

# SOPHOS

## Sophos Endpoint Security and Control 9.5 Erweiterte Upgrade-Anleitung

Stand: Juni 2010



# Inhalt

1	Einleitung.....	3
2	Überprüfen der Richtlinieneinstellungen.....	4
3	Upgrade der Sicherheitssoftware auf Endpoints.....	5
4	Konfigurieren der neuen Funktionen.....	10
5	Upgrade von Compliance Dissolvable Agent.....	11
6	Migration von EM Library nach Update Manager.....	12
7	Technischer Support.....	28
8	Rechtlicher Hinweis.....	29

# 1 Einleitung

**Wichtig:** Es wird davon ausgegangen, dass Enterprise Console und NAC Manager bereits upgegradet wurden.

Informationen zum Upgrade von Enterprise Console und NAC Manager finden Sie im **Endpoint Security and Control 9.5 Upgrade Center** unter <http://www.sophos.de/support/upgrades/>.

In dieser Anleitung wird das Upgrade der restlichen Komponenten von Endpoint Security and Control 9.5 erläutert.

## 2 Überprüfen der Richtlinieneinstellungen

**Wichtig:** In diesem Abschnitt wird davon ausgegangen, dass Enterprise Console und NAC Manager bereits upgegradet wurden.

Nach dem Upgrade von Enterprise Console und NAC Manager sollten Sie überprüfen, ob die Richtlinieneinstellungen beibehalten wurden.

Folgende Schritte sind erforderlich:

- Überprüfen Sie die Einstellungen auf ihre Richtigkeit.
- Stellen Sie sicher, dass den Gruppen die richtigen Richtlinien zugewiesen wurden.
  1. Doppelklicken Sie im Feld **Richtlinien** auf einen Richtlinientyp, z.B. **Antivirus und HIPS**. Doppelklicken Sie dann auf die gewünschte Richtlinie, um sie anzuzeigen.
  2. Sehen Sie sich die Einstellungen in folgendem Fenster an.

Die Richtlinieneinstellungen werden ausführlich in der *Hilfe zu Sophos Enterprise Console* behandelt.
  3. Um sicherzugehen, dass jeder Gruppe die richtigen Richtlinien zugewiesen wurden, rechtsklicken Sie im Fenster **Gruppen** auf eine Gruppe. Das Kontextmenü wird aufgerufen. Wählen Sie **Gruppenrichtliniendetails**.
  4. Überprüfen Sie im Dialogfeld **Gruppendetails**, ob die Gruppe den richtigen Richtlinien zugewiesen wurde. Ist dies nicht der Fall, wählen Sie für einen Richtlinientyp eine andere Richtlinie aus der Dropdown-Liste und bestätigen Sie die Auswahl.

Anweisungen zum Konfigurieren neuer Richtlinieneinstellungen für Windows 2000 oder höher finden Sie unter [Konfigurieren der neuen Funktionen](#) (Seite 10).

## 3 Upgrade der Sicherheitssoftware auf Endpoints

**Wichtig:** In diesem Abschnitt wird davon ausgegangen, dass Enterprise Console und NAC Manager bereits upgegradet wurden.

Zum Upgrade der Windows-Endpoints und optimalen Nutzung der neuen Funktionen müssen Sie die Softwareversion, anhand derer die Computer auf dem neuesten Stand gehalten wird, in Sophos Endpoint Security and Control 9.5 ändern.

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

In dieser Version wurde nur Endpoint-Software für Windows geändert.

**Hinweis:** Wenn Sie eine feste Version von Sophos Endpoint Security and Control und Compliance Agent für NAC abonniert haben, können Sie diese auf Wunsch weiterhin nutzen. Wenn diese Versionen nicht mehr von Sophos unterstützt werden, werden Ihre Computer automatisch upgegradet, wenn Sie die Option **Nicht mehr unterstützte Abonnements einer bestimmten Version automatisch updaten** im Dialogfeld **Software-Abonnement** ausgewählt haben.

### 3.1 Abonnieren der neuen Endpoint-Software

Zum Abonnieren neuer Software gibt es zwei Möglichkeiten:

- Erstellen neuer Software-Abonnements
- Anpassen der vorhandenen Software-Abonnements

#### Erstellen neuer Software-Abonnements

Wenn Sie die neue Software auf einer kleinen Computergruppe vor der Einführung im Netzwerk testen möchten, empfiehlt sich das Erstellen eines neuen Abonnements.

Führen Sie nach der Erstellung des neuen Abonnements die folgenden Schritte aus:

- Einrichten des Software-Downloads und der Bereitstellung der Software in Netzwerkfreigaben, über die die Endpoints ihre Updates beziehen.
- Erstellen neuer Update-Richtlinien, die sich auf das neue Abonnement beziehen und auf die Update-Freigaben verweisen, die im Update Manager festgelegt wurden.
- Zuweisen der neuen Update-Richtlinie an die gewünschten Endpoints.

**Wichtig:** Führen Sie kein Upgrade von Sophos Endpoint Security and Control 9.5 auf Computern mit Windows 2000 SP3 und abwärts durch. Die Software wird erst ab Windows 2000 mit SP4 unterstützt.

#### Anpassen vorhandener Software-Abonnements

Wenn Sie ein vorhandenes Abonnement um eine neue Software-Version erweitern, ist keine weitere Konfiguration erforderlich. Der Update Manager ist bereits für die Verwaltung des Abonnements und die Verteilung der Software an Update-Freigaben im Netzwerk ausgelegt. Sie verfügen bereits über Update-Richtlinien in Bezug auf das entsprechende Abonnement

und auf die betreffenden Endpoints. Die Endpoints werden automatisch auf die neue Version upgegradet.

### 3.1.1 Erstellen eines neuen Software-Abonnements

So erstellen Sie ein neues Software-Abonnement:

1. Klicken Sie in Enterprise Console im Menü **Ansicht** auf **Update Manager**.
2. Klicken Sie oben im Bereich **Software-Abonnements** auf **Hinzufügen**, um ein neues Abonnement einzurichten.

Das Dialogfenster **Software-Abonnements** wird angezeigt.

Wenn Sie eine Kopie eines vorhandenen Abonnements anlegen möchten, rechtsklicken Sie auf das Abonnement und wählen Sie **Abonnement duplizieren**. Geben Sie dem Abonnement einen neuen Namen und doppelklicken Sie darauf. Das Dialogfeld **Software-Abonnement** wird geöffnet.

3. Im Dialogfeld **Software-Abonnements** können Sie auf Wunsch den Namen des Abonnements ändern.
4. Klicken Sie neben Windows 2000 oder aufwärts auf das Feld **Version** und klicken Sie noch einmal.

Die vorhandenen Versionen werden in einer Dropdown-Liste angezeigt.

5. Wählen Sie das gewünschte Update für Version 9.5 von Sophos Endpoint Security and Control.

In der Regel bietet sich die Option **Empfohlen** an, da so sichergestellt wird, dass Software automatisch auf dem neuesten Stand gehalten wird. Im Abschnitt [Update-Arten](#) (Seite 22) können Sie sich über die unterschiedlichen Update-Arten informieren.

**Wichtig:** Wenn Sie eine feste Version auswählen, z.B. 9.5.1, empfiehlt sich die Auswahl der Option **Nicht mehr unterstützte Abonnements einer bestimmten Version automatisch updaten**. Wenn Sie nicht unterstützte Software nutzen, sind Ihre Computer vor neuen Threats nicht hinreichend geschützt.

Konfigurieren Sie den Update Manager nach dem Erstellen des neuen Software-Abonnements, damit er wie unter [Hinzufügen eines Abonnements im Update Manager](#) (Seite 7) erläutert verwaltet wird.

Bei Bedarf können Sie anschließend E-Mail-Benachrichtigungen für Ihr Abonnement einrichten. Die Einrichtung von E-Mail-Benachrichtigungen zu Abonnements wird in der [Hilfe](#) zu *Sophos Enterprise Console* im Abschnitt „Alerts“ eingehend beschrieben.

### 3.1.2 Ändern eines Software-Abonnements

So richten Sie in einem vorhandenen Software-Abonnement neue Software-Downloads ein:

1. Klicken Sie in Enterprise Console im Menü **Ansicht** auf **Update Manager**.
2. Doppelklicken Sie im Feld **Software-Abonnements** auf das zu ändernde Abonnement.

Das Dialogfenster **Software-Abonnements** wird angezeigt.

3. Klicken Sie neben Windows 2000 und aufwärts auf das Feld **Version** und klicken Sie noch einmal.

Die vorhandenen Versionen werden in einer Dropdown-Liste angezeigt.

4. Wählen Sie das gewünschte Update für Version 9.5 von Sophos Endpoint Security and Control.

In der Regel bietet sich die Option **Empfohlen** an, da so sichergestellt wird, dass Software automatisch auf dem neuesten Stand gehalten wird. Im Abschnitt [Update-Arten](#) (Seite 22) können Sie sich über die unterschiedlichen Update-Arten informieren.

**Wichtig:** Wenn Sie eine feste Version auswählen, z.B. 9.5.1, empfiehlt sich die Auswahl der Option **Nicht mehr unterstützte Abonnements einer bestimmten Version automatisch updaten**. Wenn Sie nicht unterstützte Software nutzen, sind Ihre Computer vor neuen Threats nicht sicher.

Die neue Version wird gemäß dem Zeitplan des Update Managers heruntergeladen. Die Endpoints werden beim nächsten Abruf von Updates auf die neue Version upgedatet.

Wenn die neue Version sofort heruntergeladen werden soll, rechtsklicken Sie in der Ansicht **Update Manager** auf den Update Manager mit dem geänderten Abonnement und wählen Sie **Jetzt updaten**.

Wenn Sie Computer sofort upgraden möchten, warten Sie, bis der Update Manager den Software-Download fertiggestellt hat. (Sehen Sie in der Ansicht **Update Manager** in der Spalte **Download-Status** neben dem Update Manager nach.) Rechtsklicken Sie in der Ansicht **Endpoints** auf die Computer in der Computerliste oder im Bereich **Gruppen** auf eine Computergruppe und wählen Sie **Jetzt updaten**.

## 3.2 Hinzufügen eines Abonnements im Update Manager

Wenn Sie ein neues Abonnement für die neue Softwareversion erstellt haben, konfigurieren Sie den Update Manager zur Verwaltung des Abonnements.

1. Wählen Sie den Update Manager in der Ansicht **Update Manager** aus, rechtsklicken Sie darauf und klicken Sie auf **Konfiguration öffnen/ändern**.
2. Wählen Sie im Dialogfeld **Update Manager konfigurieren** auf der Registerkarte **Abonnements** das Software-Abonnement aus der Liste der verfügbaren Abonnements aus. Details zum Abonnement (z.B. vom Abonnement erfasste Software) können Sie per Klick auf **Details** aufrufen.
3. Klicken Sie zum Verschieben des gewählten Abonnements in die Liste „Abonniert für“ auf die Schaltfläche „Hinzufügen“.

Standardmäßig wird Software in der folgenden Freigabe abgelegt:

\\<ComputerName>\SophosUpdate. ComputerName steht dabei für den Namen des Computers, auf dem der Update Manager installiert wurde. Anhand der Anweisungen im Abschnitt [Festlegen des Download-Verzeichnisses](#) (Seite 25) können Sie weitere Freigaben hinzufügen.

Wenn Sie die neue Version sofort heruntergeladen möchten, wählen Sie den Update Manager aus, rechtsklicken Sie darauf und wählen Sie die Option **Jetzt updaten** im Kontextmenü aus.

### 3.3 Konfigurieren von Update-Richtlinien

Wenn Sie ein neues Software-Abonnement erstellt haben und den Update Manager zur Verwaltung des Abonnements konfiguriert haben, konfigurieren Sie Update-Richtlinien zum Updaten der Computer mit der im Abonnement festgelegten Software.

Führen Sie einen der folgenden Schritte durch:

- Ändern Sie Ihre vorhandene(n) Update-Richtlinie(n) so ab, dass sie sich auf das neue Abonnement beziehen.

Bei der nächsten Update-Prüfung wird ein Endpoint-Upgrade auf die neue Version durchgeführt.

- Erstellen Sie neue Update-Richtlinien.

Übertragen Sie dann die neuen Richtlinien auf die Endpoints, um ein Upgrade darauf durchzuführen und die Endpoints auf dem neuesten Stand zu halten.

1. Öffnen Sie zum Erstellen einer neuen Update-Richtlinie in der Ansicht **Endpoints** das Fenster **Richtlinien**, rechtsklicken Sie auf **Update** und wählen Sie die Option **Richtlinie erstellen** aus.

Eine „Neue Richtlinie“, deren Name markiert ist, wird zur Liste hinzugefügt.

2. Geben Sie der Richtlinie einen neuen Namen.
3. Doppelklicken Sie auf die Richtlinie, um sie zu ändern.
4. Rufen Sie im Dialogfeld **Update-Richtlinie** die Registerkarte **Abonnements** auf und wählen Sie das Abonnement der Software aus, die auf dem neuesten Stand gehalten werden soll.
5. Ändern Sie gegebenenfalls weitere Einstellungen. Weitere Informationen finden Sie unter [Erstellen neuer Update-Richtlinien](#) (Seite 26).

Wenn Sie eine neue Update-Richtlinie erstellt haben, weisen Sie sie anhand der Anweisungen im folgenden Abschnitt einer oder mehreren Endpointgruppe(n), um diese upzugraden.

### 3.4 Upgrade von Sicherheitssoftware auf Windows-Computern

**Wichtig:** Führen Sie kein Upgrade auf Sophos Endpoint Security and Control 9.5 auf Computern mit Windows 2000 SP3 und abwärts durch. Die Software wird erst ab Windows 2000 mit SP4 unterstützt.

So können Sie einer Computergruppe eine neue Update-Richtlinie zuweisen:

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

Sie können auch auf eine Gruppe rechtsklicken und die Option **Gruppenrichtliniendetails ansehen** wählen. Anschließend können Sie Richtlinien für die Gruppe aus den Dropdown-Menüs auswählen.

Beim nächsten Computer-Update wird das Upgrade auf Sophos Endpoint Security and Control 9.5 durchgeführt.

**Hinweis:** Wenn Computer auf Sophos Endpoint Security and Control 9.5 upgegradet werden, werden die Computerdetails in der Computerliste von Enterprise Console in der Spalte **Richtlinienkonformität** unter Umständen als „Abweichend von Richtlinie“ ausgewiesen. Dieses Problem können Sie beheben, indem Sie auf die Computer rechtsklicken und die Option **Konformität mit** wählen und anschließend die erforderliche(n) Richtlinie(n) auswählen.

## 4 Konfigurieren der neuen Funktionen

### Live-Schutz

Mit dieser Funktion lässt sich über ein "In-the-Cloud"-Verfahren sofort feststellen, ob eine Datei eine Bedrohung darstellt. Bei Bedarf werden umgehend die in der Schutzkonfiguration der Antivirensoftware festgelegten Maßnahmen ergriffen.

Nähere Informationen zu dieser neuen Funktion entnehmen Sie bitte dem Abschnitt „Konfigurieren der Anti-Virus- und HIPS-Richtlinie“ in der *Hilfe zu Sophos Enterprise Console*.

### Web-Schutz

Diese Funktion bietet mehr Sicherheit vor Threats im Internet: Der Web-Schutz unterbindet den Zugriff auf Seiten, die bekanntermaßen Malware hosten.

Nähere Informationen zum Web-Schutz und dessen Einrichtung entnehmen Sie bitte dem Abschnitt „Konfigurieren der Anti-Virus- und HIPS-Richtlinie in der *Hilfe zu Sophos Enterprise Console*.

### Manipulationsschutz

Mit dem Manipulationsschutz können Sie verhindern, dass nicht autorisierte Benutzer sowie bekannte Malware Sophos Sicherheitssoftware deinstallieren.

Näheres zur Einrichtung des Manipulationsschutzes erfahren Sie in der *Hilfe zu Sophos Enterprise Console* im Abschnitt „Konfigurieren der Manipulationsschutz-Richtlinie“.

## 5 Upgrade von Compliance Dissolvable Agent

**Wichtig:** In diesem Abschnitt wird davon ausgegangen, dass Enterprise Console und NAC Manager bereits upgegradet wurden.

Compliance Dissolvable Agent ist für Benutzer (z.B. Geschäftspartner oder Gastbenutzer) bestimmt, auf deren Endpoints Compliance Agent nicht installiert wurde oder installiert werden konnte .

Weitere Informationen zu Dissolvable Agent finden Sie in der *Konfigurationsanleitung zu Sophos Compliance Agent, Version 3.5*. Sie finden die Anleitung sowie sonstige Sophos Dokumentation unter <http://www.sophos.de/support/docs/>.

Verfahren Sie zum Upgrade von Compliance Dissolvable Agent von Version 3.3 auf Version 3.5 wie folgt:

1. Rufen Sie <http://www.sophos.de/support/updates/> auf.
2. Geben Sie Ihre MySophos-Zugangsdaten ein.
3. Laden Sie auf der Download-Seite zu Endpoint Security and Control den Installer für Sophos NAC Compliance Dissolvable Agent, Version 3.5 herunter.
4. Starten Sie den Installer für Sophos NAC Compliance Dissolvable Agent, Version 3.5.
5. Es wird ein Assistent gestartet, der Sie durch die Installation leitet. Übernehmen Sie unter Beachtung der folgenden Ausnahmen die Voreinstellungen:
6. Sie können das Standardinstallationsverzeichnis **C:\Programme\Sophos\Sophos Dissolvable Agent** übernehmen oder per Klick auf **Ändern** das gewünschte Installationsverzeichnis auswählen.
7. Geben Sie die IP-Adresse des Sophos NAC-Servers oder den DNS-Namen ein.  
Wenn Sophos NAC auf mehreren Servern installiert wurde, ist die Serveradresse die IP-Adresse bzw. der DNS-Name des NAC Manager-Servers – nicht des NAC-Datenbankservers.  
Wenn die Sophos NAC-Serveradresse nach der Installation von Dissolvable Agent geändert wird, muss Dissolvable Agent nochmals auf dem Webserver installiert und dabei die neue Serveradresse angegeben werden.
8. Wenn Sie HTTPS mit NAC verwenden, aktivieren Sie das Kontrollkästchen **Secure Sophos Server (use HTTPS)**.

### Hinweise

- Wenn Installationsfehler auftreten, suchen Sie im Ereignisprotokoll des Webserver nach Anhaltspunkten.
- Wenn Dissolvable Agent im Standardverzeichnis installiert wird, können Endpoints über folgende URL darauf zugreifen: `http(s)://<IP address/DNS name>/dissolvableagent`. Die IP-Adresse oder der DNS-Name gibt den Webserver an, auf dem Dissolvable Agent installiert wurde.

## 6 Migration von EM Library nach Update Manager

Wenn Sie **EM Library** noch nutzen, empfiehlt sich, auf **Update Manager** umzusteigen. Die aktuelle Sicherheitssoftware für Endpoints kann nicht mit **EM Library** heruntergeladen werden. Wenn Sie etwa Computer mit Windows 7 oder Windows 2008 schützen möchten, müssen Sie **Sophos Endpoint Security and Control** für diese Betriebssysteme mit **Update Manager** herunterladen.

Beim Upgrade von **Enterprise Console** 4.0 auf Version 4.5 werden die Einstellungen von **EM Library** sowie die alten Update-Richtlinien nämlich nicht geändert.

- Wenn EM Library (die Updates von Sophos bezieht) und Enterprise Console auf verschiedenen Computern installiert sind, müssen Sie Sophos Update Manager auf dem Remote-Computer installieren, auf dem sich EM Library befindet, und die Update-Einstellungen von dort migrieren, wie in diesem Kapitel erläutert wird
- Wenn Sie EM Library weiterhin nutzen und sich die Software auf dem Management-Server von Enterprise Console befindet, müssen Sie die alten Update-Einstellungen manuell für Update Manager übernehmen. Anweisungen hierzu finden Sie unter *Update-Einstellungen wurden nicht auf Sophos Update Manager migriert* (Seite 21).

### 6.1 Überblick über die wichtigsten Migrationsschritte

Im Folgenden wird die im Rahmen der Installation stattfindende Migration eingehend erläutert. Enterprise Console Management Server und EM Library sind dabei auf verschiedenen Computern installiert.

In diesem Abschnitt wird davon ausgegangen, dass Sie den **Software-Download-Assistenten** abgebrochen haben und der Update Manager, der zusammen mit Enterprise Console auf demselben Computer installiert wird, nicht konfiguriert wurde.

Alte Update-Richtlinien, die vor dem Upgrade vorhanden waren, werden jetzt im Bereich **Richtlinien** unter **Alte Richtlinien einbeziehen** angezeigt. EM Library wird weiterhin ausgeführt. Endpoints nutzen alte Update-Richtlinien und beziehen Updates weiterhin über zentrale Installationsverzeichnisse, die von EM Library verwaltet werden.

**Hinweis:** NetWare-Computer stellen eine Ausnahme dar: NetWare-Computer werden automatisch auf Updates von den von Sophos Update Manager erstellten zentralen Installationsverzeichnissen umgestellt.

**Wichtig:** Wenn Sie Computer mit Sophos Anti-Virus für UNIX/Linux, Version 4.x (unverwaltet) besitzen, müssen Sie diese manuell konfigurieren und ihnen die neuen Update-Verzeichnisse zuweisen. Nähere Informationen finden Sie im Support-Artikel **64214** (<http://www.sophos.de/support/knowledgebase/article/64214.html>).

Computer mit Sophos Anti-Virus für UNIX/Linux, Version 7.x, erkennen und übernehmen die neuen Update-Verzeichnisse automatisch.

So läuft die Migration nach Sophos Update Manager ab:

- Überprüfen Sie die Einstellungen von EM Library, um Migrationsfehler zu vermeiden.
- Installieren Sie Sophos Update Manager auf dem EM Library-Computer.

- Öffnen Sie auf dem Enterprise Console-Computer den Migrations-Report des Update Managers. Vergewissern Sie sich, dass der Update Manager einwandfrei konfiguriert wurde.
  - Wenn der Update Manager nicht vollständig konfiguriert wurde, holen Sie dies jetzt nach und erstellen Sie die neuen Update-Richtlinien.
- Richten Sie im Update Manager, der sich auf demselben Computer wie Enterprise Console befindet, die Updates über den Remote Update Manager ein. Dieser ersetzt die Funktion von EM Library.
- Wenn Sie weitere Librarys verwenden, sehen Sie im Updatehierarchie-Bericht nach, welche Librarys noch migriert werden müssen.
- Migrieren Sie weitere verwaltete Librarys auf dem Netzwerk.
- Wenn sich im zentralen Installationsverzeichnis benutzerspezifische Dateien befanden, kopieren Sie sie in die neuen Update-Verzeichnisse.
- Testen Sie die neuen Update-Freigaben und Update-Richtlinien.
- Übertragen Sie neue Update-Richtlinien auf Computergruppen.
- Deinstallieren Sie EM Library, wenn sie nicht mehr für Updates benötigt wird.

Nach diesen Schritten ist die Migration zum Update Manager abgeschlossen. Der Update Manager nutzt jedoch noch die „alten“ Update-Einstellungen von EM Library, und die Endpoints sind immer noch auf die „alte“ Sicherheitssoftware eingestellt. Wenn Sie die neuen Funktionen von Enterprise Console nutzen möchten, müssen die Endpoints entsprechend upgegradet werden. Dies wird im Abschnitt [Upgrade der Sicherheitssoftware auf Endpoints](#) (Seite 5) beschrieben.

Das folgende Diagramm veranschaulicht die Migration.

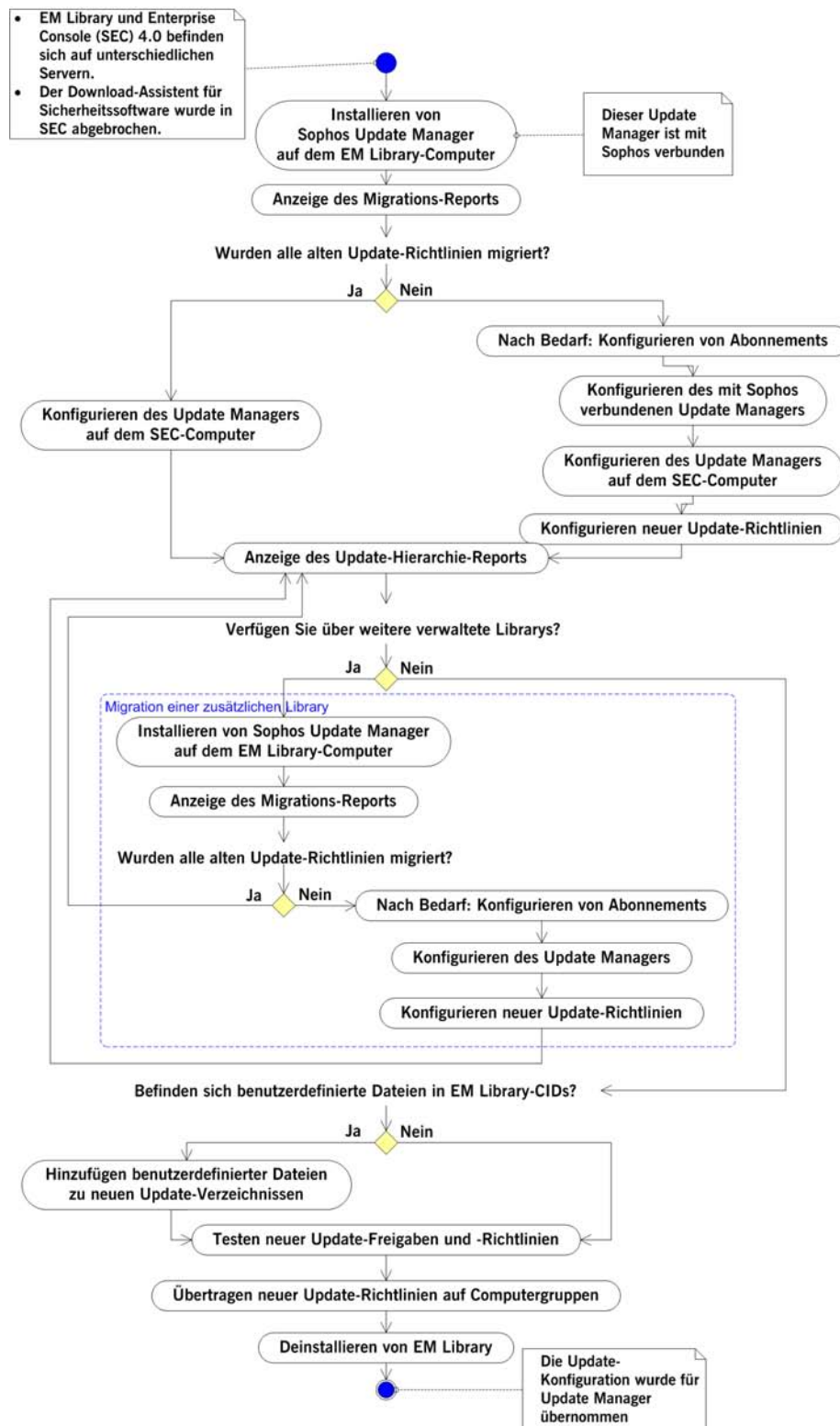


Abbildung 1: Migration der Remote-EM Library nach Sophos Update Manager

## 6.2 Überprüfen der EM Library-Einstellungen

Überprüfen Sie vor der Umstellung von EM Library auf Update Manager, ob EM Library Pakete verwendet, die auf dem Parent nicht mehr gepflegt werden. So vermeiden Sie Fehler bei der Suche des Migrationsassistenten nach nicht vorhandenen Paketen.

So stellen Sie sicher, dass EM Library keine Pakete verwendet, die nicht mehr auf dem Parent gepflegt werden:

1. Klicken Sie in der Symbolleiste von Enterprise Console auf das **Librarys**-Symbol.

Das Sophos EM Library-Fenster wird angezeigt. Standardmäßig wird die Ansicht **Konfiguration** angezeigt.

2. Sehen Sie sich den Benachrichtigungsbereich unten rechts im Bildschirm an.

Wenn EM Library ein Paket verwendet, das nicht mehr auf dem Parent gepflegt wird, wird folgende Meldung angezeigt:

Warning: You have a package in use that is no longer maintained on the parent. Click "Select packages" and subscribe to another package.

3. Wenn Sie noch über veraltete Pakete verfügen, abonnieren Sie entweder ein anderes Paket, das eine aktuelle Software-Version enthält, oder melden Sie die veralteten Pakete ab, wenn sie nicht mehr benötigt werden.

Näheres zum Upgrade erfahren Sie im Support-Artikel „Upgrade auf die neuen Sophos Endpoint Security and Control-Produkte“

(<http://www.sophos.de/support/knowledgebase/article/14844.html>).

## 6.3 Installieren von Sophos Update Manager

Wenn EM Library und der Management-Server von Enterprise Console auf unterschiedlichen Computern installiert wurden, muss Sophos Update Manager auf dem Computer installiert werden, auf dem sich EM Library befindet.

**Hinweis:** Der Installer von Enterprise Console installiert Sophos Update Manager immer auf dem Computer, auf dem sich der Management-Server von Enterprise Console befindet.

Außerdem wird der Installer für Sophos Update Manager in der SUMInstallSet-Freigabe auf dem Computer abgelegt.

Sie können Sophos Update Manager über die Remotedesktop-Funktion in Windows installieren.

So installieren Sie Sophos Update Manager manuell:

1. Wenn der Computer, auf dem sich EM Library befindet, mit einer über Enterprise Console verwalteten Version von Sophos ausgestattet ist, deinstallieren Sie Sophos Remote Management System. Öffnen Sie in der **Systemsteuerung** das Dienstprogramm **Software**, suchen Sie Sophos Remote Management System in der Liste und klicken Sie auf **Ändern/Entfernen** bzw. **Entfernen**. Befolgen Sie die Anweisungen zur Deinstallation der Komponente.

2. Suchen Sie den Installer von Sophos Update Manager. Klicken Sie in Enterprise Console im Menü **Ansicht** auf **Update Manager-Verzeichnis**.  
  
Notieren Sie sich im Dialogfeld **Update Manager-Installationsverzeichnis** das Verzeichnis des Installers.
3. Gehen Sie zu dem Computer mit EM Library und führen Sie den Installer aus.  
Sie können Sophos Update Manager jedoch auch über die Remotedesktop-Funktion in Windows auf dem Computer installieren.
4. Befolgen Sie die Anweisungen des **Sophos Update Manager InstallShield-Assistenten**.
5. Wählen Sie auf der Seite **Sophos Update Manager-Konto** ein Konto aus, über das Endpoints auf die vom Update Manager erstellte Standard-Update zugreifen können. Die Standard-Update-Freigabe lautet \\<ComputerName>\SophosUpdate. ComputerName steht dabei für den Namen des Computers, auf dem der Update Manager installiert wurde. Das Konto muss Lesezugriff auf die Freigabe haben. Administratorrechte sind jedoch nicht erforderlich.  
  
Sie können den Standardbenutzer oder einen vorhandenen Benutzer auswählen oder einen neuen Benutzer erstellen.  
  
Standardmäßig weist der Installer dem **SophosUpdateMgr**-Konto Lesezugriff auf die Update-Freigabe, jedoch keine interaktiven Anmelderechte zu.
6. Geben Sie auf der Seite **Kontodetails zu Sophos Update Manager** in Abhängigkeit von der auf der vorherigen Seite gewählten Option das Kennwort des Standardbenutzers oder die Kontodaten des neuen Benutzers ein oder wählen Sie ein vorhandenes Konto aus.  
  
Das Kennwort des Kontos muss Ihrer Kennwortrichtlinie entsprechen.
7. Klicken Sie im Dialogfeld **Das Programm kann jetzt installiert werden** auf die Option **Installieren**.
8. Klicken Sie nach Abschluss der Installation auf **Fertig stellen**.

Der Computer, auf dem Sophos Update Manager installiert wurde, wird nun in Enterprise Console in der Ansicht **Update Manager** angezeigt. (Klicken Sie im Menü **Ansicht** auf **Update Manager**).

**Hinweis:** Der neue Update Manager wird unter Umständen erst nach einigen Minuten in Enterprise Console angezeigt.

Wenn die Update-Einstellungen erfolgreich von EM Library zum Sophos Update Manager migriert wurden, wird der Update Manager anhand dieser Einstellungen konfiguriert. Aus dem Migrations-Report des Update Managers geht hervor, ob die Migration erfolgreich war.

## 6.4 Aufrufen des Migrations-Reports des Update Managers

Gehen Sie zu dem Computer, auf dem Enterprise Console installiert wurde. Rufen Sie in Enterprise Console die Ansicht **Update Manager** auf. Wenn Sie sich in der Ansicht **Endpoints** befinden, klicken Sie im Menü **Ansicht** auf die Option **Update Manager**.

**Hinweis:** Der neue Update Manager wird unter Umständen erst nach einigen Minuten in Enterprise Console angezeigt.

Öffnen Sie den Migrations-Report des Update Managers und überprüfen Sie, ob die Konfiguration von EM Library für den Update Manager übernommen wurde.

So rufen Sie den Migrations-Report des Update Managers auf:

1. Wählen Sie den Computer aus, dessen Migrations-Report angezeigt werden soll. Rechtsklicken Sie darauf und klicken Sie anschließend auf **Migrations-Report öffnen**.
2. Überprüfen Sie im **Migrations-Report** des Update Managers, ob Folgendes zutrifft:

- Der Update Manager greift auf die richtigen Update-Quellen zu.

Wenn es sich hierbei um den Master Update Manager handelt, der Updates von Sophos herunterlädt, muss als primäre Update-Quelle **Sophos** ausgewählt werden. Anleitungen zur Auswahl einer Update-Quelle entnehmen Sie bitte dem Abschnitt [Auswahl einer Update-Quelle für den Update Manager](#) (Seite 23).

- Der Update-Zeitplan wurde von EM Library migriert. (Wenn dies nicht der Fall ist, wurde ein Standard-Update-Zeitplan übernommen.)
- Die Endpoint-Update-Verzeichnisse wurden erfolgreich migriert.
- Die Update-Richtlinien wurden erfolgreich von alten Update-Richtlinien migriert.

**Hinweis:** Wenn in den alten Update-Richtlinien eine nicht-standardmäßige Installationsquelle festgelegt war, wurde diese Einstellung nicht migriert und die Standardquelle (die primäre Server-Adresse) wurde für die neue Update-Richtlinie übernommen. Dies liegt daran, dass die Update-Verzeichnisstrukturen von EM Library und Sophos Update Manager voneinander abweichen und eine nicht standardmäßige Update-Richtlinie von einem neuen Update-Verzeichnis nicht erkannt wird.

Wählen Sie die Methode aus, die auf Ihre Situation zutrifft:

- Wenn die Update-Einstellungen erfolgreich migriert wurden, wurde der Update Manager auf der Basis dieser Einstellungen konfiguriert. Neue Update-Richtlinien, die den alten Richtlinien entsprechen, wurden zwar erstellt, die Endpoints greifen jedoch noch nicht darauf zu. Fahren Sie mit der Migration anhand der Anweisungen im nächsten Abschnitt fort.
- Wenn die Update-Einstellungen nicht migriert werden konnten, finden Sie im Abschnitt [Update-Einstellungen wurden nicht auf Sophos Update Manager migriert](#) (Seite 21) entsprechende Anweisungen.

## 6.5 Konfigurieren des Update Managers auf dem Computer mit Enterprise Console

Das Netzwerk kann erst dann in vollem Umfang mit Enterprise Console geschützt werden, wenn der Update Manager, der auf dem gleichen Computer wie der Management-Server installiert ist, mit einer Update-Quelle konfiguriert wird. Enterprise Console empfängt dann die erforderlichen Updates (Informationen zu den empfohlenen Sicherheitssoftware-Versionen, neue und aktualisierte Content Control Lists für Data Control oder die aktualisierte Liste überwachter Geräte und Anwendungen).

So konfigurieren Sie den Update Manager:

1. Wählen Sie in der Ansicht **Update Manager** den Computer aus, auf dem Enterprise Console installiert ist. Rechtsklicken Sie und wählen Sie aus dem Kontextmenü die Option **Konfiguration öffnen/ändern**.
2. Klicken Sie im Fenster **Update Manager konfigurieren** auf der Registerkarte **Quellen** auf die Option **Hinzufügen**.
3. Klicken Sie im Dialogfeld **Quellenangaben** auf den Dropdown-Pfeil im Feld **Adresse** und wählen Sie die Standard-Update-Freigabe aus, die von dem Update Manager erstellt wurde, der Updates von Sophos bezieht.  
Sie können jedoch auch die Adresse eingeben oder auf **Durchsuchen** klicken und die Freigabe auswählen.  
Die Standard-Update-Freigabe ist eine UNC-Freigabe \\<ComputerName>\SophosUpdate. ComputerName steht dabei für den Namen des Computers, auf dem der Update Manager installiert wurde, der Updates von Sophos bezieht.
4. Geben Sie gegebenenfalls Benutzernamen, Kennwörter und Proxyserver-Einstellungen ein.

Der Update Manager kann damit Updates für Enterprise Console herunterladen.

Wenn Sie den Update Manager auf dem Computer mit Enterprise Console so konfigurieren möchten, dass er Endpoint-Software-Updates im gesamten Netzwerk bereitstellt, orientieren Sie sich bei der Konfiguration des entsprechenden Software-Abonnements, der Bereitstellung und des Zeitplans an den Einstellungen des Update Managers, der Updates von Sophos bezieht.

Auf Wunsch können Sie zudem die Standardeinstellungen des Update Manager-Protokolls oder der Selbst-Updates ändern. Sie können die hierzu Einstellungen auf den Registerkarten **Protokoll** und **Erweitert** ändern.

## 6.6 Migrieren zusätzlicher verwalteter Librarys

Wenn Sie weitere Librarys mit Enterprise Console verwalten, migrieren Sie die Update-Einstellungen zum Sophos Update Manager.

Im **Update Hierarchie**-Report werden alle Update Manager und Librarys im Netzwerk sowie die von ihnen verwalteten Update-Freigaben und die Anzahl der Computer aufgelistet, die Updates von den Freigaben beziehen. Klicken Sie zum Aufrufen des Reports im Menü **Extras** auf **Report-Verwaltung**. Wählen Sie im Dialogfeld **Update-Richtlinie** die Option **Report Manager** und klicken Sie auf **Ausführen**.

So migrieren Sie die Update-Einstellungen einer weiteren Library:

- Installieren Sie Sophos Update Manager auf dem Computer mit EM Library (mehr zu diesem Thema erfahren Sie im Abschnitt *Installieren von Sophos Update Manager* (Seite 15)).
- Öffnen Sie auf dem Enterprise Console-Computer den Migrations-Report des neuen Update Managers. Vergewissern Sie sich, dass der Update Manager einwandfrei konfiguriert wurde (im Abschnitt *Aufrufen des Migrations-Reports des Update Managers* (Seite 16) finden Sie entsprechende Anweisungen).

- Wenn der Update Manager nicht vollständig konfiguriert wurde, holen Sie dies jetzt nach und erstellen Sie die neuen Update-Richtlinien (mehr dazu erfahren Sie im Abschnitt *Update-Einstellungen wurden nicht auf Sophos Update Manager migriert* (Seite 21)).

## 6.7 Testen der neuen Update-Freigabe(n)

Sie sollten überprüfen, ob die richtige(n) Update-Freigabe(n) verwendet werden und die Freigabe(n) upgedatet wird/werden. Dies empfiehlt sich insbesondere bei einem HTTP-Verzeichnis (z.B. einer internetbasierten Update-Freigabe) oder einer Freigabe, die nicht von einem verwalteten Update Manager verwaltet wird.

Wenn Sie eine Update-Freigabe testen möchten, migrieren Sie einen Endpoint oder einige Testcomputer so, dass sie Updates von einer von einer neuen Update-Freigabe beziehen, die von einem Update Manager verwaltet wird. Dies erreichen Sie, indem Sie der Freigabe eine Update-Richtlinie zuweisen.

1. Wählen Sie in der Ansicht **Endpoints** im Feld **Gruppen** die Testgruppe aus, rechtsklicken Sie darauf und klicken Sie auf **Gruppenrichtliniendetails**.
2. Wählen Sie im Dialogfeld **Gruppendetails** die Update-Richtlinie aus, die auf die gewünschte Freigabe gerichtet ist, und klicken Sie auf **OK**.

Beim nächsten geplanten Update suchen die Testcomputer nach Updates.

3. Warten Sie, bis die Updatesuche abgeschlossen ist. Rufen Sie anschließend die Registerkarte **Status** auf und sehen Sie sich die Spalte **Auf dem neuesten Stand** an. Sie können jedoch auch die Registerkarte **Updatedetails** aufrufen.
  - Wenn in der Spalte **Auf dem neuesten Stand** „Ja“ steht, konnten die Computer über die neue Update-Freigabe upgedatet werden.
  - Wenn ein Uhrensymbol angezeigt wird, befindet sich der Computer nicht auf dem neuesten Stand. Aus dem Text geht hervor, seit wann sich der Computer nicht mehr auf dem neuesten Stand befindet. Nähere Anweisungen zum Updaten von Computern, die sich nicht auf dem neuesten Stand befinden, entnehmen Sie bitte dem Abschnitt „Updates“ in der *Hilfe* zu *Sophos Enterprise Console*.

## 6.8 Zuweisen neuer Update-Richtlinien

So weisen Sie einer Computergruppe eine neue Update-Richtlinie zu:

1. Wählen Sie in der Ansicht **Endpoints** im Feld **Gruppen** die Gruppe aus, rechtsklicken Sie darauf und klicken Sie auf **Gruppenrichtliniendetails**.
2. Deaktivieren Sie im Dialogfeld **Gruppendetails** das Kontrollkästchen **Alte Richtlinien einbeziehen**.

Wenn Sie der Gruppe eine Update-Richtlinie zuweisen möchten, deren Name von der bisherig zugewiesenen Update-Richtlinie abweicht, wählen Sie aus der Dropdown-Liste eine Update-Richtlinie.

Wenn alle Computer auf die Verwendung der neuen Update-Richtlinien umgestellt wurden und diese nun vom Update Manager verwaltet werden, können Sie EM Library deinstallieren.

**Hinweis:** Die gleichzeitige Ausführung von EM Library und Sophos Update Manager erhöht den Datenverkehr im Netzwerk.

Jetzt können Sie Software-Upgrades über den Update Manager durchführen (Näheres hierzu erfahren Sie unter [Upgrade der Sicherheitssoftware auf Endpoints](#) (Seite 5)).

Wenn Sie Device Control mit Sophos Anti-Virus 7 genutzt haben, müssen Sie die Device Control-Richtlinien in eine neue Richtlinie übertragen, sofern Sie dies nicht bereits erledigt haben (Nähere Anweisungen hierzu entnehmen Sie bitte dem nächsten Abschnitt).

## 6.9 Übertragen von Device Control-Einstellungen auf die neue Richtlinie

Wenn Sie Device Control bereits in Enterprise Console 4,0 und Sophos Anti-Virus 7 genutzt haben, befinden sich Ihre Device Control-Einstellungen in der Application Control-Richtlinie. Computer mit Endpoint Security and Control 9.5 beziehen die Device Control-Einstellungen aus der Device Control-Richtlinie. Alle weiteren Device Control-Einstellungen, die zuvor in der Application Control-Richtlinie festgelegt wurden, werden nur für die Computer übernommen, auf denen weiterhin Sophos Anti-Virus 7 ausgeführt wird.

Sie können die Einstellungen der Application Control-Richtlinie mit dem **DeviceControlMigration**-Tool auf die Device Control-Richtlinie übertragen.

Mit dem **DeviceControlMigration**-Tool werden neue Device Control-Richtlinien erstellt. Das Tool orientiert sich an den Application Control-Richtlinien zu gesperrten Geräten. Die Richtlinien werden dann auf Computergruppen übertragen. Ihre Application Control-Richtlinien bleiben unverändert.

So können Sie Device Control-Einstellungen von Application Control-Richtlinien auf Device Control-Richtlinien übertragen:

1. Gehen Sie zu dem Computer, auf dem der Management-Server von Enterprise Console installiert ist. Suchen Sie in Ihrem Installationsverzeichnis (in der Regel C:\Programme) den Ordner Sophos\Enterprise Console.
2. Suchen Sie das Tool **DeviceControlMigration.exe** und führen Sie es aus.  
Das Migrations-Tool kann ohne Vorgabe spezieller Einstellungen ausgeführt werden. Es stehen folgende Zusatzoptionen zur Auswahl:

Option	Funktion
<b>-h</b>	Anzeige der Befehlszeilenhilfe
<b>-noconfirm</b>	Ausführung ohne Benutzerbestätigung
<b>-v</b>	Ausführliche Befehlsausgabe

## 6.10 Update-Einstellungen wurden nicht auf Sophos Update Manager migriert

In einigen Fällen ist die Migration der EM Library-Einstellungen auf Sophos Update Manager nicht möglich. Dies kann z.B. vorkommen, wenn EM Library mit den benutzerdefinierten Paketen arbeitet, da diese nicht migriert werden können. Oder EM Library bezieht Updates aus einer für den Update Manager ungültigen Quelle.

Wenn bestimmte Update-Einstellungen nicht migriert werden können, führen Sie die erforderlichen Schritte durch:

- Konfigurieren Sie die Abonnements (siehe [Abonnieren von Sophos Software und Updates](#) (Seite 21)).
- Richten Sie im Update Manager Abonnements für das Herunterladen und Verteilen der Software im Netzwerk ein (siehe [Konfigurieren des Update Managers](#) (Seite 23)).
- Erstellen Sie neue Update-Richtlinien (siehe [Erstellen neuer Update-Richtlinien](#) (Seite 26)).

### 6.10.1 Abonnieren von Sophos Software und Updates

Mit Abonnements können Sie festlegen, welche Software von Sophos heruntergeladen werden soll.

Dabei können Sie eine Softwareversion für jede unterstützte Plattform festlegen. Wenn Sie unterschiedliche Softwareversionen für die gleiche Plattform herunterladen möchten, benötigen Sie mehrere Abonnements.

**Wichtig:** Wenn Sie Sophos Anti-Virus für NetWare herunterladen möchten, lesen Sie bitte auf der Sophos Website den Support-Artikel 59192 (<http://www.sophos.de/support/knowledgebase/article/59192.html>).

So abonnieren Sie Sophos Sicherheitssoftware und Updates:

1. Doppelklicken Sie in der Ansicht **Update Manager** im Feld **Software-Abonnements** auf das gewünschte Abonnement (z.B. „Empfohlen“) oder klicken Sie zum Erstellen eines neuen Abonnements oben im Fenster auf **Hinzufügen**.
2. Im Dialogfeld **Software-Abonnements** können Sie auf Wunsch den Namen des Abonnements ändern.
3. Klicken Sie neben der Plattform, für die Sie Software herunterladen möchten, in das Feld **Version** und klicken Sie erneut.

Die vorhandenen Versionen werden in einer Dropdown-Liste angezeigt.

4. Wählen Sie die Update-Art und Softwareversion (z.B. „Empfohlen: 7“ für Windows 2000 und höher), die Sie herunterladen möchten.

In der Regel bietet sich die Option **Empfohlen** an, da so sichergestellt wird, dass Software automatisch auf dem neuesten Stand gehalten wird. Im Abschnitt *Update-Arten* (Seite 22) können Sie sich über die unterschiedlichen Update-Arten informieren.

**Wichtig:** Wenn Sie eine „feste Version“ (z.B. 7.6.5) ausgewählt haben, empfiehlt sich, die Option **Nicht mehr unterstützte Abonnements einer bestimmten Version automatisch updaten** nicht zu deaktivieren. Wenn Sie nicht unterstützte Software nutzen, sind Ihre Computer vor neuen Threats nicht hinreichend geschützt.

5. Wiederholen Sie die Schritte 3 und 4 für alle Plattformen, für die Sie Software herunterladen möchten.

Wenn Sie die Sicherheitssoftware abonniert haben, muss der Update Manager zur Verwaltung der Abonnements und Bereitstellung der Software im gesamten Netzwerk konfiguriert werden.

Sie können auch E-Mail-Benachrichtigungen für Abonnements einrichten. Die Einrichtung von E-Mail-Benachrichtigungen zu Abonnements wird in der *Hilfe* zu *Sophos Enterprise Console* im Abschnitt „Alerts“ eingehend beschrieben.

## 6.10.2 Update-Arten

Jede Hauptversion einer Softwarelösung (z.B. Sophos Endpoint Security and Control 9) für die jeweiligen Betriebssysteme (z.B. Windows 2000 und höher) umfasst mehrere Versionen. Durch Festlegen einer Update-Art können Sie die Softwareversion auswählen, die von Sophos heruntergeladen werden und auf den Endpoints installiert werden soll. Es stehen drei Software-Versionen kategorisierter Updates und drei Software-Versionen fester Updates zur Auswahl.

### Kategorisierte Updates

Folgende Kategorien werden angeboten:

Kategorie	Beschreibung
<b>Empfohlen</b>	Die von Sophos für angemessen erachtete Version zum Bezug der aktuellen Produktversion. Sophos empfiehlt in der Regel die Installation der neuesten Version der Endpoint-Software auf Computern.
<b>Vorherig</b>	Die vor der aktuellen Version empfohlene Version.
<b>Alt</b>	Die älteste Softwareversion, für die Sophos Updates anbietet.

**Hinweis:** Möglicherweise werden künftig weitere Kategorien folgen.

Wenn Sie mit dem **Download-Assistent für Sicherheitssoftware** ein Abonnement einrichten, werden jeweils die empfohlenen Softwareversionen für Updates ausgewählt.

Wenn Sie eine bestimmte Version abonniert haben, etwa „empfohlen“ oder „vorherig“, lädt Enterprise Console stets die Version mit der entsprechenden Bezeichnung von Sophos herunter. Die Download-Versionen werden in der Regel jeden Monat geändert.

### Feste Updates

Feste Versionen werden mit neuen Threat-Erkennungsdaten, jedoch nicht mit den monatlichen Software-Updates upgedatet.

Wenn Sie neue Versionen vor der Installation im Hauptnetzwerk testen möchten, empfiehlt sich, bis zum Abschluss der Tests feste Updates im Hauptnetzwerk einzusetzen.

In der Regel sind drei Versionen fester Updates für jedes Betriebssystem erhältlich (die Updates der vergangenen drei Monate). Ein festes Update kann etwa wie folgt aussehen: Sophos Endpoint Security and Control für Windows 2000 und höher, Version 9.4.3.

Feste Updates werden von Sophos heruntergeladen, bis sie eingestellt werden. Bei Einstellung eines festen Updates wird neben allen **Update Managern**, die diese Version herunterladen, ein Alert angezeigt. Wenn Sie E-Mail-Benachrichtigungen eingerichtet haben, wird der Administrator zudem per E-Mail darüber informiert.

Standardmäßig nimmt Enterprise Console bei Einstellung eines festen Updates das älteste verfügbare feste Update in das Abonnement auf.

**Hinweis:** Diese Option können Sie durch Deaktivieren des Kontrollkästchens **Nicht mehr unterstützte Abonnements einer bestimmten Version automatisch updaten** im Abonnement ändern. Wenn Sie nicht unterstützte Software ausführen, ist Ihr Computer vor neuen Threats nicht geschützt. Sophos rät daher zu umgehenden Updates auf eine unterstützte Version.

## 6.10.3 Konfigurieren des Update Managers

So konfigurieren Sie den Update Manager:

1. Wählen Sie in der Ansicht **Update Manager** den Update Manager aus, den Sie konfigurieren möchten. Rechtsklicken Sie und wählen Sie aus dem Kontextmenü die Option **Konfiguration öffnen/ändern**.

Das Dialogfenster **Update Manager konfigurieren** wird angezeigt.

2. Ändern Sie die Konfiguration anhand der Anweisungen in den folgenden Abschnitten ab.

### 6.10.3.1 Auswahl einer Update-Quelle für den Update Manager

Es muss eine Quelle angegeben werden, von der der Update Manager Sicherheitssoftware und Updates herunterlädt, die dann im Netzwerk bereitgestellt werden.

Sie können mehrere Quellen angeben. Dabei ist die erste der ausgewählten Update-Quellen die Primärquelle. Die übrigen Quellen in der Liste können auf Wunsch für den Fall angegeben werden, dass der Update Manager nicht auf die Primärquelle zugreifen kann.

Die Primärquelle des Update Managers an der Spitze der Update-Hierarchie, der Software von Sophos herunterlädt, muss „Sophos“ lauten.

So wählen Sie eine Update-Quelle aus:

1. Klicken Sie im Fenster **Update Manager konfigurieren** auf der Registerkarte **Quellen** auf die Option **Hinzufügen**.
2. Geben Sie in das Dialogfeld **Quellenangaben** im Feld **Adresse** die Adresse der Update-Quelle ein. Es kann sich bei der Adresse um einen UNC- oder einen HTTP-Pfad handeln.

Wenn Sie Software und Updates direkt von Sophos herunterladen möchten, wählen Sie **Sophos**.

3. Geben Sie bei Bedarf den **Benutzernamen** und das **Kennwort** für den Zugriff auf die Update-Quelle in die entsprechenden Felder ein.
  - Wenn die Update-Quelle „Sophos“ lautet, geben Sie die Download-Zugangsdaten ein, die Sie von Sophos erhalten haben.
  - Wenn es sich bei der Update-Quelle um die von einem Update Manager einer höheren Hierarchieebene erstellte Standard-Update-Quelle handelt, sind die Felder **Benutzername** und **Kennwort** bereits ausgefüllt.

Die Standard-Update-Freigabe ist eine UNC-Freigabe  
\\<ComputerName>\SophosUpdate. ComputerName steht dabei für den Namen des Computers, auf dem der Update Manager installiert wurde.

- Wenn Sie nicht auf einen Standard-Update-Quelle im Netzwerk zugreifen, geben Sie die Zugangsdaten des Kontos ein, das Lesezugriff auf die Freigabe besitzt. Falls der **Benutzername** auch eine Domäne erfordert, geben Sie ihn im Format Domäne\Benutzername ein.
4. Wenn Sie auf die Update-Quelle über einen Proxyserver zugreifen, wählen Sie die Option **Über Proxyserver verbinden**. Geben Sie anschließend die **Adresse** und den **Port** des Proxyservers an. Geben Sie die **Zugangsdaten** des Proxyservers ein. Falls der Benutzername auch eine Domäne erfordert, geben Sie ihn im Format Domäne\Benutzername ein. Klicken Sie auf **OK**.

Die neue Quelle wird in der Liste im Dialogfeld **Update Manager konfigurieren** angezeigt.

Wenn Sie einen weiteren Update Manager konfigurieren und bereits einen Update Manager auf einem anderen Computer installiert haben, wird die Freigabe, auf die der Update Manager zugreift, in der Adressenliste angezeigt. Sie können die Freigabe als Quelle für den Update Manager angeben, den Sie konfigurieren. Anschließend können Sie die gewünschte Primäradresse mit Hilfe der Pfeilschaltflächen rechts neben der Liste ganz nach oben verschieben.

### 6.10.3.2 Auswahl der Software zum Download

Sie müssen die Abonnements auswählen, auf die sich der Update Manager beim Download und der Bereitstellung der Software im Netzwerk bezieht.

So wählen Sie Abonnements aus:

1. Wählen Sie im Dialogfeld **Update Manager konfigurieren** auf der Registerkarte **Abonnements** ein Software-Abonnement aus der Liste der verfügbaren Abonnements aus. Details zum Abonnement (z.B. vom Abonnement erfasste Software) können Sie per Klick auf **Details** aufrufen.

2. Klicken Sie auf >, um das gewählte Abonnement in die Liste „Abonniert für“ aufzunehmen. Klicken Sie zum Verschieben aller Abonnements in die Liste „Abonniert für“ auf die Schaltfläche >>.

### 6.10.3.3 Festlegen des Download-Verzeichnisses

Wenn Sie angegeben haben, welche Software heruntergeladen werden soll, können Sie nun das Download-Verzeichnis im Netzwerk angeben. Standardmäßig wird Software in einer UNC-Freigabe abgelegt: \\<Computername>\SophosUpdate. ComputerName steht dabei für den Namen des Computers, auf dem der Update Manager installiert wurde.

Sie können heruntergeladene Software in weiteren Freigaben im Netzwerk bereitstellen. Nehmen Sie hierzu eine vorhandene Netzwerkfreigabe in die Liste der verfügbaren Freigaben auf und verschieben Sie sie von dort anhand der folgenden Anweisungen in die Liste der Update-Freigaben.

So legen Sie das Download-Verzeichnis fest:

1. Wählen Sie im Dialogfeld **Update Manager konfigurieren** auf der Registerkarte **Verteilung** ein Software-Abonnement aus der Liste aus.
2. Wählen Sie eine Freigabe aus der Liste der verfügbaren Freigaben aus und verschieben Sie sie durch Klicken auf die Schaltfläche > in die Liste „Update auf“.

Die Standardfreigabe \\<Computername>\SophosUpdate befindet sich immer in der Liste „Update auf“. Die Freigabe kann nicht gelöscht werden.

Die Liste der verfügbaren Freigaben umfasst alle Freigaben, die Enterprise Console bekannt sind und nicht bereits von einem anderen Update Manager genutzt werden.

Über die Schaltflächen **Hinzufügen** bzw. **Entfernen** können Sie vorhandene Freigaben in die Liste der verfügbaren Freigaben aufnehmen oder daraus entfernen.

3. Wenn Sie eine Beschreibung zu einer Freigabe oder Zugangsdaten zum Schreiben in die Freigabe angeben möchten, wählen Sie die Freigabe aus und klicken Sie auf **Konfigurieren**.
4. Geben Sie im Dialogfeld **Freigaben-Manager** die Beschreibung und die Zugangsdaten ein.

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

Anweisungen zum Ändern des Standard-Update-Zeitplans entnehmen Sie bitte dem Abschnitt [Ändern eines Update-Zeitplans](#) (Seite 25).

Wenn Sie die Software sofort herunterladen möchten, rechtsklicken auf den Update Manager, Sie darauf und klicken Sie auf **Jetzt updaten**.

### 6.10.3.4 Ändern eines Update-Zeitplans

Standardmäßig sucht ein Update Manager alle 10 Minuten nach Updates für Threat-Erkennungsdaten. Sie können das Update-Intervall ändern. Der Mindestwert beträgt 5 Minuten. Der Höchstwert beträgt 1440 Minuten (24 Stunden). Sophos empfiehlt ein Update-Intervall von 10 Minuten für Threat-Erkennungsdaten, um sicherzustellen, dass Sie umgehend vor neu erkannten Threats geschützt sind.

Standardmäßig sucht ein Update Manager alle 60 Minuten nach Software-Updates. Sie können das Update-Intervall ändern. Der Mindestwert beträgt 10 Minuten. Der Höchstwert beträgt 1440 Minuten (24 Stunden).

Als Update-Intervall ist etwa „stündlich an allen Tagen“ denkbar. Sie können jedoch auch komplexere Zeitpläne erstellen und etwa unterschiedliche Update-Zeiträume für unterschiedliche Tage festlegen.

**Hinweis:** Sie können unterschiedliche Zeitpläne für alle Tagen festlegen. Jedem Wochentag kann jeweils nur ein Zeitplan zugeordnet werden.

So können Sie den Standard-Zeitplan ändern:

- Wenn Sie einen komplexeren Zeitplan wünschen oder den einzelnen Wochentagen unterschiedliche Zeitpläne zuweisen möchten, machen Sie im Dialogfeld **Update Manager konfigurieren** auf der Registerkarte **Zeitplan** die nötigen Angaben.

Auf Wunsch können Sie zudem die Standardeinstellungen des Update Manager-Protokolls oder der Selbst-Updates ändern. Sie können die Einstellungen auf den Registerkarten **Protokoll** und **Erweitert** ändern.

#### 6.10.4 Erstellen neuer Update-Richtlinien

Wenn eine oder mehrere neue Update-Richtlinien, die den alten Update-Richtlinien entsprechen, nicht im Zuge der Migration zu Sophos Update Manager erstellt wurden, erstellen Sie sie manuell.

So erstellen Sie eine neue Update-Richtlinie:

1. Rechtsklicken Sie in der Ansicht **Endpoints** im Fenster **Richtlinien** auf **Update** und wählen Sie die Option **Richtlinie erstellen** aus.

Eine „Neue Richtlinie“, deren Name markiert ist, wird zur Liste hinzugefügt.

2. Geben Sie der Richtlinie einen neuen Namen.
3. Doppelklicken Sie auf die neue Richtlinie. Klicken Sie im Dialogfeld **Update-Richtlinie** auf die Registerkarte **Abonnements** und wählen Sie ein Abonnement für Software, die Sie auf dem neuesten Stand halten möchten.
4. Übernehmen Sie auf der Registerkarte **Primärserver** die Standardeinstellungen für das Feld **Adresse** oder geben Sie eine andere Freigabe an (UNC-Pfad oder Web-Adresse), von der Endpoints in der Regel Updates beziehen sollen.

Standardmäßig beziehen die Computer von folgender Freigabe Updates:

\\<ComputerName>\SophosUpdate. ComputerName steht dabei für den Namen des Computers, auf dem der Update Manager installiert wurde.

**Wichtig:** Bei Verwendung einer HTTP-Adresse (z.B. einer internetbasierten Update-Freigabe) oder einer Freigabe, die nicht von einem verwalteten Update Manager verwaltet wird, kann Enterprise Console nicht feststellen, ob die im Abonnement angegebene Software unter dieser Adresse verfügbar ist. Sie müssen manuell überprüfen, ob die Freigabe die in der Abonnement-Richtlinie festgelegte Software enthält. Andernfalls werden die Computer nicht upgedatet.

5. Wenn Sie Macintosh-Computer mit Enterprise Console verwalten möchten und im Feld **Adresse** eine UNC-Freigabe angegeben haben, wählen Sie im Bereich **Mac OS-spezifische Optionen** ein Protokoll aus, über das die Macs auf die Update-Freigabe zugreifen sollen.
6. Geben Sie bei Bedarf den **Benutzernamen** für den Zugriff auf den Server ein. Geben Sie dann das Kennwort ein und bestätigen Sie das Kennwort. Das Konto muss Lesezugriff auf die Freigabe besitzen, die Sie oben in das Adressfeld eingegeben haben.

**Hinweis:** Falls der Benutzername auch eine Domäne erfordert, geben Sie ihn im Format Domäne\Benutzername ein.

7. Wenn Sie über einen Proxyserver auf die Update-Quelle zugreifen, klicken Sie auf **Proxyserver-Details**. Wählen Sie im Dialogfeld **Proxyserver-Details** die Option **Internetverbindung über Proxyserver herstellen** aus. Geben Sie anschließend die **Adresse** und den **Port** des Proxyservers an. Geben Sie die **Zugangsdaten** des Proxyservers ein. Falls der Benutzername auch eine Domäne erfordert, geben Sie ihn im Format Domäne\Benutzername ein.

Jetzt können Sie die Richtlinie auf eine oder mehrere Gruppen übertragen, um die Sicherheitssoftware der Computer in den Gruppen auf dem neuesten Stand zu halten.

Auf Wunsch können Sie zudem die genutzte Bandbreite verringern, eine alternative Update-Quelle eingeben oder den Update-Zeitplan, den Anmeldevorgang und die Details der Erstinstallationsquelle ändern. Anweisungen zum Konfigurieren der Update-Richtlinien entnehmen Sie bitte dem Abschnitt „Konfigurieren der Update-Richtlinie“ der *Hilfe* zu Sophos Enterprise Console.

Setzen Sie die Migration anhand der Anweisungen im Abschnitt [Konfigurieren des Update Managers auf dem Computer mit Enterprise Console](#) (Seite 17) fort.

## 7 Technischer Support

Technischen Support zu Sophos Produkten können Sie wie folgt abrufen:

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

## 8 Rechtlicher Hinweis

Copyright © 2010 Sophos Group. Alle Rechte vorbehalten. Kein Teil dieser Publikation darf in jeglicher Form, weder elektronisch oder mechanisch, reproduziert, elektronisch gespeichert oder übertragen werden, noch fotokopiert oder aufgenommen werden, es sei denn, Sie haben entweder eine gültige Lizenz, gemäß der die Dokumentation in Übereinstimmung mit den Lizenzvereinbarungen reproduziert werden darf oder Sie haben eine schriftliche Genehmigung des Copyright-Inhabers.

Sophos und Sophos Anti-Virus sind eingetragene Warenzeichen der Sophos Plc und Sophos Group. Alle anderen erwähnten Produkt- und Unternehmensnamen sind Warenzeichen oder eingetragene Warenzeichen der jeweiligen Inhaber.

### Common Public License

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

### ACE™, TAO™, CIAO™, and CoSMIC™

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

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

You can use DOC software in commercial and/or binary software releases and are under no obligation to redistribute any of your source code that is built using DOC software. Note, however, that you may not do anything to the DOC software code, such as copyrighting it yourself or claiming authorship of the DOC software code, that will prevent DOC software from being distributed freely using an open-source development model. You needn't inform anyone that you're using DOC software in your software, though we encourage you to let us<sup>11</sup> know so we can promote your project in the DOC software success stories<sup>12</sup>.

DOC software is provided as is with no warranties of any kind, including the warranties of design, merchantability, and fitness for a particular purpose, noninfringement, or arising from a course of dealing, usage or trade practice. Moreover, DOC software is provided with no support and without any obligation on the part of Washington University, UC Irvine, Vanderbilt University, their employees, or students to assist in its use, correction, modification, or enhancement. A number of companies<sup>13</sup> around the world provide commercial support

for DOC software, however. DOC software is Y2K-compliant, as long as the underlying OS platform is Y2K-compliant.

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

The ACE<sup>14</sup>, TAO<sup>15</sup>, CIAO<sup>16</sup>, and CoSMIC<sup>17</sup> web sites are maintained by the DOC Group<sup>18</sup> at the Institute for Software Integrated Systems (ISIS)<sup>19</sup> and the Center for Distributed Object Computing of Washington University, St. Louis<sup>20</sup> for the development of open-source software as part of the open-source software community<sup>21</sup>. By submitting comments, suggestions, code, code snippets, techniques (including that of usage), and algorithms, submitters acknowledge that they have the right to do so, that any such submissions are given freely and unreservedly, and that they waive any claims to copyright or ownership. In addition, submitters acknowledge that any such submission might become part of the copyright maintained on the overall body of code, which comprises the DOC software. By making a submission, submitter agree to these terms. Furthermore, submitters acknowledge that the incorporation or modification of such submissions is entirely at the discretion of the moderators of the open-source DOC software projects or their designees.

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

If you have any suggestions, additions, comments, or questions, please let me<sup>22</sup> know.

Douglas C. Schmidt<sup>23</sup>

### **Quellen**

1. <http://www.cs.wustl.edu/~schmidt/ACE.html>
2. <http://www.cs.wustl.edu/~schmidt/TAO.html>
3. <http://www.dre.vanderbilt.edu/CIAO/>
4. <http://www.dre.vanderbilt.edu/cosmic/>
5. <http://www.dre.vanderbilt.edu/~schmidt/>
6. <http://www.cs.wustl.edu/~schmidt/ACE-members.html>
7. <http://www.wustl.edu/>
8. <http://www.uci.edu/>
9. <http://www.vanderbilt.edu/>
10. <http://www.the-it-resource.com/Open-Source/Licenses.html>
11. [mailto:doc\\_group@cs.wustl.edu](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/>

## ConvertUTF

Copyright 2001–2004 Unicode, Inc.

This source code is provided as is by Unicode, Inc. No claims are made as to fitness for any particular purpose. No warranties of any kind are expressed or implied. The recipient agrees to determine applicability of information provided. If this file has been purchased on magnetic or optical media from Unicode, Inc., the sole remedy for any claim will be exchange of defective media within 90 days of receipt.

Unicode, Inc. hereby grants the right to freely use the information supplied in this file in the creation of products supporting the Unicode Standard, and to make copies of this file in any form for internal or external distribution as long as this notice remains attached.

## OpenSSL cryptographic toolkit

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

## OpenSSL license

Copyright © 1998–2006 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](mailto:openssl-core@openssl.org).
5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

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

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young ([ey@cryptsoft.com](mailto:ey@cryptsoft.com)). This product includes software written by Tim Hudson ([tjh@cryptsoft.com](mailto:tjh@cryptsoft.com)).

#### **Original SSLeay license**

Copyright © 1995–1998 Eric Young ([ey@cryptsoft.com](mailto:ey@cryptsoft.com)) All rights reserved.

This package is an SSL implementation written by Eric Young ([ey@cryptsoft.com](mailto:ey@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](mailto: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 ([ey@cryptsoft.com](mailto:ey@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](mailto: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.]

## Index

### A

- Abonnements
  - Ändern 6
  - Bearbeiten 6
  - Duplizieren 6
  - Erstellen 6
  - Hinzufügen in Update Manager 7
  - Kopieren 6
- Abonnieren neuer Software 5
- Abonnieren von Software 6
- Abonnieren von Software und Updates 21

### B

- benannte Software-Versionen 22
- Bereitstellung von Software 25

### C

- Compliance Dissolvable Agent
  - Upgrade 11

### D

- Device Control
  - Übertragen von Einstellungen 20

### E

- EM Library
  - Beheben von Migrations-Fehlern 21
  - Migration nach Update Manager 12
  - Migration weiterer Librarys nach Update Manager 18
  - Migrations-Report 16
  - Probleme bei der Migration nach Update Manager 21
  - Überprüfen der Einstellungen vor der Migration 15
  - Wichtigste Schritte bei der Migration nach Update Manager 12
- Endpoint-Software
  - Upgrade 5
- Endpoint-Software-Upgrade 5, 8
- Erstellen von Update-Richtlinien 26

### F

- festе Software-Versionen 22

### K

- Konfigurieren neuer Funktionen 10

### L

- Live-Schutz
  - Info 10

### M

- Manipulationsschutz
  - Info 10

### N

- Neue Funktionen
  - Konfiguration 10
  - Live-Schutz 10
  - Manipulationsschutz 10
  - Web-Schutz 10

### S

- Software
  - Auswahl 24
- Softwareauswahl 24
- Sophos Update Manager
  - Konfigurieren der Updates 21
- Sophos Update Manager
  - Installieren 15
  - Migrations-Report 16

### T

- Testen von Update-Freigaben 19
- Testen von Update-Richtlinien 19

### U

- Überprüfen der EM Library-Einstellungen 15
- Überprüfen von Richtlinien 4
- Übertragen von Device Control-Einstellungen 20
- Update Manager
  - auf dem Computer mit Enterprise Console 17
  - Auswahl einer Update-Quelle 23

Update Manager (*Fortsetzung*)

- Bereitstellung von Software 25
  - Hinzufügen von Abonnements 7
  - Installieren 15
  - Konfiguration 23
  - Konfigurieren der Updates 21
  - Migrations-Report 16
  - Zeitplan 25
- Update-Arten 22
- Update-Freigaben
- Testen 19
- Update-Quelle 23
- Update-Richtlinien
- Erstellen 26
  - Konfiguration 8
  - Zuweisen 19

Update-Zeitplan 25

Updates von Richtlinien

- Testen 19

Updates

- Arten 22
- benannte Software-Versionen 22
- feste Software-Versionen 22

**W**

Web-Schutz

- Info 10

**Z**

- Zuweisen von Update-Richtlinien 19