl.edu/~schmidt/ACE-users.html>
13. <http://www.cs.wustl.edu/~schmidt/commercial-support.html>
14. <http://www.cs.wustl.edu/~schmidt/ACE.html>
15. <http://www.cs.wustl.edu/~schmidt/TAO.html>
16. <http://www.dre.vanderbilt.edu/CIAO/>

17. <http://www.dre.vanderbilt.edu/cosmic/>
18. <http://www.dre.vanderbilt.edu/>
19. <http://www.isis.vanderbilt.edu/>
20. <http://www.cs.wustl.edu/~schmidt/doc-center.html>
21. <http://www.opensource.org/>
22. <mailto:d.schmidt@vanderbilt.edu>
23. <http://www.dre.vanderbilt.edu/~schmidt/>

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.

OpenSSL-Lizenz

Copyright © 1998–2006 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.
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 licence 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 licence [including the GNU Public Licence.]

iMatix SFL

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