

SOPHOS

simple + secure

Sophos NAC Advanced Installationsanleitung

Produktversion: 3.2

Stand: September 2011



Inhalt

1	Einleitung.....	3
2	Systemvoraussetzungen.....	5
3	Installations-Checkliste.....	6
4	Checkliste für die Konfiguration.....	7
5	Installation auf einem Einzelserver.....	14
6	Installation auf mehreren Servern	16
7	Software-Upgrades.....	20
8	Software-Deinstallation.....	24
9	Konfiguration.....	25
10	Installation des Dissolvable Agent.....	54
11	Deinstallation des Dissolvable Agent auf einem Webserver.....	56
12	Installation des Agenten.....	57
13	Deinstallation des Agenten.....	59
14	Optionale Einstellungen.....	60
15	Technischer Support.....	64
16	Rechtlicher Hinweis.....	65

1 Einleitung

Dieses Dokument beschreibt die Installation und Konfiguration von Sophos NAC Advanced. Folgende Themen werden behandelt:

- Systemvoraussetzungen
- Checklisten für die Installation und Konfiguration
- Softwareinstallation
- Software-Deinstallation
- Konfiguration
- Systemvoraussetzungen
- Installation des Dissolvable Agent
- Deinstallation des Dissolvable Agent
- Systemvoraussetzungen des Agenten
- Installation des Agenten
- Deinstallation des Agenten
- Optionale Einstellungen (nur für mehrere Serverinstallationen)

1.1 Zielpublikum

Diese Anleitung richtet sich an IT-Fachkräfte in kleinen und mittelständischen Unternehmen. Doch auch für IT-Spezialisten in größeren Unternehmen, die mehr als 25.000 Endpoints umfassen, ist die Lektüre dieser Anleitung sinnvoll. Wenn Ihr Unternehmen über mehr als 1000 Endpoints verfügt, empfehlen wir Ihnen Sophos Professional Services. Die Professional Services erarbeiten mit Ihrem Sicherheitsteam einen Softwareinstallationsplan für Ihr Unternehmen.

1.2 Begleitmaterial

Die Sophos NAC Advanced-Dokumentation wird gemeinsam mit Sophos NAC Advanced installiert. Sie kann über **Start-Menü > Sophos > Compliance Manager** aufgerufen werden. Adobe® Acrobat® Reader ist erforderlich.

1.3 Anmeldung an Compliance Manager

Der Zugriff auf Compliance Manager ist nur über einen Kontonamen und ein Kennwort möglich.

Für die erste Anmeldung an Compliance Manager können Sie die folgenden Zugangsdaten verwenden:

- **Account Name** = admin
- **Password** = beliebiges Kennwort

Notieren Sie sich dieses Kennwort: Bis Sie andere Benutzerkonten angelegt haben, können Sie nur über dieses Kennwort auf Compliance Manager zugreifen. Weitere Informationen finden Sie unter [Starten von Compliance Manager](#) (Seite 28).

2 Systemvoraussetzungen

Der Sophos NAC Advanced Installationsagent leitet Sie durch die Installation der erforderlichen Komponenten für Sophos NAC Advanced. Einige Komponenten müssen über eine Betriebssystem-CD installiert werden. Achten Sie darauf, dass Sie die richtige Betriebssystem-CD zur Hand haben.

Die folgenden Komponenten müssen von der Betriebssystem-CD installiert werden, falls sie nicht bereits auf den Servern vorhanden sind:

- Internetauthentifizierungsdienst (IAS) (Windows Server 2003) bzw. Netzwerkrichtlinienserver (Windows Server 2008)
- Microsoft Messaging Queue (MSMQ)
- Internet Information Services (IIS) Version 6.0 oder höher
- ASP.NET

Voraussetzungen für Domain Controller

Sie müssen auf dem Domain Controller manuell ein Standard-Domänenkonto erstellen und festlegen, dass das Kennwort nie abläuft und der Benutzer das Kennwort nicht ändern kann. Hierzu müssen Sie auf dem Domain Controller als Domänenadministrator angemeldet sein. Bei der Installation von Sophos NAC Advanced wird dieses Dienstkonto zur lokalen Administratorgruppe auf dem Compliance Agent hinzugefügt, damit Sophos NAC Advanced auf die SQL-Serverdatenbanken zugreifen kann. Dieses Dienstkonto muss auf das Attribut **Mitglied** des Benutzers **Lesezugriff** haben.

Erforderliches Webzertifikat

Policy Interface, Reporting Interface und Registration Interface sind Internetdienste, für die HTTPS zur Kommunikation mit dem Compliance Agent auf jedem Endpoint erforderlich ist. Damit Sophos NAC Advanced einwandfrei funktioniert, müssen Sie auf dem Compliance Anwendungsserver für diese Komponenten ein Webzertifikat installieren. Diese Komponenten können unter einem Webzertifikat zusammengefasst sein. Wenn Sie Ihr eigenes Webzertifikat erstellen, müssen Sie überprüfen, ob alle Endpoints dieses Webzertifikat akzeptieren. Wenn Sie Sophos NAC Advanced testen und HTTPS deaktiviert ist, wird kein Webzertifikat benötigt.

Hinweis: Wenn Sie über mehrere Compliance Anwendungsserver verfügen und Load Balancing-Software verwenden möchten, muss das Webzertifikat mit der URL für den "Server Pool" übereinstimmen, die außerdem auf allen Agenten konfiguriert wird.

Die Systemanforderungen entnehmen Sie bitte der Sophos Website:

<http://www.sophos.de/products/all-sysreqs.html>.

3 Installations-Checkliste

Prüfen Sie anhand dieser Installations-Checkliste, ob alle Voraussetzungen für die Installation von Sophos NAC Advanced erfüllt wurden.

Schritt	Beschreibung	Erledigt
1.	Sie benötigen die Betriebssystem-CDs für Windows Server. Der Sophos NAC Advanced Installationsagent leitet Sie durch die Installation der erforderlichen Komponenten. Einige Komponenten müssen u.U. von der Betriebssystem-CD installiert werden.	
2.	Richten Sie auf dem Domain Controller ein Sophos NAC Advanced -Dienstkonto ein.	
3.	<p>Installieren Sie ein Web-Zertifikat auf dem/den Sophos Compliance Anwendungsserver(n).</p> <p>Benutzernamen, Kennwörter und andere vertrauliche Daten werden von Sophos in einer Arbeitsumgebung über HTTPS geschützt. Für Testzwecke kann HTTPS deaktiviert werden. Weitere Informationen finden Sie unter Deaktivieren von HTTPS zum Test außerhalb einer Arbeitsumgebung (Seite 62). Wenn Sie Sophos NAC Advanced testen und HTTPS deaktiviert ist, wird kein Webzertifikat benötigt.</p>	
4.	<p>Installieren Sie die Sophos Compliance Datenbankserver.</p> <p>Für Implementierungen und Tests von geringem Ausmaß können Sie Sophos NAC Advanced auf einem Einzelsystem installieren.</p>	
5.	<p>Installieren Sie die Sophos Compliance Application Server.</p> <p>Bei umfangreichen Implementierungen sind weitere Sophos Compliance Anwendungsserver erforderlich.</p>	
6.	<p>Installieren Sie RADIUS Enforcer auf den entsprechenden Servern. (Optional)</p> <p>RADIUS Enforcer wird gemeinsam mit dem Compliance Anwendungsserver installiert. Sie können RADIUS Enforcer auch separat auf weiteren Servern installieren.</p>	

4 Checkliste für die Konfiguration

Nach Abschluss der Installation müssen Sie Sophos NAC Advanced konfigurieren. Prüfen Sie anhand dieser Konfigurations-Checkliste, ob alle Voraussetzungen für die Konfiguration von Sophos NAC Advanced erfüllt sind. Sophos NAC Advanced Die Konfiguration von DHCP ist optional und richtet sich danach, ob Sie DHCP Enforcement benötigen.

Checkliste für die Konfiguration (Windows Server 2003)

Schritt	Beschreibung	Erledigt
Sophos NAC Advanced Konfiguration		
1.	Starten Sie den SQL Server Agent und bestätigen/ändern Sie die Report-Standardinstellungen. Weitere Informationen finden Sie unter Starten des SQL Server-Agenten und Prüfen/Ändern der Report-Standardinstellungen (Seite 25).	
2.	Bestimmen Sie die Größe der Compliance Datenbanken und Transaktionsprotokolle. Weitere Informationen finden Sie unter Bestimmen der Größe der SQL Server-Datenbanken und -Transaktionsprotokolle (Seite 26).	
3.	Konfigurieren Sie für den Zugriff auf Compliance Manager externe Benutzerspeicher. (Optional) Weitere Informationen finden Sie unter Konfigurieren eines externen Benutzerspeichers für den Zugriff auf Compliance Manager (optional) (Seite 29).	
4.	Starten Sie Sophos Compliance Manager. Hinweis: In Compliance Manager müssen Sie die vorhandenen Access Templates, Profile, Richtlinien und Gruppen erstellen oder verwenden. Weitere Informationen finden Sie unter Starten von Compliance Manager (Seite 28).	
5.	Installieren Sie Dissolvable Agent auf einem Webserver. Hinweis: Dabei kann es sich um den gleichen Server handeln wie den, auf dem Sie Sophos Compliance Manager installiert haben. Weitere Informationen finden Sie unter Installation des Dissolvable Agent auf einem Webserver (Seite 54).	
Einstellungen des Internetauthentifizierungsdiensts (IAS) (Windows Server 2003)		
6.	Ermöglichen Sie IAS Zugriff auf Active Directory. Hinweis: Bei LDAP-Implementierungen, oder wenn Sie Sophos NAC Advanced als einen RADIUS-Proxy verwenden (indem Sophos NAC Advanced vor einem anderen RADIUS-Server im Proxymodus konfiguriert wird), müssen Sie diesen Schritt nicht durchführen.	

Schritt	Beschreibung	Erledigt
	Weitere Informationen finden Sie unter <i>Ermöglichen des Zugriffs auf Active Directory für IAS</i> (Seite 31).	
7.	Konfigurieren Sie eine Zugriffsrichtlinie. Weitere Informationen finden Sie unter <i>Konfigurieren einer RAS-Richtlinie</i> (Seite 32).	
8.	Deaktivieren Sie IAS-Protokollierung für erfolgreiche Authentifizierungsanforderungen. (Optional) Weitere Informationen finden Sie unter <i>Deaktivieren der IAS-Protokollierung für erfolgreiche Authentifizierungsanforderungen (optional)</i> (Seite 34).	
9.	Fügen Sie für jedes Gerät, das auf das Netzwerk zugreifen kann, RADIUS Clients hinzu. (Optional) Hinweis: Führen Sie diesen Schritt nur aus, wenn Sie die Durchsetzung von RADIUS implementieren möchten. Die Durchsetzung von RADIUS wird mit VPN, 802.1x, Cisco NAC und erweiterten RADIUS-Implementierungen eingesetzt. Für jeden VPN-Gateway (VPN-Concentrator) müssen Sie zu IAS einen RADIUS Client-Eintrag hinzufügen. Weitere Informationen finden Sie unter <i>Hinzufügen eines RADIUS Clients für jedes Netzwerkgerät (optional)</i> (Seite 34).	
Sophos NAC Advanced als RADIUS-Proxy (Windows Server 2003) (Optional) Hinweis: Diese Schritte sind nur notwendig, wenn Sie Sophos NAC Advanced vor einem anderen RADIUS-Server im Proxymodus konfigurieren.		
10.	Fügen Sie eine Servergruppe für den Remote-Zugriff hinzu. Weitere Informationen finden Sie unter <i>Hinzufügen einer Remote-RADIUS-Servergruppe</i> (Seite 39).	
11.	Erstellen Sie eine Verbindungsanforderungsrichtlinie. Weitere Informationen finden Sie unter <i>Erstellen einer Verbindungsanforderungsrichtlinie</i> (Seite 40).	
12.	Prüfen Sie die Voraussetzungen für die Richtlinie. Weitere Informationen finden Sie unter <i>Prüfen der Richtlinienbedingungen</i> (Seite 41).	
13.	Ändern Sie die Ports zur RADIUS-Authentifizierung. Weitere Informationen finden Sie unter <i>Ändern der RADIUS-Authentifizierungs- und Kontoführungsports</i> (Seite 41).	

Schritt	Beschreibung	Erledigt
14.	<p>Ändern Sie das Registrierungsauthentifizierungsprotokoll in der Sophos NAC Advanced Registration Interface.</p> <p>Weitere Informationen finden Sie unter Ändern des Registrierungsauthentifizierungsprotokolls in der Registrierungsschnittstelle (Seite 42).</p>	
15.	<p>Konfigurieren Sie den RADIUS-Server für Gruppenverknüpfungen/-profile. (Optional)</p> <p>Weitere Informationen finden Sie unter Konfigurieren des RADIUS-Servers für Gruppenverknüpfungen/-profile (optional) (Seite 42).</p>	
<p>LDAP-Implementierung (optional)</p> <p>Hinweis: Dieser Schritt muss nur durchgeführt werden, wenn Sie bestehende LDAP-Verzeichnisse mit dem RADIUS Enforcer verwenden.</p>		
16.	<p>In der <i>Sophos NAC Advanced LDAP-Implementierungsanleitung</i> finden Sie eine Checkliste aller LDAP-Schritte.</p>	
<p>Konfiguration von Sophos mit mehreren Compliance Anwendungsservern</p> <p>Hinweis: Die Konfiguration der Compliance Anwendungsserver muss dem primären Compliance Anwendungsserver entsprechen. Um bei LDAP-Implementierungen eine Konfigurationsdatei auf mehreren Servern verwenden zu können, müssen Sie das Password Encryption-Tool auf jedem Server ausführen, um das Bindekennwort zu aktualisieren und zu verschlüsseln. Weitere Informationen finden Sie in der <i>Sophos NAC Advanced Tools-Anleitung</i> .</p>		
17.	<p>Exportieren Sie den Serverschlüssel vom primären Compliance Anwendungsserver und importieren Sie den Serverschlüssel auf weitere Compliance Anwendungsserver.</p> <p>Weitere Informationen finden Sie unter Export und Import des Serverschlüssels zu weiteren Compliance Anwendungsservern (Seite 52).</p>	
18.	<p>Konfigurieren Sie DNS-Round-Robin auf Windows Server 2003. Führen Sie diesen Schritt auf dem Windows-Server aus, auf dem der DNS (Domain Name Service) läuft, wenn andere Load Balancing-Software oder Anwendungen nicht aktiv sind.</p> <p>Weitere Informationen finden Sie unter Konfigurieren von DNS-Round-Robin auf Windows Server 2003 oder höher (Seite 52).</p>	
<p>DHCP Implementation (optional)</p>		
19.	<p>In der <i>Sophos NAC Advanced DHCP Enforcement-Anleitung</i> finden Sie eine Checkliste aller DHCP-Schritte.</p>	
<p>Installieren Sie den Sophos Compliance Agent</p>		

Schritt	Beschreibung	Erledigt
20.	<p>Installieren Sie den Compliance Agent auf Endpoints.</p> <p>Weitere Informationen finden Sie unter <i>Installation des Agenten</i> (Seite 57).</p>	

Checkliste für die Konfiguration (Windows Server 2008)

Schritt	Beschreibung	Erledigt
Sophos NAC Advanced Konfiguration		
1.	<p>Starten Sie den SQL Server Agent und bestätigen/ändern Sie die Report-Standardinstellungen.</p> <p>Weitere Informationen finden Sie unter <i>Starten des SQL Server-Agenten und Prüfen/Ändern der Report-Standardinstellungen</i> (Seite 25).</p>	
2.	<p>Bestimmen Sie die Größe der Compliance Datenbanken und Transaktionsprotokolle.</p> <p>Weitere Informationen finden Sie unter <i>Bestimmen der Größe der SQL Server-Datenbanken und -Transaktionsprotokolle</i> (Seite 26).</p>	
3.	<p>Konfigurieren Sie für den Zugriff auf Compliance Manager externe Benutzerspeicher. (Optional)</p> <p>Weitere Informationen finden Sie unter <i>Konfigurieren eines externen Benutzerspeichers für den Zugriff auf Compliance Manager (optional)</i> (Seite 29).</p>	
4.	<p>Starten Sie Sophos Compliance Manager.</p> <p>Hinweis: In Compliance Manager müssen Sie die vorhandenen Access Templates, Profile, Richtlinien und Gruppen erstellen oder verwenden.</p> <p>Weitere Informationen finden Sie unter <i>Starten von Compliance Manager</i> (Seite 28).</p>	
5.	<p>Installieren Sie Dissolvable Agent auf einem Webserver.</p> <p>Hinweis: Dabei kann es sich um den gleichen Server handeln wie den, auf dem Sie Sophos Compliance Manager installiert haben.</p> <p>Weitere Informationen finden Sie unter <i>Installation des Dissolvable Agent auf einem Webserver</i> (Seite 54).</p>	
Network Policy-Einstellungen (Windows Server 2008)		
6.	<p>Gewähren Sie dem Netzwerkrichtlinienserver Zugriff auf Active Directory.</p> <p>Hinweis: Bei LDAP-Implementierungen, oder wenn Sie Sophos NAC Advanced als einen RADIUS-Proxy verwenden (indem Sophos NAC</p>	

Schritt	Beschreibung	Erledigt
	<p>Advanced vor einem anderen RADIUS-Server im Proxymodus konfiguriert wird), müssen Sie diesen Schritt nicht durchführen.</p> <p>Weitere Informationen finden Sie unter <i>Freigeben des Zugriffs auf Active Directory für den Netzwerkrichtlinienserver</i> (Seite 36).</p>	
7.	<p>Konfigurieren Sie eine Netzwerkrichtlinie.</p> <p>Weitere Informationen finden Sie unter <i>Konfigurieren einer Netzwerkrichtlinie</i> (Seite 36).</p>	
8.	<p>Deaktivieren Sie die Netzwerkrichtlinienserver-Protokollierung für erfolgreiche Authentifizierungsanforderungen. (Optional)</p> <p>Weitere Informationen finden Sie unter <i>Deaktivieren der Netzwerkrichtlinienserverprotokollierung für erfolgreiche Authentifizierungsanforderungen (optional)</i> (Seite 38).</p>	
9.	<p>Fügen Sie für jedes Gerät, das auf das Netzwerk zugreifen kann, RADIUS Clients hinzu. (Optional)</p> <p>Hinweis: Führen Sie diesen Schritt nur aus, wenn Sie die Durchsetzung von RADIUS implementieren möchten. Die Durchsetzung von RADIUS wird mit VPN, 802.1x, Cisco NAC und erweiterten RADIUS-Implementierungen eingesetzt. Für jeden VPN-Gateway (VPN-Concentrator) müssen Sie zu Netzwerkrichtlinienserver einen RADIUS Client-Eintrag hinzufügen.</p> <p>Weitere Informationen finden Sie unter <i>Hinzufügen eines RADIUS Clients für jedes Netzwerkgerät (optional)</i> (Seite 38).</p>	
<p>Sophos NAC Advanced als RADIUS-Proxy (Windows Server 2008) (Optional)</p> <p>Hinweis: Diese Schritte sind nur notwendig, wenn Sie Sophos NAC Advanced vor einem anderen RADIUS-Server im Proxymodus konfigurieren.</p>		
10.	<p>Fügen Sie eine Servergruppe für den Remote-Zugriff hinzu.</p> <p>Weitere Informationen finden Sie unter <i>Hinzufügen einer Remote-RADIUS-Servergruppe</i> (Seite 46).</p>	
11.	<p>Erstellen Sie eine Verbindungsanforderungsrichtlinie.</p> <p>Weitere Informationen finden Sie unter <i>Erstellen einer Verbindungsanforderungsrichtlinie</i> (Seite 46).</p>	
12.	<p>Prüfen Sie die Voraussetzungen für die Richtlinie.</p> <p>Weitere Informationen finden Sie unter <i>Prüfen der Richtlinienbedingungen</i> (Seite 47).</p>	

Schritt	Beschreibung	Erledigt
13.	<p>Ändern Sie das Registrierungsauthentifizierungsprotokoll in der Sophos NAC Advanced Registration Interface.</p> <p>Weitere Informationen finden Sie unter Ändern des Registrierungsauthentifizierungsprotokolls in der Registrierungsschnittstelle (Seite 48).</p>	
14.	<p>Konfigurieren Sie den RADIUS-Server für Gruppenverknüpfungen/-profile. (Optional)</p> <p>Weitere Informationen finden Sie unter Konfigurieren des RADIUS-Servers für Gruppenverknüpfungen/-profile (optional) (Seite 48).</p>	
<p>LDAP-Implementierung (optional)</p> <p>Hinweis: Dieser Schritt muss nur durchgeführt werden, wenn Sie bestehende LDAP-Verzeichnisse mit dem RADIUS Enforcer verwenden.</p>		
15.	In der <i>Sophos NAC Advanced LDAP-Implementierungsanleitung</i> finden Sie eine Checkliste aller LDAP-Schritte.	
<p>Konfiguration von Sophos mit mehreren Compliance Anwendungsservern</p> <p>Hinweis: Die Konfiguration der Compliance Anwendungsserver muss dem primären Compliance Anwendungsserver entsprechen. Um bei LDAP-Implementierungen eine Konfigurationsdatei auf mehreren Servern verwenden zu können, müssen Sie das Password Encryption-Tool auf jedem Server ausführen, um das Bindekennwort zu aktualisieren und zu verschlüsseln. Weitere Informationen finden Sie in der <i>Sophos NAC Advanced Tools-Anleitung</i>.</p>		
16.	<p>Exportieren Sie den Serverschlüssel vom primären Compliance Anwendungsserver und importieren Sie den Serverschlüssel auf weitere Compliance Anwendungsserver.</p> <p>Weitere Informationen finden Sie unter Export und Import des Serverschlüssels zu weiteren Compliance Anwendungsservern (Seite 52).</p>	
17.	<p>Konfigurieren Sie DNS-Round-Robin auf Windows Server 2003. Führen Sie diesen Schritt auf dem Windows-Server aus, auf dem der DNS (Domain Name Service) läuft, wenn andere Load Balancing-Software oder Anwendungen nicht aktiv sind.</p> <p>Weitere Informationen finden Sie unter Konfigurieren von DNS-Round-Robin auf Windows Server 2003 oder höher (Seite 52).</p>	
<p>DHCP Implementation (optional)</p>		
18.	In der <i>Sophos NAC Advanced DHCP Enforcement-Anleitung</i> finden Sie eine Checkliste aller DHCP-Schritte.	
<p>Installieren Sie den Sophos Compliance Agent</p>		

Schritt	Beschreibung	Erledigt
19.	Installieren Sie den Compliance Agent auf Endpoints. Weitere Informationen finden Sie unter <i>Installation des Agenten</i> (Seite 57).	

5 Installation auf einem Einzelserver

Bei der Installation von Sophos NAC Advanced auf einem Einzelserver werden zuerst die Sophos Compliance Datenbanken und dann der Compliance Anwendungsserver installiert.

Für die Sophos NAC Advanced-Installation ist ein Domänenkonto mit lokalen Administratorrechten erforderlich. Das Konto, auf dem NAC installiert wird, muss als „SQL Server-Benutzer“ definiert werden oder der Gruppe angehören, die als „SQL Server-Benutzer“ definiert wurde. Außerdem muss dem SQL Server in SQL die Sysadmin-Serverrolle zugewiesen werden.

1. Sie müssen auf dem Domain Controller manuell ein Standard-Domänenkonto erstellen und festlegen, dass das Kennwort nie abläuft und der Benutzer das Kennwort nicht ändern kann.

Die Installation fügt dieses Dienstkonto der lokalen Administratorgruppe auf dem Compliance Server hinzu, damit Compliance Server auf die SQL-Serverdatenbanken zugreifen kann. Dieses Dienstkonto muss auf das Attribut **Mitglied** des Benutzers **Lesezugriff** haben.

2. Laden Sie Sophos NAC Advanced von der Sophos Website herunter.
3. Doppelklicken Sie auf die Installationsdatei, um die Installation zu starten.

Es empfiehlt sich, Trace Logging bei der Installation von Sophos NAC Advanced zu aktivieren. Geben Sie in eine Befehlszeile den Namen der Installationsdatei von Sophos NAC Advanced, gefolgt von einem Leerzeichen, ein. Geben Sie dann Folgendes ein: /trace (z.B. nac_xx_sfx.exe /trace). Wenn die Installationsmeldung angezeigt wird, klicken Sie in der Meldung auf **OK**, um die Installation auszuführen. Die Installationsprotokolle werden im Verzeichnis „%temp%“ gespeichert.

4. Klicken Sie auf **Next**.
5. Lesen Sie den Endbenutzer-Lizenzvertrag und wählen Sie die Schaltfläche **I Accept the terms of the License Agreement**. Klicken Sie dann auf **Next**.
6. Wählen Sie die Optionsschaltfläche **Sophos Compliance Anwendungsserver, Compliance Datenbanken, and RADIUS Enforcer**. Klicken Sie auf **Next**.
7. Geben Sie die Dienstkontodaten in die entsprechenden Felder ein. Klicken Sie auf **Next**.
Hierbei handelt es sich um das Standard-Domänenkonto, das vom SQL-Server und vom Compliance Anwendungsserver benötigt wird. Dieses Dienstkonto wurde unter Schritt 1 erstellt.
8. Legen Sie ggf. die Internet-Proxyeinstellungen dieses Servers fest, indem Sie das Kontrollkästchen **Use Proxy** wählen. Klicken Sie auf **Next**.

Die Adresse und der Port des Proxys müssen eingegeben werden. Benutzername, Kennwort und Bestätigung des Kennworts sind nur erforderlich, wenn ein authentifizierter Proxyserver verwendet wird.

9. Geben Sie die Sophos Download Account Details in die entsprechenden Felder ein. Klicken Sie auf **Next**.

Sie erhalten diese Zugangsdaten beim Kauf von Sophos NAC Advanced. Benutzername und Kennwort sind zum Update von Patches und zum Abrufen der neuesten Signaturdaten zu jeder Viren- und Spywareschutzanwendung erforderlich. Wenn Sie bei der Installation nicht die richtigen Daten eingegeben haben, können Sie Ihre Angaben mit Compliance Manager ändern. Weitere Informationen finden Sie in der Compliance Manager Hilfe.

10. Ändern Sie das Compliance Manager-IIS-Komponentenverzeichnis den Anforderungen entsprechend. Klicken Sie auf **Next**.

11. Klicken Sie auf **Install**.

Die Sophos Compliance Anwendungsserver und Compliance Manager 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.

12. Klicken Sie auf **Finish**.

Hinweis:

- Bei Installationsfehlern finden Sie im Ereignisprotokoll weitere Informationen. Wenn die Installation der Datenbanken abgebrochen wird, müssen ggf. die folgenden Datenbanken gelöscht werden: AlertStore, AuditStore, GeneralStore, PolicyStore, ReportStore, ReportStoreCache, ReportStoreWH und SecurityStore. Wenn Sie die Datenbanken gelöscht haben, können Sie die Installation wiederholen.
- Nach der Installation sind weitere Schritte erforderlich. Nähere Informationen finden Sie unter [Konfiguration](#) (Seite 25).

6 Installation auf mehreren Servern

Bei umfangreichen Installationen müssen die SQL-Server-Datenbanken und die Anwendung auf separaten Servern installiert werden. Die SQL Server-Datenbanken müssen vor der Anwendung installiert werden.

6.1 Installieren der Datenbanken

Wenn Sie die SQL-Server-Datenbanken und die Anwendung auf separaten Servern installieren, müssen die Server zur gleichen Domäne gehören. Außerdem ist für die Installation der SQL-Server-Datenbank ein Domänenkonto mit lokalen Administratorrechten erforderlich. Das Konto, auf dem NAC installiert wird, muss als „SQL Server-Benutzer“ definiert werden oder der Gruppe angehören, die als „SQL Server-Benutzer“ definiert wurde. Außerdem muss dem SQL Server in SQL die Sysadmin-Serverrolle zugewiesen werden.

1. Sie müssen auf dem Domain Controller manuell ein Standard-Domänenkonto erstellen und festlegen, dass das Kennwort nie abläuft und der Benutzer das Kennwort nicht ändern kann.

Die Installation fügt dieses Dienstkonto der lokalen Administratorgruppe auf dem Compliance Anwendungsserver hinzu, damit Sophos Compliance Anwendungsserver auf die SQL-Serverdatenbanken zugreifen kann. Dieses Dienstkonto muss auf das Attribut **Mitglied** des Benutzers **Lesezugriff** haben.

Hinweis: Der Schritt ist für Upgrades von Sophos NAC Advanced nicht erforderlich.

2. Laden Sie Sophos NAC Advanced von der Sophos Website herunter.
3. Doppelklicken Sie auf die Installationsdatei, um die Installation zu starten.
Es empfiehlt sich, Trace Logging bei der Installation von Sophos NAC Advanced zu aktivieren. Geben Sie in eine Befehlszeile den Namen der Installationsdatei von Sophos NAC Advanced, gefolgt von einem Leerzeichen, ein. Geben Sie dann Folgendes ein: /trace (z.B. nac_xx_sfx.exe /trace). Wenn die Installationsmeldung angezeigt wird, klicken Sie in der Meldung auf **OK**, um die Installation auszuführen. Die Installationsprotokolle werden im Verzeichnis „%temp%“ gespeichert.
4. Klicken Sie auf **Next**.
5. Lesen Sie den Endbenutzer-Lizenzvertrag und wählen Sie die Schaltfläche **I Accept the terms of the License Agreement**. Klicken Sie dann auf **Next**.
6. Führen Sie einen der folgenden Schritte aus:
 - Bei der Installation der Sophos Compliance Datenbanken auf Windows Server 2003 wählen Sie die Optionsschaltfläche **Sophos Compliance Datenbankserver Only**. Klicken Sie auf **Next**.
 - Wenn Sie die Sophos Compliance Datenbanken unter Windows Server 2000 SP3 oder Windows Server 2003 64-Bit installieren und der Installer feststellt, dass Sie nur die SQL-Datenbanken installieren können, klicken Sie auf **OK**.

7. Geben Sie die Dienstkontodaten in die entsprechenden Felder ein. Klicken Sie auf **Next**. Hierbei handelt es sich um das Standard-Domänenkonto, das vom SQL-Server und vom Compliance Anwendungsserver benötigt wird. Dieses Dienstkonto wurde unter Schritt 1 erstellt. Verwenden Sie für Upgrades die Kontodaten der Originalinstallation.
8. Führen Sie einen der folgenden Schritte aus:
 - Wenn Sie auf dem Server über mehr als eine lokale Datenbankinstanz verfügen, wählen Sie die passende Datenbankinstanz. Klicken Sie auf **Next**.
 - Wenn Sie nur über eine Datenbankinstanz verfügen, fahren Sie mit dem nächsten Schritt fort.
9. Klicken Sie auf **Install**.

Die Sophos Compliance 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.
10. Klicken Sie auf **Fertigstellen**.

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

6.2 Installieren der Anwendung

Wenn die Datenbanken und die Anwendungen auf separaten Servern installiert werden, müssen sie der gleichen Domäne angehören. Außerdem ist für die Installation der Anwendung ein Domänenkonto mit lokalen Administratorrechten erforderlich.

Wichtig: Sie müssen alle weiteren Compliance Anwendungsserver installieren und so konfigurieren, dass sie mit dem primären Compliance Anwendungsserver übereinstimmen. Nähere Informationen finden Sie unter [Konfigurieren mehrerer Compliance Anwendungsserver \(optional\)](#) (Seite 51).

1. Laden Sie Sophos NAC Advanced von der Sophos Website herunter.
2. Doppelklicken Sie auf die Installationsdatei, um die Installation zu starten.

Es empfiehlt sich, Trace Logging bei der Installation von Sophos NAC Advanced zu aktivieren. Geben Sie in eine Befehlszeile den Namen der Installationsdatei von Sophos NAC Advanced, gefolgt von einem Leerzeichen, ein. Geben Sie dann Folgendes ein: /trace (z.B. nac_xx_sfx.exe /trace). Wenn die Installationsmeldung angezeigt wird, klicken Sie in der Meldung auf **OK**, um die Installation auszuführen. Die Installationsprotokolle werden im Verzeichnis „%temp%“ gespeichert.
3. Klicken Sie auf **Next**.
4. Lesen Sie den Endbenutzer-Lizenzvertrag und wählen Sie die Schaltfläche **I Accept the terms of the License Agreement**. Klicken Sie dann auf **Next**.
5. Wählen Sie die Optionsschaltfläche **Sophos Compliance Anwendungsserver and RADIUS Enforcer**. Klicken Sie auf **Next**.

6. Geben Sie die Dienstkontodaten in die entsprechenden Felder ein. Klicken Sie auf **Next**.
Hierbei handelt es sich um das Standard-Domänenkonto, das vom SQL-Server und vom Compliance Anwendungsserver benötigt wird. Die Angaben zu diesem Dienstkonto müssen mit den Angaben, die Sie bei der Installation der Sophos Compliance Datenbanken eingegeben haben, übereinstimmen.
7. Legen Sie ggf. die Internet-Proxyeinstellungen dieses Servers fest, indem Sie das Kontrollkästchen **Use Proxy** wählen. Klicken Sie auf **Next**.
Die Adresse und der Port des Proxys müssen eingegeben werden. Benutzername, Kennwort und Bestätigung des Kennworts sind nur erforderlich, wenn ein authentifizierter Proxyserver verwendet wird.
8. Geben Sie den Namen des Compliance Datenbankservers ein. Klicken Sie auf **Next**.
Wenn Sie die Standard-SQL-Instanz nicht verwenden, müssen Server- und Instanzname im Format Server\Instanzname eingegeben werden. Die Installation prüft die Verbindung zwischen dem Server, den Sie installieren, und dem Compliance Datenbankserver.
9. Geben Sie die Sophos Download Account Details in die entsprechenden Felder ein. Klicken Sie auf **Next**.
Sie erhalten diese Zugangsdaten beim Kauf von Sophos NAC Advanced. Benutzername und Kennwort sind zum Update von Patches und zum Abrufen der neuesten Signaturdaten zu jeder Viren- und Spywareschutzanwendung erforderlich. Wenn Sie bei der Installation nicht die richtigen Daten eingegeben haben, können Sie Ihre Angaben mit Compliance Manager ändern. Weitere Informationen finden Sie in der Compliance Manager Hilfe.
10. Ändern Sie das Compliance Manager-IIS-Komponentenverzeichnis den Anforderungen entsprechend. Klicken Sie auf **Next**.
11. Klicken Sie auf **Install**.
Der Sophos Compliance Anwendungsserver 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.
12. Klicken Sie auf **Fertigstellen**.
Hinweis:
 - Bei Installationsfehlern finden Sie im Ereignisprotokoll weitere Informationen.
 - Nach der Installation sind weitere Schritte erforderlich. Nähere Informationen finden Sie unter [Konfiguration](#) (Seite 25). Wenn Sie ein Upgrade durchführen, befolgen Sie die Anweisungen im Abschnitt [Software-Upgrades](#) (Seite 20), anstatt die Konfigurationsschritte nach der Installation durchzuführen.

6.3 Installation von RADIUS Enforcer

RADIUS Enforcer wird gemeinsam mit dem Compliance Anwendungsserver installiert. Sie können RADIUS Enforcer auch separat auf weiteren Servern installieren. Je nach Skalierbarkeit, Netzwerkkonfiguration oder Netzwerkanforderungen kann die Installation von RADIUS Enforcer auf mehreren Servern erforderlich sein. Bei umfangreichen Installationen können Sie RADIUS Enforcer auf einem anderen Server installieren, um die Durchsetzungsaktivitäten von den Agentenaktivitäten auf den Compliance Anwendungsservern zu trennen.

Hinweis: Sophos stellt in direkter Zusammenarbeit mit jedem Unternehmen fest, ob RADIUS Enforcer auf separaten Servern installiert werden soll.

1. Laden Sie Sophos NAC Advanced von der Sophos Website herunter.
2. Doppelklicken Sie auf die Installationsdatei, um die Installation zu starten.
Es empfiehlt sich, Trace Logging bei der Installation von Sophos NAC Advanced zu aktivieren. Geben Sie in eine Befehlszeile den Namen der Installationsdatei von Sophos NAC Advanced, gefolgt von einem Leerzeichen, ein. Geben Sie dann Folgendes ein: /trace (z.B. nac_xx_sfx.exe /trace). Wenn die Installationsmeldung angezeigt wird, klicken Sie in der Meldung auf **OK**, um die Installation auszuführen. Die Installationsprotokolle werden im Verzeichnis „%temp%“ gespeichert.
3. Klicken Sie auf **Next**.
4. Lesen Sie den Endbenutzer-Lizenzvertrag und wählen Sie die Schaltfläche **I Accept the terms of the License Agreement**. Klicken Sie dann auf **Next**.
5. Wählen Sie die Schaltfläche **Sophos RADIUS Enforcer Only**. Klicken Sie auf **Next**.
6. Geben Sie die Dienstkontodaten in die entsprechenden Felder ein. Klicken Sie auf **Next**.
Hierbei handelt es sich um das Standard-Domänenkonto, das vom SQL-Server und vom Compliance Anwendungsserver benötigt wird. Die Angaben zu diesem Dienstkonto müssen mit den Angaben, die Sie bei der Installation der Sophos Compliance Datenbanken eingegeben haben, übereinstimmen.
7. Geben Sie den Namen des Compliance Datenbankservers ein. Klicken Sie auf **Next**.
Wenn Sie die Standard-SQL-Instanz nicht verwenden, müssen Server- und Instanzname im Format *Server\Instanzname* eingegeben werden. Die Installation prüft die Verbindung zwischen dem Server, den Sie installieren, und dem Compliance Datenbankserver.
8. Klicken Sie auf **Install**.
RADIUS Enforcer wird konfiguriert und der Installationsfortschritt angezeigt.
9. Klicken Sie auf **Finish**.

Hinweis: Bei Installationsfehlern finden Sie im Ereignisprotokoll weitere Informationen.

7 Software-Upgrades

Sie können ein Upgrade von Sophos NAC Advanced 3.2.x auf 3.0.x durchführen. upgegradet werden. Sophos NAC für Endpoint Security and Control ist in Sophos Endpoint Security and Control integriert und kann nicht auf Sophos NAC Advanced upgegradet werden.

Wichtig: Um ein Software-Upgrade durchzuführen, müssen Sie genau die gleichen Informationen bei der Installation eingeben oder auswählen, die bei der ursprünglichen Installation eingegeben oder ausgewählt wurden.

1. Rufen Sie vor dem Upgrade Compliance Manager auf und konfigurieren Sie einen Test-Agenten, der die IP-Adresse von einem der Compliance Anwendungsserver verwendet.

Wichtig: Die in diesem Schritt verwendete IP-Adresse des Compliance Anwendungsservers muss die des ersten Compliance Anwendungsservers sein, auf dem ein Upgrade durchgeführt wird.

2. Legen Sie ein Backup des Compliance Anwendungsserver-Schlüssels und aller Datenbanken an.

Hinweis: Legen Sie ein Backup von folgenden Datenbanken an: AlertStore, AuditStore, GeneralStore, PolicyStore, ReportStore, ReportStoreCache, ReportStoreWH und SecurityStore.

3. Stellen Sie alle Compliance Anwendungsserver mithilfe des Maintenance Mode-Tools in den Modus „Maintenance“. Führen Sie das Tool über eine Befehlszeile auf allen Compliance Anwendungsservern aus.

- Wenn Sie von Version 3.0.x upgraden, öffnen Sie eine Befehlszeile und wechseln Sie in das Verzeichnis „Programme\Endforce\Support Tools“. Geben Sie **MaintMode.exe /start** ein.

- Wenn Sie von Version 3.2 upgraden, öffnen Sie eine Befehlszeile und wechseln Sie in das Verzeichnis „Programme\Sophos\NAC\Support Tools“. Geben Sie **MaintMode.exe /start** ein.

Hinweis: Wenn sich die Software im Verwaltungsmodus befindet, erkennt der Agent den Modus und läuft ohne Fehler, Unterbrechung oder Maintenance Mode-Anzeige. Der Agent speichert lokal alle Analyse- und Reportinformationen, bis die Software wieder in den Arbeitsmodus geschaltet wird. Weitere Informationen finden Sie in der *Sophos NAC Advanced Tools-Anleitung*.

4. Installieren Sie das Datenbank-Upgrade auf dem SQL Server anhand der Anweisungen im Abschnitt *Installieren der Datenbanken* (Seite 16).

Hinweis: Sophos NAC Advanced verfügt über eine Installationsdatei, die auf dem Compliance Datenbankserver und den Compliance Anwendungsservern ausgeführt werden kann. Wenn Sie die Installationsdatei ausführen, können Sie die erforderlichen Installationsoptionen für alle Server angeben. Sie müssen zunächst die Datenbanken updaten. Bei Installationsfehlern finden Sie im Ereignisprotokoll weitere Informationen.

Hinweis: Upgrades von SQL Server 2000 werden unterstützt. Upgraden Sie zunächst Sophos NAC Advanced und dann SQL Server.

Wenn das Upgrade der Datenbanken abgebrochen wird, müssen ggf. die folgenden Datenbanken gelöscht werden: AlertStore, AuditStore, GeneralStore, PolicyStore, ReportStore, ReportStoreCache, ReportStoreWH und SecurityStore. Nach dem Löschen der Datenbanken sollten Sie die Datenbanken über das Backup wieder anbinden. Wiederholen Sie die Installation.

5. Gehen Sie am SQL Server folgendermaßen vor:
 - a) Starten Sie ggf. den SQL Server-Agenten. Weitere Informationen finden Sie unter *Starten des SQL Server-Agenten und Prüfen/Ändern der Report-Standard Einstellungen* (Seite 25).
 - b) Prüfen/ändern Sie die Ausführungszeit des Schritts „Report Warehouse Loader“. Diese Einstellung bestimmt, wann aktuelle Reportdaten in die Archivreports verschoben werden. Weitere Informationen finden Sie unter *Prüfen/Ändern des Report Warehouse Loader-Tasks* (Seite 61).
 - c) Prüfen/ändern Sie die Standardreporteinstellungen. Weitere Informationen finden Sie unter *Starten des SQL Server-Agenten und Prüfen/Ändern der Report-Standard Einstellungen* (Seite 25).
6. Entfernen Sie den Compliance Anwendungsserver, für den ein Upgrade durchgeführt werden soll, zuerst aus dem Load Balancing Pool.

Hinweis: Die IP-Adresse dieses Servers muss mit dem unter Schritt 1 konfigurierten Test-Agenten übereinstimmen. Dieser Schritt muss nur ausgeführt werden, wenn Sophos NAC Advanced in einer Load Balancing-Umgebung installiert wird.

7. Installieren Sie das Anwendungs-Upgrade auf diesem Compliance Anwendungsserver. Befolgen Sie hierzu die Anweisungen im Abschnitt *Installieren der Anwendung* (Seite 17).

Hinweis: Bei Installationsfehlern finden Sie im Ereignisprotokoll weitere Informationen.
8. Stellen Sie diesen Compliance Anwendungsserver mithilfe des Maintenance Mode-Tools zurück in den Modus „Production“. Öffnen Sie eine Befehlszeile und wechseln Sie in das Verzeichnis „Programme\Sophos\NAC\Support Tools“. Geben Sie **MaintMode.exe /stop** ein.
9. Prüfen Sie, ob der konfigurierte Test-Agent registrieren, abrufen, analysieren, durchsetzen, korrigieren und berichten kann.
10. Stellen Sie diesen Compliance Anwendungsserver mithilfe des Maintenance Mode-Tools zurück in den Modus „Maintenance“. Öffnen Sie eine Befehlszeile und wechseln Sie in das Verzeichnis „Programme\Sophos\NAC\Support Tools“. Geben Sie **MaintMode.exe /start** ein.

11. Nehmen Sie diesen Compliance Anwendungsserver wieder im Load Balancing Pool auf.
Hinweis: Dieser Schritt muss nur ausgeführt werden, wenn Sophos NAC Advanced in einer Load Balancing-Umgebung installiert wird.
12. Installieren Sie das Anwendungs-Upgrade auf diesem Compliance Anwendungsserver. Befolgen Sie hierzu die Anweisungen im Abschnitt *Installieren der Anwendung* (Seite 17).
13. Führen Sie auf allen Compliance Anwendungsservern die folgenden Schritte durch:
 - Prüfen/ändern Sie die Ausführungszeit des Schritts „Patch Loader“ auf allen Compliance Anwendungsservern. Weitere Informationen finden Sie unter *Prüfen/Ändern des CurrentDefsLoader-Tasks* (Seite 60).
 - Zu Testzwecken und wenn Sie Software nicht in einer Arbeitsumgebung verwenden, deaktivieren Sie HTTPS. Weitere Informationen finden Sie unter *Deaktivieren von HTTPS zum Test außerhalb einer Arbeitsumgebung* (Seite 62).
14. Stellen Sie alle Compliance Anwendungsserver mithilfe des Maintenance Mode-Tools zurück in den Modus „Production“. Öffnen Sie eine Befehlszeile und wechseln Sie auf allen Compliance Anwendungsservern in das Verzeichnis „Programme\Sophos\NAC\Support Tools“. Geben Sie **MaintMode.exe /start** ein.
15. Installieren Sie das Agenten-Upgrade auf einem Test-Endpoint und prüfen Sie, ob er registrieren, abrufen, analysieren, durchsetzen, korrigieren und berichten kann.
16. Installieren Sie das Agenten-Upgrade auf den entsprechenden Endpoints.
17. Installieren Sie den Dissolvable Agent auf dem entsprechenden Webserver anhand der Anweisungen im Abschnitt *Installation des Dissolvable Agent auf einem Webserver* (Seite 54).
Hinweis: Der Dissolvable Agent ersetzt den Web Agent. Der Weg-Agent wird im Zuge der Installation des Dissolvable Agents deinstalliert.
Hinweis: Das Software-Upgrade entfernt Zugriffsbeschränkungen auf Verzeichnisse, die von Sophos NAC Advanced verwendet werden. Sie müssen die Beschränkungen wieder einrichten, nachdem das Upgrade abgeschlossen ist.

Sophos NAC Advanced-Upgrade von Version 3.0.x:

- Durch das Upgrade werden die neuen Funktionen der Version konfiguriert. Um die neuen Richtlinienfunktionen nutzen zu können, müssen vorhandene Richtlinien aktualisiert werden.
- Das Upgrade aktualisiert Compliance Manager mit vordefinierten Profilen, Anwendungen, Fähigkeiten und Maßnahmen. Das Upgrade entfernt außerdem nicht mehr unterstützte Profile, Anwendungen, Fähigkeiten und Maßnahmen. Diese Änderungen können sich auf einige der erstellten Richtlinien auswirken.
- Das Upgrade wandelt Agent Deployment Templates in Agent Configuration Templates um. Agent Configuration Templates enthalten Agenteneinstellungen, die den Einstellungen der Agent Deployment Templates ähnlich sind. Mithilfe der Agent Configuration Templates können Sie Agenteneinstellungen über Richtlinien aktualisieren.
- Da Windows 98 nicht mehr unterstützt wird, wurden alle diesbezüglichen Verweise und Links entfernt. Die Windows 98-Reportdaten werden beibehalten.

- Die Namen der SQL-Ansichten wurden geändert. Die SQL-Ansichten beginnen nun mit NACVP statt mit EFVP. SQL-Abfragen, die noch auf EFVP-Ansichten zurückgreifen, müssen geändert werden.

Hinweis: Die Änderungen sind bei einem Upgrade von Version 3.2 auf 3.2.x nicht relevant, da sie bereits beim Upgrade auf Version 3.2 erfolgten.

8 Software-Deinstallation

Bei der Deinstallation von Sophos NAC Advanced müssen Sie zuerst die Anwendung und danach die Datenbanken deinstallieren, anderenfalls gibt die Anwendung Fehler aus, da die Datenbanken deinstalliert wurden.

8.1 Deinstallieren der Anwendung

Durch die Deinstallation der Anwendung werden keine Objekte gelöscht, die Sie in Compliance Manager angelegt haben. Alle Objekte wie Richtlinien und Benutzerkonten sind in den Compliance Datenbanken gespeichert.

1. Rufen Sie über das Startmenü **Systemsteuerung > Software** auf.
2. Wählen Sie **Sophos Compliance Anwendungsserver** und klicken Sie auf **Entfernen**.
3. Klicken Sie auf **Ja**, um die Entfernung des Compliance Anwendungsservers zu bestätigen. Die Anwendung wurde nun deinstalliert.

8.2 Deinstallieren der Datenbanken

Durch die Deinstallation der Datenbanken werden nur die Dateien entfernt, die zur Erstellung der Datenbanken verwendet wurden, jedoch nicht die Datenbanken.

1. Rufen Sie über das Startmenü **Systemsteuerung > Software** auf.
2. Wählen Sie **Sophos Compliance Datenbankserver** und klicken Sie auf **Entfernen**.
3. Klicken Sie auf **Ja**, um die Entfernung der Serverdateien zu bestätigen, die zur Erstellung der Datenbanken verwendet wurden. Die Serverdateien werden entfernt und die Datenbanken bleiben unbeschädigt.

8.3 Deinstallation von RADIUS Enforcer

RADIUS Enforcer muss nur deinstalliert werden, wenn RADIUS Enforcer auf einem anderen Server als Sophos NAC Advanced installiert wurde.

1. Rufen Sie über das Startmenü **Systemsteuerung > Software** auf.
2. Wählen Sie **Sophos RADIUS Enforcer** und klicken Sie auf **Entfernen**.
3. Klicken Sie auf **Ja**, um RADIUS Enforcer zu entfernen. RADIUS Enforcer wurde damit entfernt.

9 Konfiguration

Hierbei handelt es sich um zusätzliche Konfigurationsschritte, die für die einwandfreie Funktion von Sophos NAC Advanced erforderlich sind.

9.1 Starten des SQL Server-Agenten und Prüfen/Ändern der Report-Standard Einstellungen

Sophos NAC Advanced erstellt Reports, die Aufschluss darüber geben, ob Sicherheitsrichtlinien eingehalten werden und ob Endpoints Risiken ausgesetzt sind. Diese Reports enthalten Informationen, die bei der Fehlersuche hilfreich sind. Die Reporterstellung funktioniert nur bei gestartetem SQL Server-Agent einwandfrei.

Reports sind sowohl in Kurzform als auch in ausführlichen Versionen erhältlich. Sie können aktuelle sowie archivierte Daten enthalten. Die Reporteinstellungen bestimmen, wie lange Daten in einem aktuellen Report aufbewahrt und wann sie archiviert werden. Es empfiehlt sich, die anderen Reporteinstellungen unverändert zu lassen.

Die Voreinstellungen für alle Reports lauten:

- Überprüfungsdaten alle **90** Tage ändern. Hierbei handelt es sich um den Wert „auditStorePurgeDays“. Wenn der Wert **-1** lautet, wird der Löschvorgang deaktiviert.
- Daten aus den aktuellen Reports alle **2** Tage löschen. Hierbei handelt es sich um den Wert „reportStorePurgeDays“.
- Daten alle **30** Tage aus den Archivreports löschen. Hierbei handelt es sich um den Wert „reportStoreWHPurgeDays“.

Hinweis: Der Wert „reportstoreWHPurgeDays“ muss größer als der Wert „reportStorePurgeDays“ und die Anzahl der Tage bis zum Verschieben sein.

- Move data to the archive reports **1** time each day for all reports at 2:30 AM. Dieser Wert befindet sich ist Teil des Schritts „Report Warehouse Loader“. Weitere Informationen zum Ändern der Uhrzeit finden Sie unter [Prüfen/Ändern des Report Warehouse Loader-Tasks](#) (Seite 61).

1. Rufen Sie das Start-Menü in SQL Server auf.

- Klicken Sie in SQL Server 2000 auf **Microsoft SQL Server > Enterprise Manager** . SQL Enterprise Manager wird geöffnet.
- In SQL Server 2005 oder höher klicken Sie auf **Microsoft SQL Server 2005 (Version) > SQL Server Management Studio** . SQL Server Management Studio wird geöffnet.

2. So starten Sie den SQL Server-Agenten:

- Suchen Sie in SQL Server 2000 im Management-Ordner **SQL Server-Agent**. Rechtsklicken Sie darauf und wählen Sie **Starten**.
- Suchen Sie in SQL Server 2005 und höher **SQL Server-Agent**. Rechtsklicken Sie darauf und wählen Sie **Starten**.

Wichtig: Damit SQL Server-Agent beim Neustart von SQL-Server automatisch gestartet wird, müssen Sie Windows Services Control Manager öffnen und den Starttyp des

SQLSERVERAGENT-Dienstes (SQL Server 2000) bzw. des SQL Server-Agenten (SQL Server 2005 und höher) auf „automatisch“ setzen.

3. Um Löschwerte zu ändern, suchen Sie in der **ReportStore**-Datenbank nach der **LoadParam**-Tabelle.
4. So öffnen Sie die **LoadParam**-Tabelle:
 - Rechtsklicken Sie in SQL Server 2000 auf die Tabelle **LoadParam** und wählen Sie **Tabelle öffnen > Alle Zeilen anzeigen** .
 - Unter SQL Server 2005 oder höher rechtsklicken Sie auf die Tabelle **LoadParam** und wählen **Tabelle öffnen**.
5. Um den Löschedatenwert für Überprüfungsdaten zu ändern, geben Sie in der Zeile **auditStorePurgeDays** in der Spalte **paramValue** einen neuen Wert ein.
Wenn der Wert -1 lautet, wird das Löschen von Überprüfungsdaten deaktiviert.
6. Um den Löschedatenwert für die aktuellen Reports zu ändern, geben Sie in der Zeile **reportStorePurgeDays** in der Spalte **paramValue** einen neuen Wert ein.
7. Um den Löschedatenwert für die archivierten Reports zu ändern, geben Sie in der Zeile **reportStoreWHPurgeDays** in der Spalte **paramValue** einen neuen Wert ein.
Hinweis: Der Wert „reportStoreWHPurgeDays“ muss größer als der Wert „reportStorePurgeDays“ und die Anzahl der Tage bis zum Verschieben sein.
8. Schließen Sie SQL Enterprise Manager bzw. SQL Server Management Studio.

9.2 Bestimmen der Größe der SQL Server-Datenbanken und -Transaktionsprotokolle

Bei der Installation werden die Datenbanken so eingerichtet, dass sich deren Größe automatisch anpasst und Statistiken automatisch aktualisiert werden. Es empfiehlt sich, diese Datenbankeigenschaften nicht zu ändern.

Für eine optimale Datenbank empfiehlt sich Folgendes:

- Damit sich die Datenbanken und entsprechenden Transaktionsprotokolle nicht ständig vergrößern, legen Sie für sie eine ausreichende Größe fest.
- Legen Sie für Datenbanken und Transaktionsprotokolle die maximale Größe als Absolutwert fest, statt ein prozentuales Wachstum anzugeben.

9.2.1 Empfohlene Datenbankgrößen

Datenbank	Bestimmung der Größe	Richtwert
ReportStore	0,4 KB x (Anzahl Profile in der Richtlinie) x (Anzahl Endpoints)	500 MB

Datenbank	Bestimmung der Größe	Richtwert
ReportStoreWH Hinweis: Die Vorgabe für das Löschen der Daten ist 30 Tage.	1,5 KB x (Anzahl Profile in der Richtlinie) x (Anzahl Endpoints) x (Löschwert in Tagen)	500 MB
PolicyStore	Für ein Unternehmen mit tausenden Anwendern und einer Richtlinie, die weniger als 100 Anwendungen abdeckt, setzen Sie PolicyStore auf 500 MB.	100 MB

9.2.2 Empfohlene Größen für Transaktionsprotokolle

Protokoll	Bestimmung der Größe	Richtwert
ReportStore	500 MB	100 MB
ReportStoreWH	2 GB	250 MB
PolicyStore	Standardgröße beibehalten	100 MB

9.2.3 Ändern der SQL Server-Datenbank- und Transaktionsprotokollgrößen (SQL Server 2000)

Die Größe der SQL Server-Datenbank und der Transaktionsprotokolle finden Sie unter *Empfohlene Datenbankgrößen* (Seite 26) und *Empfohlene Größen für Transaktionsprotokolle* (Seite 27). Die folgenden Einstellungen gelten für SQL Server 2000.

1. Klicken Sie im Startmenü von SQL Server auf **Microsoft SQL Server > Enterprise Manager**.
SQL Enterprise Manager wird geöffnet.
2. Rechtsklicken Sie zum Bestimmen der Größe von ReportStore im Datenbank-Ordner auf **ReportStore** und wählen Sie **Eigenschaften**.
3. Klicken Sie auf die Registerkarte **Datendateien**.
4. Wählen Sie das Feld **Zugeordneter Speicherplatz (MB)** und geben Sie eine angemessene Größe für ReportStore ein.
5. Wählen Sie die Option **In Megabyte** und geben Sie eine angemessene Größe für das Dateiwachstum von ReportStore ein.
6. Klicken Sie auf die Registerkarte **Transaktionsprotokoll**.
7. Wählen Sie das Feld **Zugeordneter Speicherplatz (MB)** und geben Sie eine angemessene Größe für das Transaktionsprotokoll von ReportStore ein.

8. Wählen Sie die Option **In Megabyte** und geben Sie eine angemessene Größe für das Dateiwachstum des Transaktionsprotokolls von ReportStore ein.
9. Klicken Sie auf **OK**.
10. Wiederholen Sie die Schritte 2 bis 9 für ReportStoreWH und PolicyStore.
11. Beenden Sie SQL Enterprise Manager.

9.2.4 Ändern der SQL Server-Datenbank- und Transaktionsprotokollgrößen (ab SQL Server 2005)

Die Größe der SQL Server-Datenbank und der Transaktionsprotokolle finden Sie unter [Empfohlene Datenbankgrößen](#) (Seite 26) und [Empfohlene Größen für Transaktionsprotokolle](#) (Seite 27). Die folgenden Einstellungen gelten für SQL Server 2005 und höher.

1. Klicken Sie im Startmenü von SQL Server auf **Microsoft SQL Server (Version) > SQL Server Management Studio**.
2. Suchen Sie im Dialogfeld „SQL Server Management Studio“ die **ReportStore**-Datenbank im Datenbankordner. Rechtsklicken Sie auf die Datenbank und wählen Sie die Option **Eigenschaften**.
3. Wählen Sie im Dialogfeld „Eigenschaften“ **Dateien** aus.
4. Suchen Sie die Datei **ReportStore_Data**. Geben Sie die gewünschte Datenbankgröße in das Feld **Anfangsgröße (MB)** ein.
5. Suchen Sie die Datei **ReportStore_Log**. Geben Sie die gewünschte Größe der Protokolldatei in das Feld **Anfangsgröße (MB)** ein.
6. Klicken Sie auf **OK**.
7. Wiederholen Sie die Schritte 2 bis 6 für ReportStoreWH und PolicyStore.
8. Schließen Sie SQL Server Management Studio.

9.3 Starten von Compliance Manager

Der Compliance Manager ist die zentrale Stelle zur Verwaltung von Sophos NAC Advanced. Compliance Manager wird als Standard-Website in folgendem Verzeichnis installiert:
<LokalesLaufwerk>\Inetpub\wwwroot\SophosNAC.

Wichtig: Damit Compliance Manager Daten anzeigen und speichern sowie Grafiken darstellen kann, müssen folgende Voraussetzungen erfüllt sein:

- Compliance Manager muss in Internet Explorer unter den vertrauenswürdigen Websites aufgelistet werden. Dieser Schritt trifft nicht für Internet Explorer 7.x zu.
- Popup-Blocker müssen beim Aufruf von Compliance Manager deaktiviert sein.

Wichtig: Damit Sophos NAC Advanced einwandfrei mit HTTPS funktioniert, müssen Sie ein Webzertifikat für die Komponenten „Web Interface“, „Policy Interface“, „Reporting Interface“ und „Registration Interface“ installieren. Die Komponenten können unter einem Webzertifikat zusammengefasst sein. Wenn Sie Ihr eigenes Webzertifikat erstellen, müssen Sie überprüfen, ob alle Endpoints dieses Webzertifikat akzeptieren. Wenn Sie Sophos NAC Advanced testen und HTTPS deaktiviert ist, wird kein Webzertifikat benötigt.

1. Öffnen Sie Internet Explorer.

2. Geben Sie folgende Adresse ein: `http://<IP-Adresse/DNS des Sophos-Servers>/SophosComplianceManager`. Die Anmeldeseite von Compliance Manager wird aufgerufen.

Hinweis: Informationen zum Deaktivieren von HTTPS finden Sie unter [Deaktivieren von HTTPS zum Test außerhalb einer Arbeitsumgebung](#) (Seite 62). Sobald HTTPS deaktiviert ist, können Sie über folgende Adresse auf Compliance Manager zugreifen: `http://<IP-Adresse/DNS des Sophos-Servers>/SophosComplianceManager`.

3. Geben Sie in das Feld **Account Name** den Namen **Admin** und in das Feld **Password** ein Kennwort Ihrer Wahl ein.
4. Klicken Sie auf **OK**.

Hinweis:

- Notieren Sie sich dieses Kennwort: Bis Sie andere Benutzerkonten angelegt haben, können Sie nur über dieses Kennwort auf Compliance Manager zugreifen.
- In Compliance Manager müssen Sie die vorhandenen Access Templates, Profile, Gruppen und Richtlinien erstellen oder verwenden.

9.4 Konfigurieren eines externen Benutzerspeichers für den Zugriff auf Compliance Manager (optional)

Beim Erstellen von Benutzerkonten für den Zugriff auf Compliance Manager können Sie festlegen, dass diese Konten einen externen Benutzerspeicher verwenden. Wenn es sich hier um die gleiche Art von Benutzerspeicher handelt, wie bei dem, der von Compliance Manager zur Authentifizierung verwendet wird, muss keine weitere Konfiguration durchgeführt werden. Wenn sich Compliance Manager-Benutzerkonten von denen für die Compliance Agenten unterscheidet, müssen Sie eine separate Verbindungsanforderungsrichtlinie erstellen.

Hinweis: Sophos arbeitet direkt mit solchen Unternehmen zusammen, deren Benutzerkonten von Compliance Manager andere Benutzerspeicher verwenden, als ihre Agenten-Benutzer. Diese direkte Zusammenarbeit sorgt dafür, dass die Konfiguration ordnungsgemäß implementiert wird.

9.4.1 Erstellen einer Verbindungsanforderungsrichtlinie für einen externen Benutzerspeicher (Windows Server 2003)

Wenn die Benutzerkonten von Compliance Manager eine andere Art von Benutzerspeicher als Compliance Agenten verwenden, müssen Sie eine separate Verbindungsanforderungsrichtlinie mit dem Dienstyp „administrativ“ erstellen. Diese Verbindungsanforderungsrichtlinie muss zuerst priorisiert werden.

1. Klicken Sie im Startmenü des Compliance Anwendungsservers auf **Verwaltung > Internetauthentifizierungsdienst** .
IAS wird aufgerufen.
2. Doppelklicken Sie auf **Verbindungsanforderungsverarbeitung**.

3. Rechtsklicken Sie auf **Verbindungsanforderungsrichtlinien** und dann auf **Neu Verbindungsanforderungsrichtlinie**.

Das Fenster „Assistent für neue Verbindungsanforderungsrichtlinie“ wird angezeigt.

4. Klicken Sie auf **Weiter**.
5. Wählen Sie die Option **Benutzerdefinierte Richtlinie**. Geben Sie im entsprechenden Feld einen Namen für die Verbindungsanforderungsrichtlinie ein. Klicken Sie auf **Weiter**.
6. Klicken Sie auf **Hinzufügen**, um die entsprechenden Bedingungen für die Richtlinie festzulegen.
7. Wählen Sie die Richtlinienbedingung **Diensttyp** und klicken Sie dann auf **Hinzufügen**.
8. Wählen Sie **Administrativ** unter **Verfügbare Typen** aus und klicken Sie auf **Hinzufügen**. Klicken Sie auf **OK**.
9. Klicken Sie auf **Weiter**.
10. Klicken Sie auf **Weiter**.
11. Prüfen Sie die Angaben der Verbindungsanforderungsrichtlinie und klicken Sie auf **Fertigstellen**.

Diese Verbindungsanforderungsrichtlinie muss die höchste Priorität erhalten. Um die Priorität der Richtlinie zu erhöhen, rechtsklicken Sie auf den Richtliniennamen und wählen Sie **Nach oben**.

9.4.2 Erstellen einer Verbindungsanforderungsrichtlinie für einen externen Benutzerspeicher (Windows Server 2008)

Wenn die Benutzerkonten von Compliance Manager eine andere Art von Benutzerspeicher als Compliance Agenten, verwenden, müssen Sie eine separate Verbindungsanforderungsrichtlinie mit dem Diensttyp „administrativ“ erstellen. Diese Verbindungsanforderungsrichtlinie muss zuerst priorisiert werden.

1. Klicken Sie im Startmenü des Compliance Anwendungsservers auf **Verwaltung > Netzwerkrichtlinienserver**.

Der Netzwerkrichtlinienserver wird geöffnet.

2. Rechtsklicken Sie unter „Richtlinien“ auf **Verbindungsanforderungsrichtlinien** und klicken Sie anschließend auf **Neu**.

Das Fenster „Assistent für neue Verbindungsanforderungsrichtlinie“ wird angezeigt.

3. Geben Sie einen Richtliniennamen ein. Die Netzwerkverbindungsmethode sollte **Nicht angegeben** lauten.
4. Klicken Sie auf **Weiter**.
5. Klicken Sie auf **Hinzufügen**, um die entsprechenden Bedingungen für die Richtlinie festzulegen.
6. Wählen Sie die Richtlinienbedingung **Diensttyp** und klicken Sie dann auf **Hinzufügen**.
7. Klicken Sie auf **Verwaltung** und anschließend auf **OK**.
8. Klicken Sie auf **Weiter**.
9. Wählen Sie im Bereich **Authentifizierung** die Option **Benutzer ohne Überprüfung der Anmeldeinformationen akzeptieren**.

10. Klicken Sie auf **Weiter**.
11. Klicken Sie auf **Weiter**. Für diese Richtlinie sind keine Attribute erforderlich.
12. Prüfen Sie die Angaben der Verbindungsanforderungsrichtlinie und klicken Sie auf **Fertigstellen**.
Diese Verbindungsanforderungsrichtlinie muss die höchste Priorität erhalten. Um die Priorität der Richtlinie zu erhöhen, rechtsklicken Sie auf den Richtliniennamen und wählen Sie **Nach oben**.

9.5 Einstellungen des Internetauthentifizierungsdiensts (IAS) (Windows Server 2003)

IAS wird für die Suche nach und für die Authentifizierung von Gruppen sowie zur Durchsetzung von RADIUS verwendet.

Die meisten Sophos NAC Advanced-Implementierungen erfordern die Suche nach und Authentifizierung von Gruppen. Sie müssen folgendermaßen vorgehen:

- Ermöglichen Sie IAS Zugriff auf Active Directory.

Hinweis: Bei LDAP-Implementierungen, oder wenn Sie Sophos NAC Advanced als einen RADIUS-Proxy verwenden (indem Sophos NAC Advanced vor einem anderen RADIUS-Server im Proxymodus konfiguriert wird), müssen Sie diesen Schritt **nicht** durchführen.

- Erstellen Sie eine Remote-Zugriffsrichtlinie (RAS-Richtlinie).

Wenn RADIUS Enforcement mit VPN, 802.1x, Cisco NAC oder erweiterten RADIUS-Implementierungen verwendet wird, müssen Sie folgendermaßen vorgehen:

- Ermöglichen Sie IAS Zugriff auf Active Directory.
- Konfigurieren Sie eine Zugriffsrichtlinie.
- Fügen Sie für jedes Gerät, das auf das Netzwerk zugreifen kann, wie VPN-Concentrators, RADIUS Clients hinzu.

9.5.1 Ermöglichen des Zugriffs auf Active Directory für IAS

Standardmäßig hat der IAS-Dienst **keine** Rechte, Benutzer in Active Directory zu authentifizieren. Der IAS-Server benötigt das Recht, Benutzer in Active Directory authentifizieren zu können.

Wichtig:

- Bei LDAP-Implementierungen, oder wenn Sie Sophos NAC Advanced als einen RADIUS-Proxy verwenden (indem Sophos NAC Advanced vor einem anderen RADIUS-Server im Proxymodus konfiguriert wird), müssen Sie diesen Schritt **nicht** durchführen.

- Die genannten Schritte müssen auf allen Compliance Anwendungsservern und auf allen RADIUS Enforcer-Servern durchgeführt werden.
- 1. Melden Sie sich auf einem Compliance Anwendungsserver oder RADIUS Enforcer-Server mit Administratorrechten an.
- 2. Klicken Sie im Startmenü des Compliance Anwendungsservers oder eines RADIUS Enforcer-Servers auf **Verwaltung > Internetauthentifizierungsdienst** .
IAS wird aufgerufen.
- 3. Rechtsklicken Sie auf **Internetauthentifizierungsdienst** und wählen Sie dann **Server im Active Directory registrieren**.
- 4. Klicken Sie auf **Ja**, um den IAS-Zugriff auf Active Directory zu bestätigen.
Wenn IAS auf Active Directory zugreifen kann, erhalten Sie eine darauf hinweisende Meldung. Es sind keine weiteren Schritte erforderlich.
- 5. Schließen Sie IAS.
- 6. Wiederholen Sie diese Schritte auf allen Compliance Anwendungsservern und RADIUS Enforcer-Servern.

9.5.2 Konfigurieren einer RAS-Richtlinie

Für die meisten Sophos NAC Advanced-Implementierungen muss eine RAS-Richtlinie erstellt werden. Dieses Dokument beschreibt nur eine häufig verwendete RAS-Richtlinie für VPN. Sophos NAC Advanced-Implementierungen für LAN erfordern eine RAS-Richtlinie für die Suche nach und Authentifizierung von Gruppen.

Wichtig:

- Netzwerkrichtlinien müssen **nicht** konfiguriert werden, wenn Sie Sophos NAC Advanced als RADIUS-Proxy verwenden (indem Sophos NAC Advanced vor einem anderen RADIUS-Server im Proxymodus konfiguriert wird).
- Die genannten Schritte müssen auf allen Compliance Anwendungsservern und auf allen RADIUS Enforcer-Servern durchgeführt werden.
- 1. Klicken Sie im Startmenü des Compliance Anwendungsservers oder eines RADIUS Enforcer-Servers auf **Verwaltung > Internetauthentifizierungsdienst** .
IAS wird aufgerufen.
- 2. Klicken Sie auf **RAS-Richtlinien**.
- 3. Löschen Sie die beiden vorhandenen Richtlinien: Verbindungen mit anderen Zugriffsservern sowie mit dem Microsoft Routing- und RAS-Server. Rechtsklicken Sie auf jeden Richtliniennamen und wählen Sie **Löschen**.
- 4. Rechtsklicken Sie auf **RAS-Richtlinien** und wählen Sie dann **Neue RAS-Richtlinie**.
Das Fenster „Assistent für neue RAS-Richtlinien“ wird angezeigt.
- 5. Klicken Sie auf **Weiter**.

6. Wählen Sie die Schaltfläche **Benutzerdefinierte Richtlinie einrichten**. Geben Sie im entsprechenden Feld einen Namen für die RAS-Richtlinie ein. Geben Sie beispielsweise „VPN-Benutzerzugriff gewähren“ als Namen für die RAS-Richtlinie ein. Klicken Sie auf **Weiter**.
7. Klicken Sie auf **Hinzufügen**, um die entsprechenden Bedingungen für die Richtlinie festzulegen.
8. Führen Sie einen der folgenden Schritte aus:
 - Falls alle Benutzer ungeachtet ihrer Domänengruppe Zugriff benötigen, fahren Sie mit dem nächsten Schritt fort.
 - Falls nur bestimmte Domänengruppen Zugriff benötigen, fahren Sie mit Schritt 11 fort.
9. Wählen Sie die Richtlinienbedingung **Tag- und Uhrzeiteinschränkungen**, wenn alle Benutzer ungeachtet ihrer Domänengruppe Zugriff benötigen. Klicken Sie auf **Hinzufügen**.

Hinweis: Die Richtlinienbedingung „Tag- und Uhrzeiteinschränkungen“ ermöglicht allen Benutzern Zugriff, während mit der Richtlinienbedingung „Windows-Gruppen“ der Zugriff auf Domänengruppen beschränkt werden kann.
10. Wählen Sie die Schaltfläche **Zugelassen** und klicken Sie dann auf **OK**. Fahren Sie mit Schritt 15 fort.
11. Wählen Sie die Richtlinienbedingung **Windows-Gruppen**, wenn nur bestimmte Domänengruppen Zugriff benötigen. Klicken Sie auf **Hinzufügen**.

Hinweis: Die Richtlinienbedingung „Windows-Gruppen“ beschränkt den Zugriff auf Domänengruppen, während die Richtlinienbedingung „Tag- und Uhrzeiteinschränkungen“ allen Benutzern Zugriff ermöglicht.
12. Klicken Sie auf **Hinzufügen**, um die Domänengruppen hinzuzufügen, auf die diese RAS-Richtlinie zutreffen soll.
13. Geben Sie den Namen der Domänengruppen ein. Beispielsweise ist „DOCLAB\VPN Users“ eine gültige Domänengruppe. Klicken Sie auf **OK**.

Wiederholen Sie die Schritte 12 und 13, um weitere Domänengruppen hinzuzufügen.
14. Klicken Sie auf **OK**, wenn die Domänengruppen festgelegt sind.

Im Gruppen-Fenster werden alle hinzugefügten Domänengruppen angezeigt.
15. Klicken Sie auf **Weiter**.

Hinweis: Die angezeigten Richtlinienbedingungen hängen davon ab, ob die „Tag- und Uhrzeiteinschränkungen“ oder „Windows-Gruppen“ festgelegt wurden.
16. Klicken Sie auf die Schaltfläche **RAS-Berechtigung erteilen**. Klicken Sie auf **Weiter**.
17. Klicken Sie auf **Profil bearbeiten**.

18. Klicken Sie auf die Registerkarte **Authentifizierung**. Aktivieren Sie die Kontrollkästchen für die entsprechenden Authentifizierungsmethoden. Klicken Sie auf **OK**.

Hinweis:

- Bei einer LDAP-Implementierung müssen Sie das Kontrollkästchen „Unverschlüsselte Authentifizierung (PAP, SPAP)“ wählen.
- Wenn Sie die Kontrollkästchen für „Verschlüsselte Authentifizierung (CHAP)“ oder „Unverschlüsselte Authentifizierung (PAP, SPAP)“ wählen, wird ein Dialogfeld angezeigt, das danach fragt, ob Zugriff auf die Online-Hilfe benötigt wird. Klicken Sie auf **Nein**.

19. Klicken Sie auf die Registerkarte **Erweitert**. Klicken Sie auf **Hinzufügen**.
20. Wählen Sie **Ignore-User-Dialin-Properties** aus der Attributliste aus. Klicken Sie auf **Hinzufügen**.
21. Wählen Sie die Option **True**. Klicken Sie auf **OK**.
22. Klicken Sie auf **Schließen**. Klicken Sie auf **OK**.
23. Klicken Sie auf **Weiter**.
24. Prüfen Sie die Angaben der RAS-Richtlinie und klicken Sie auf **Fertigstellen**.

9.5.3 Deaktivieren der IAS-Protokollierung für erfolgreiche Authentifizierungsanforderungen (optional)

Um die Anzahl der Ereignisprotokollmeldungen zu reduzieren, empfiehlt es sich, die Protokollierung für erfolgreiche Authentifizierungsanforderungen zu deaktivieren.

Hinweis: Führen Sie diese Anweisungen auf allen Compliance Anwendungsservern und RADIUS Enforcer-Servern aus.

1. Klicken Sie im Startmenü des Compliance Anwendungsservers oder eines RADIUS Enforcer-Servers auf **Verwaltung > Internetauthentifizierungsdienst** .
IAS wird aufgerufen.
2. Rechtsklicken Sie auf **Internetauthentifizierungsdienst** und wählen Sie dann **Eigenschaften**.
3. Deaktivieren Sie das Kontrollkästchen für **Erfolgreiche Authentifizierungsanforderungen** und klicken Sie auf **Übernehmen**.
4. Schließen Sie IAS.
5. Wiederholen Sie diese Schritte auf allen Compliance Anwendungsservern und RADIUS Enforcer-Servern.

9.5.4 Hinzufügen eines RADIUS Clients für jedes Netzwerkgerät (optional)

Folgende Anweisungen sind nur für die Durchsetzung von RADIUS erforderlich. Die Durchsetzung von RADIUS wird mit VPN, 802.1x, Cisco NAC und erweiterten RADIUS-Implementierungen eingesetzt. Für jeden VPN-Gateway (VPN-Concentrator) müssen

Sie zu IAS einen RADIUS Client-Eintrag hinzufügen. Führen Sie diese Anweisungen auf allen Compliance Anwendungsservern und RADIUS Enforcer-Servern aus.

1. Klicken Sie im Startmenü des Compliance Anwendungsservers oder eines RADIUS Enforcer-Servers auf **Verwaltung > Internetauthentifizierungsdienst** .
IAS wird aufgerufen.
2. Rechtsklicken Sie auf **RADIUS-Clients** und wählen Sie dann **Neuer RADIUS-Client**.
Das Fenster „Neuer RADIUS-Client“ wird angezeigt.
3. Geben Sie einen Namen und die IP-Adresse oder den DNS-Namen ein, über die der VPN-Gateway sich mit dem Compliance Anwendungsserver verbindet. Klicken Sie auf **Weiter**.
4. Geben Sie den gemeinsamen geheimen Schlüssel des VPN-Gateways in die entsprechenden Felder ein und bestätigen Sie ihn. Dabei handelt es sich um den gleichen gemeinsamen geheimen Schlüssel, der bei der Konfiguration des VPN-Gateways verwendet wurde.
Hinweis: Im Listenfeld „Clienthersteller“ muss der RADIUS-Standard ausgewählt sein.
5. Das Kontrollkästchen **Anforderung muss das Attribut „Message Authenticator“** enthalten darf **nicht** aktiviert sein.
6. Klicken Sie auf **Fertigstellen**.
Wiederholen Sie diese Anweisungen für jeden VPN-Concentrator, der mit Sophos NAC Advanced verwendet wird. Wiederholen Sie diese Schritte auf allen Compliance Anwendungsservern und RADIUS Enforcer-Servern.

9.6 Netzwerkrichtlinienserver-Einstellungen (Windows Server 2008)

Der Netzwerkrichtlinienserver wird für die Suche nach und für die Authentifizierung von Gruppen sowie zur Durchsetzung von RADIUS verwendet.

Die meisten Sophos NAC Advanced-Implementierungen erfordern die Suche nach und Authentifizierung von Gruppen. Sie müssen folgendermaßen vorgehen:

- Gewähren Sie dem Netzwerkrichtlinienserver Zugriff auf Active Directory.

Hinweis: Bei LDAP-Implementierungen, oder wenn Sie Sophos NAC Advanced als einen RADIUS-Proxy verwenden (indem Sophos NAC Advanced vor einem anderen RADIUS-Server im Proxymodus konfiguriert wird), müssen Sie diesen Schritt **nicht** durchführen.

- Erstellen Sie eine Netzwerkrichtlinie.

Wenn RADIUS Enforcement mit VPN, 802.1x, Cisco NAC oder erweiterten RADIUS-Implementierungen verwendet wird, müssen Sie folgendermaßen vorgehen:

- Gewähren Sie dem Netzwerkrichtlinienserver Zugriff auf Active Directory.
- Konfigurieren Sie eine Netzwerkrichtlinie.
- Fügen Sie für jedes Gerät, das auf das Netzwerk zugreifen kann, wie VPN-Concentrators, RADIUS Clients hinzu.

9.6.1 Freigeben des Zugriffs auf Active Directory für den Netzwerkrichtlinienserver

Standardmäßig hat der Netzwerkrichtlinienserver-Dienst **keine** Rechte, Benutzer in Active Directory zu authentifizieren. Der Netzwerkrichtlinienserver benötigt das Recht, Benutzer in Active Directory authentifizieren zu können.

Wichtig:

- Bei LDAP-Implementierungen, oder wenn Sie Sophos NAC Advanced als einen RADIUS-Proxy verwenden (indem Sophos NAC Advanced vor einem anderen RADIUS-Server im Proxymodus konfiguriert wird), müssen Sie diesen Schritt **nicht** durchführen.
 - Die genannten Schritte müssen auf allen Compliance Anwendungsservern und auf allen RADIUS Enforcer-Servern durchgeführt werden.
1. Melden Sie sich auf einem Compliance Anwendungsserver oder RADIUS Enforcer-Server mit Administratorrechten an.
 2. Klicken Sie im Startmenü des Compliance Anwendungsservers oder eines RADIUS Enforcer-Servers auf **Verwaltung > Netzwerkrichtlinienserver** .
Der Netzwerkrichtlinienserver wird geöffnet.
 3. Rechtsklicken Sie auf **NPS (Lokal)** und wählen Sie dann **Server im Active Directory registrieren**.
 4. Klicken Sie auf **OK**, um den Netzwerkrichtlinienserverzugriff auf Active Directory zu bestätigen.
Wenn der Netzwerkrichtlinienserver auf Active Directory zugreifen kann, erhalten Sie eine darauf hinweisende Meldung. Es sind keine weiteren Schritte erforderlich.
 5. Verlassen Sie den Netzwerkrichtlinienserver.
 6. Wiederholen Sie diese Schritte auf allen Compliance Anwendungsservern und RADIUS Enforcer-Servern.

9.6.2 Konfigurieren einer Netzwerkrichtlinie

Für die meisten Sophos NAC Advanced-Implementierungen muss eine Netzwerkrichtlinie erstellt werden. Dieses Dokument beschreibt nur eine häufig verwendete Netzwerkrichtlinie für VPN. Sophos NAC Advanced NAC-Implementierungen für LAN erfordern eine Netzwerkrichtlinie für die Suche nach und Authentifizierung von Gruppen.

Wichtig:

- Netzwerkrichtlinien müssen **nicht** konfiguriert werden, wenn Sie Sophos NAC Advanced als Proxy verwenden (indem Sophos NAC Advanced vor einem anderen RADIUS-Server im Proxymodus konfiguriert wird).

- Die genannten Schritte müssen auf allen Compliance Anwendungsservern und auf allen RADIUS Enforcer-Servern durchgeführt werden.
1. Klicken Sie im Startmenü des Compliance Anwendungsservers oder eines RADIUS Enforcer-Servers auf **Verwaltung > Netzwerkrichtlinienserver** .
Der Netzwerkrichtlinienserver wird geöffnet.
 2. Klicken Sie im Bereich „Richtlinien“ auf **Netzwerkrichtlinien**.
 3. Löschen Sie die beiden vorhandenen Richtlinien: Verbindungen mit anderen Zugriffsservern sowie mit dem Microsoft Routing- und RAS-Server. Rechtsklicken Sie auf jeden Richtliniennamen und wählen Sie **Löschen**.
 4. Rechtsklicken Sie auf **Netzwerkrichtlinien** und wählen Sie **Neu**.
Das Fenster „Assistent für neue Netzwerkrichtlinie“ wird angezeigt.
 5. Geben Sie einen Richtliniennamen ein. Die Netzwerkverbindungsmethode sollte **Nicht angegeben** lauten. Geben Sie beispielsweise „VPN-Benutzerzugriff gewähren“ als Namen für die Netzwerkrichtlinie ein. Klicken Sie auf **Weiter**.
 6. Klicken Sie auf **Hinzufügen**, um die entsprechenden Bedingungen für die Richtlinie festzulegen.
 7. Führen Sie einen der folgenden Schritte aus:
 - Falls alle Benutzer ungeachtet ihrer Domänengruppe Zugriff benötigen, fahren Sie mit dem nächsten Schritt fort.
 - Falls nur bestimmte Domänengruppen Zugriff benötigen, fahren Sie mit Schritt 10 fort.
 8. Wählen Sie die Richtlinienbedingung **Tag- und Uhrzeiteinschränkungen**, wenn alle Benutzer ungeachtet ihrer Domänengruppe Zugriff benötigen. Klicken Sie auf **Hinzufügen**.
Hinweis: Die Richtlinienbedingung „Tag- und Uhrzeiteinschränkungen“ ermöglicht allen Benutzern Zugriff, während mit der Richtlinienbedingung „Windows-Gruppen“ der Zugriff auf Domänengruppen beschränkt werden kann.
 9. Wählen Sie die Schaltfläche **Zugelassen** und klicken Sie dann auf **OK**. Fahren Sie mit Schritt 14 fort.
 10. Wählen Sie die Richtlinienbedingung **Windows-Gruppen**, wenn nur bestimmte Domänengruppen Zugriff benötigen. Klicken Sie auf **Hinzufügen**.
Hinweis: Die Richtlinienbedingung „Windows-Gruppen“ beschränkt den Zugriff auf Domänengruppen, während die Richtlinienbedingung „Tag- und Uhrzeiteinschränkungen“ allen Benutzern Zugriff ermöglicht.
 11. Klicken Sie auf **Hinzufügen**, um die Domänengruppen hinzuzufügen, auf die diese Netzwerkrichtlinie zutreffen soll.
 12. Geben Sie den Namen der Domänengruppen ein. Beispielsweise ist „DOCLAB\VPN Users“ eine gültige Domänengruppe. Klicken Sie auf **OK**.
Wiederholen Sie die Schritte 11 und 12, um weitere Domänengruppen hinzuzufügen.
 13. Klicken Sie auf **OK**, wenn die Domänengruppen festgelegt sind.
Im Windows-Gruppen-Fenster werden alle hinzugefügten Domänengruppen angezeigt.

14. Klicken Sie auf **Weiter**.

Hinweis: Die angezeigten Richtlinienbedingungen hängen davon ab, ob die „Tag- und Uhrzeiteinschränkungen“ oder „Windows-Gruppen“ festgelegt wurden.

15. Klicken Sie auf die Option **Zugriff gewährt**. Klicken Sie auf **Weiter**.

16. Aktivieren Sie die Kontrollkästchen für die entsprechenden Authentifizierungsmethoden. Klicken Sie auf **Weiter**.

Hinweis:

- Bei einer LDAP-Implementierung müssen Sie das Kontrollkästchen „Unverschlüsselte Authentifizierung (PAP, SPAP)“ wählen.
- Wenn Sie die Kontrollkästchen für „Verschlüsselte Authentifizierung (CHAP)“ oder „Unverschlüsselte Authentifizierung (PAP, SPAP)“ wählen, wird ein Dialogfeld angezeigt, das danach fragt, ob Zugriff auf die Online-Hilfe benötigt wird. Klicken Sie auf **Nein**.

17. Klicken Sie auf **Weiter**. Für diese Richtlinie sind keine Einschränkungen erforderlich.

18. Klicken Sie auf **Weiter**. Für diese Richtlinie ist keine weitere Konfiguration erforderlich.

19. Prüfen Sie die Details der Netzwerkrichtlinie und klicken Sie auf **Fertigstellen**.

9.6.3 Deaktivieren der Netzwerkrichtlinienserverprotokollierung für erfolgreiche Authentifizierungsanforderungen (optional)

Um die Anzahl der Ereignisprotokollmeldungen zu reduzieren, empfiehlt es sich, die Protokollierung für erfolgreiche Authentifizierungsanforderungen zu deaktivieren.

Hinweis: Führen Sie diese Anweisungen auf allen Compliance Anwendungsservern und RADIUS Enforcer-Servern aus.

1. Klicken Sie im Startmenü des Compliance Anwendungsservers oder eines RADIUS Enforcer-Servers auf **Verwaltung > Netzwerkrichtlinienserver** .

Der Netzwerkrichtlinienserver wird geöffnet.

2. Rechtsklicken Sie auf **NPS (Lokal)** und wählen Sie **Eigenschaften**.

3. Deaktivieren Sie das Kontrollkästchen für **Erfolgreiche Authentifizierungsanforderungen** und klicken Sie auf **Übernehmen**.

4. Verlassen Sie den Netzwerkrichtlinienserver.

5. Wiederholen Sie diese Schritte auf allen Compliance Anwendungsservern und RADIUS Enforcer-Servern.

9.6.4 Hinzufügen eines RADIUS Clients für jedes Netzwerkgerät (optional)

Folgende Anweisungen sind nur für die Durchsetzung von RADIUS erforderlich. Die Durchsetzung von RADIUS wird mit VPN, 802.1x, Cisco NAC und erweiterten RADIUS-Implementierungen eingesetzt. Für jeden VPN-Gateway (VPN-Concentrator) müssen

Sie zu Netzwerkrichtlinienserver einen RADIUS Client-Eintrag hinzufügen. Führen Sie diese Anweisungen auf allen Compliance Anwendungsservern und RADIUS Enforcer-Servern aus.

1. Klicken Sie im Startmenü des Compliance Anwendungsservers oder eines RADIUS Enforcer-Servers auf **Verwaltung > Netzwerkrichtlinienserver** .
Der Netzwerkrichtlinienserver wird geöffnet.
2. Rechtsklicken Sie unter „RADIUS Clients and Servers“ auf **RADIUS Clients** und wählen Sie **New RADIUS Client**.
Das Fenster „Neuer RADIUS-Client“ wird angezeigt.
3. Geben Sie einen Namen und die IP-Adresse oder den DNS-Namen ein, über die der VPN-Gateway sich mit dem Compliance Anwendungsserver verbindet. Klicken Sie auf **Weiter**.
4. Geben Sie den gemeinsamen geheimen Schlüssel des VPN-Gateways in die entsprechenden Felder ein und bestätigen Sie ihn. Dabei handelt es sich um den gleichen gemeinsamen geheimen Schlüssel, der bei der Konfiguration des VPN-Gateways verwendet wurde.
Hinweis: Im Listenfeld „Vendor name“ muss der RADIUS-Standard ausgewählt sein.
5. Das Kontrollkästchen **Anforderung muss das Attribut „Message Authenticator“** enthalten darf **nicht** aktiviert sein.
6. Klicken Sie auf **OK**.
Wiederholen Sie diese Anweisungen für jeden VPN-Concentrator, der mit Sophos NAC Advanced verwendet wird. Wiederholen Sie diese Schritte auf allen Compliance Anwendungsservern und RADIUS Enforcer-Servern.

9.7 Sophos NAC Advanced als RADIUS-Proxy (Windows Server 2003) (Optional)

Wenn Sie Sophos NAC Advanced als RADIUS-Proxy verwenden möchten (indem Sophos NAC Advanced vor einem anderen RADIUS-Server im Proxymodus konfiguriert wird), muss die IAS-Konfiguration geändert werden. Wenn Sophos NAC Advanced als RADIUS-Proxy eingesetzt wird, muss keine RAS-Richtlinie erstellt werden. Stattdessen muss eine Verbindungsanforderungsrichtlinie erstellt und eine Remote-RADIUS-Servergruppe verwendet werden.

Hinweis: Die genannten Schritte müssen auf allen Compliance Anwendungsservern und auf allen RADIUS Enforcer-Servern durchgeführt werden.

9.7.1 Hinzufügen einer Remote-RADIUS-Servergruppe

1. Klicken Sie im Startmenü des Compliance Anwendungsservers oder eines RADIUS Enforcer-Servers auf **Verwaltung > Internetauthentifizierungsdienst** .
IAS wird aufgerufen.
2. Klicken Sie auf **Verbindungsanforderungsverarbeitung**.

3. Rechtsklicken Sie auf **Remote-RADIUS-Servergruppe** und wählen Sie dann **Neue Remote-RADIUS-Servergruppe**.
Das Fenster „Assistent für neue Remote-RADIUS-Servergruppe“ wird angezeigt.
4. Klicken Sie auf **Weiter**.
5. Wählen Sie die Schaltfläche **Typisch** und geben Sie dann im entsprechenden Feld den Namen der Servergruppe ein.
6. Klicken Sie auf **Weiter**.
7. Geben Sie die IP-Adresse Ihres primären Remote-RADIUS-Servers in das entsprechende Feld ein.
8. Geben Sie die IP-Adresse Ihres Backup-Remote-RADIUS-Servers ein oder deaktivieren Sie das Kontrollkästchen **Reserveserver für diese Gruppe einrichten**.
9. Geben Sie den gemeinsamen geheimen Schlüssel (Shared Secret) der Servergruppe ein und bestätigen Sie ihn durch erneute Eingabe.
10. Klicken Sie auf **Weiter**.
11. Prüfen Sie, ob das Kontrollkästchen für **Assistent für neue Verbindungsanforderungsrichtlinien nach Abschluss dieses Assistenten starten** ausgewählt ist.
12. Prüfen Sie die Angaben für die Remote-RADIUS-Servergruppe und klicken Sie auf **Fertigstellen**.
13. Rufen Sie [Erstellen einer Verbindungsanforderungsrichtlinie](#) (Seite 40) auf.

9.7.2 Erstellen einer Verbindungsanforderungsrichtlinie

Wenn Sie Sophos NAC Advanced als RADIUS-Proxy verwenden, müssen Sie eine Verbindungsanforderungsrichtlinie erstellen.

1. Führen Sie einen der folgenden Schritte aus:
 - Wenn Sie den im vorigen Abschnitt gestarteten Assistenten verwenden, fahren Sie mit dem nächsten Schritt fort.
 - Klicken Sie im Startmenü des Compliance Anwendungsservers oder eines RADIUS Enforcer-Servers auf **Verwaltung > Internetauthentifizierungsdienst**. IAS wird aufgerufen. Doppelklicken Sie auf **Verbindungsanforderungsverarbeitung**. Rechtsklicken Sie auf **Verbindungsanforderungsrichtlinien** und dann auf **Neu Verbindungsanforderungsrichtlinie**.

Das Fenster „Assistent für neue Verbindungsanforderungsrichtlinie“ wird angezeigt.

2. Klicken Sie auf **Weiter**.
3. Wählen Sie die Schaltfläche **Typische Richtlinie für ein allgemeines Szenario**.
4. Geben Sie einen Richtliniennamen für die Verbindungsanforderungsrichtlinie ein.
5. Klicken Sie auf **Weiter**.
6. Wählen Sie die Schaltfläche **Verbindungsanforderungen an Remote-RADIUS-Server zur Authentifizierung weiterleiten**.
7. Klicken Sie auf **Weiter**.

8. Geben Sie den/die Bereichsnamen ein, für die Sie einen Proxy verwenden, oder einen Platzhalter .*, wenn Sie für alle Bereiche einen Proxy verwenden.
9. Deaktivieren Sie das Kontrollkästchen für **Bereichsnamen vor der Authentifizierung vom Benutzernamen entfernen**.
10. Wählen Sie die erstellte Servergruppe aus dem Listenfenster.
11. Klicken Sie auf **Weiter**.
12. Klicken Sie auf **Fertigstellen**.
13. Rufen Sie [Prüfen der Richtlinienbedingungen](#) (Seite 41) auf.

9.7.3 Prüfen der Richtlinienbedingungen

1. Rechtsklicken Sie in der Liste der Verbindungsanforderungsrichtlinien in IAS auf die gerade erstellte Richtlinie und wählen Sie dann **Eigenschaften**.

Das Eigenschaften-Fenster wird angezeigt.

2. Prüfen Sie die Richtlinienbedingungen der erstellten Richtlinie.
3. Sollten die Richtlinienbedingungen falsch oder unvollständig sein, klicken Sie auf **Hinzufügen** oder **Bearbeiten**, um sie zu ändern.

Hinweis: Wenn eine Richtlinienbedingung stellvertretend für alle Benutzer gelten soll, legen Sie die Tageszeit als Bedingung mit der Einstellung **24x7** fest.

4. Klicken Sie auf **OK**.
5. Fahren Sie mit [Ändern der RADIUS-Authentifizierungs- und Kontoführungsports](#) (Seite 41) fort.

9.7.4 Ändern der RADIUS-Authentifizierungs- und Kontoführungsports

Die Standard-RADIUS-Authentifizierungs- und Kontoführungsports sind auf 1812 und 1813 festgelegt. Wenn andere Authentifizierungs- und Kontoführungsports verwendet werden, müssen diese geändert werden.

Hinweis: Als Authentifizierungsport wird häufig Port 1645 verwendet, und als Kontoführungsport ist Port 1646 verbreitet.

1. Rechtsklicken Sie in der Liste der Remote-RADIUS-Servergruppen von IAS auf die gerade erstellte Servergruppe und wählen Sie **Eigenschaften**.

Das Eigenschaften-Fenster wird angezeigt.

2. Wählen Sie den ersten Server in der Liste der Server, die Sie zu dieser Gruppe hinzugefügt haben und klicken Sie dann auf **Eigenschaften**.
3. Klicken Sie auf die Registerkarte **Authentifizierung/Kontoführung**.
4. Ändern Sie ggf. den Authentifizierungsport, den gemeinsamen geheimen Schlüssel und den Kontoführungsport.

Hinweis: Als Authentifizierungsport wird häufig Port 1645 verwendet, und als Kontoführungsport ist Port 1646 verbreitet.

5. Wiederholen Sie Schritte 2 bis 5, um die Authentifizierungs- und Kontoführungsports für alle weiteren Server in der Servergruppe festzulegen.
6. Klicken Sie auf **OK**.
7. Fahren Sie mit [Ändern des Registrierungsauthentifizierungsprotokolls in der Registrierungsschnittstelle](#) (Seite 42) fort.

9.7.5 Ändern des Registrierungsauthentifizierungsprotokolls in der Registrierungsschnittstelle

Sophos NAC Advanced verwendet MSchapV2 RADIUS als Standard-Authentifizierungsprotokoll. Sollte Ihr Remote-RADIUS-Server dieses Authentifizierungsprotokoll nicht verwenden, muss das RADIUS-Authentifizierungsprotokoll in der Registrierungsschnittstelle geändert werden.

1. Suchen Sie auf dem Anwendungsserver die Datei „Web.config“ für das Registration Interface auf dem Compliance Anwendungsserver oder dem RADIUS Enforcer-Server. Wenn Sophos NAC Advanced im Standardverzeichnis installiert wurde, befindet sich die Datei unter folgendem Pfad: `<lokales Laufwerk>\inetpub\wwwroot\RegistrationInterface\web.config`.
2. Öffnen Sie die Datei „Web.config“ in einem Texteditor.
3. Suchen Sie den Bereich **authInterface** und den untergeordneten Bereich **radius**.
4. Geben Sie in der Zeile `<add key="authType" value =mschapv2">` als Wert (value) das RADIUS-Authentifizierungsprotokoll an, das von Ihrem Remote-RADIUS-Server installiert wird.

Der geänderte Abschnitt sollte wie folgt aussehen:

```
<radius>
<add key="authType" value="Ihr
Remote-RADIUS-Authentifizierungsprotokoll"/> <add
key="serverRetries" value="1"/> <add key="listRetries"
value="1"/> </radius>
```

5. Speichern und schließen Sie die Datei.
6. Sie können nun mit dem folgenden Abschnitt fortfahren.

9.7.6 Konfigurieren des RADIUS-Servers für Gruppenverknüpfungen/-profile (optional)

Sie können sowohl Sophos NAC Advanced als auch den RADIUS-Server für Gruppenverknüpfungen verwenden. Für beide Konfigurationen müssen Gruppen mit Sophos NAC Advanced erstellt werden. Weitere Informationen finden Sie in der Compliance Manager Hilfe.

Um Gruppenverknüpfungen/-profile des RADIUS-Servers mit Sophos NAC Advanced verwenden zu können, müssen Sie die Gruppeninformationen über ein RADIUS-Paket mit einem herstellerspezifischen Attribut (VSA) an Sophos NAC Advanced senden. Weitere Informationen zur Ausgabe von VSA finden Sie in Ihren RADIUS-Benutzerdokumenten.

Sophos Vendor-Specific Attribute (VSA)

Die Syntax des VSA basiert auf den Richtlinien, die in Abschnitt 5.26 des RADIUS-Dokuments (URL RFC2685) unter <http://www.rfc-archive.org/getrfc.php?rfc=2865> beschrieben werden.

Sophos Vendor ID

Die Vendor ID identifiziert den Hersteller. Die Sophos Vendor ID lautet 5428 (dezimal) oder 0x00001534 (hexadezimal in Netzwerkfolge).

EF-GroupID VSA

Das EF-GroupID VSA weist darauf hin, welche Gruppe zur Durchsetzung der Sitzungseinstellungen für einen authentifizierten Benutzer verwendet werden.

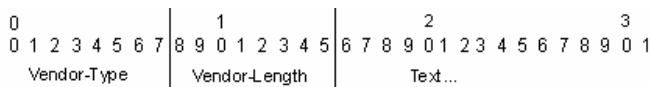
Die RADIUS Enforcer Access Templates bestimmen den Netzwerkzugriff. Zuerst werden jedoch Ausnahmen berücksichtigt. Bei Ausschluss einer Anforderung wird Netzwerkzugriff ungeachtet der Gruppe zugelassen. In der folgenden Tabelle werden die Szenarien beschrieben, wenn eine Standardrichtlinie in Compliance Manager festgelegt wird oder nicht:

Szenarien	Standardrichtlinie ist angegeben	Standardrichtlinie ist nicht angegeben
EF-GroupID VSA ist nicht vorhanden	Die Standardrichtlinie wird übernommen. Netzwerkzugriff wird ermittelt, wenn eine RADIUS Enforcer Access Template mit der Anforderung übereinstimmt. Mit der Richtlinie verbundene RADIUS Enforcer Access Templates werden zuerst analysiert. Wenn keine Übereinstimmung gefunden wird, werden die Standard RADIUS Enforcer Access Templates analysiert. Wenn keine Übereinstimmung gefunden werden kann, wird der Netzwerkzugriff verweigert.	Es wird keine Richtlinie zugewiesen. Netzwerkzugriff wird ermittelt, wenn eine RADIUS Enforcer Access Template mit der Anforderung übereinstimmt. Die Standard RADIUS Enforcer Access Templates werden zuerst analysiert. Wenn keine Übereinstimmung gefunden werden kann, wird der Netzwerkzugriff verweigert.
EF-GroupID VSA ist nicht vorhanden oder wurde nicht definiert.	Die Standardrichtlinie wird übernommen. Netzwerkzugriff wird ermittelt, wenn eine RADIUS Enforcer Access Template mit der Anforderung übereinstimmt. Mit der Richtlinie verbundene RADIUS Enforcer Access Templates werden zuerst analysiert. Wenn keine Übereinstimmung gefunden wird, werden die Standard RADIUS Enforcer Access Templates analysiert. Wenn keine Übereinstimmung gefunden werden	Es wird keine Richtlinie zugewiesen. Netzwerkzugriff wird ermittelt, wenn eine RADIUS Enforcer Access Template mit der Anforderung übereinstimmt. Die Standard RADIUS Enforcer Access Templates werden zuerst analysiert. Wenn keine Übereinstimmung gefunden werden kann, wird der Netzwerkzugriff verweigert.

Szenarien	Standardrichtlinie ist angegeben	Standardrichtlinie ist nicht angegeben
	kann, wird der Netzwerkzugriff verweigert.	
EF-GroupID VSA ist gültig	Der Benutzer wird in einer bestimmten Gruppe abgelegt und die damit verbundene Richtlinie übernommen. Netzwerkzugriff wird ermittelt, wenn eine RADIUS Enforcer Access Template mit der Anforderung übereinstimmt. Mit der Richtlinie verbundene RADIUS Enforcer Access Templates werden zuerst analysiert. Wenn keine Übereinstimmung gefunden wird, werden die Standard RADIUS Enforcer Access Templates analysiert. Wenn keine Übereinstimmung gefunden werden kann, wird der Netzwerkzugriff verweigert.	Der Benutzer wird in einer bestimmten Gruppe abgelegt und die damit verbundene Richtlinie übernommen. Netzwerkzugriff wird ermittelt, wenn eine RADIUS Enforcer Access Template mit der Anforderung übereinstimmt. Mit der Richtlinie verbundene RADIUS Enforcer Access Templates werden zuerst analysiert. Wenn keine Übereinstimmung gefunden wird, werden die Standard RADIUS Enforcer Access Templates analysiert. Wenn keine Übereinstimmung gefunden werden kann, wird der Netzwerkzugriff verweigert.

EF-GroupID VSA-Format

Das Informationsformat für den EF-GroupID VSA-Wert wird in folgender Abbildung und Tabelle dargestellt. Die Felder werden von links nach rechts übertragen.



Vendor-Typ	Vendor-Länge	Text
20 (14 hexadezimal) für EF-User-Group	>2	<p>Das Textfeld besteht aus einem oder mehreren Oktetten visuell lesbarer Zeichen. Es darf nicht auf Null enden. Der Wert des Textfelds legt eine bestimmte Benutzergruppe für die authentifizierte Sitzung des Benutzers fest.</p> <p>Benutzergruppen-ID-Textparameter:</p> <ul style="list-style-type: none"> Maximal 253 Zeichen, die aus Zahlen und Buchstaben bestehen kann. Andere Zeichen sind nicht zulässig.

Vendor-Typ	Vendor-Länge	Text
		<ul style="list-style-type: none"> ■ Es muss nicht auf Groß- und Kleinschreibung geachtet werden. ■ Leerzeichen sind nicht zulässig.

EF-User-Group VSA-Beispiel

Wenn z.B. das VSA auf EF-User-Group = "WestCoastSales" gesetzt ist, besteht es aus den hexadezimalen Ziffern (Netzwerkfolge), die in der folgenden Tabelle beschrieben werden:

Beschreibung	Hexadezimale Ziffern
Kopfzeile	
Geben Sie folgenden Befehl ein: RADIUS-Attribut 26 (dezimal)	1A
Länge: Einschließlich Bytes für Typ und Länge	16
MSB der Vendor-ID ist immer 00	00
Sophos Vendor-ID	00 15 34
Vendor-Typ: EF-User-Group	14
Wertinformationen	
Vendor-Länge: Einschließlich Bytes für Typ und Länge	0E
Text: "WestCoastSales" (keine Anführungszeichen)	57 65 73 74 43 6F 61 73 74 53 61 6C 65 73

9.8 Sophos NAC Advanced als RADIUS-Proxy (Windows Server 2008) (Optional)

Wenn Sie Sophos NAC Advanced als RADIUS-Proxy verwenden möchten (indem Sophos NAC Advanced vor einem anderen RADIUS-Server im Proxymodus konfiguriert wird), muss die Konfiguration des Netzwerkrichtlinienservers geändert werden. Wenn Sophos NAC Advanced als RADIUS-Proxy eingesetzt wird, muss keine Netzwerkrichtlinie erstellt werden. Stattdessen muss eine Verbindungsanforderungsrichtlinie erstellt und eine Remote-RADIUS-Servergruppe verwendet werden.

Hinweis: Die genannten Schritte müssen auf allen Compliance Anwendungsservern und auf allen RADIUS Enforcer-Servern durchgeführt werden.

9.8.1 Hinzufügen einer Remote-RADIUS-Servergruppe

1. Klicken Sie im Startmenü des Compliance Anwendungsservers oder eines RADIUS Enforcer-Servers auf **Verwaltung > Netzwerkrichtlinienserver** .
Der Netzwerkrichtlinienserver wird geöffnet.
2. Rechtsklicken Sie unter „RADIUS-Clients und -Server“ auf **Remote-RADIUS-Servergruppen** und wählen Sie **Neuer RADIUS-Client**.
Das Fenster „Assistent für neue Remote-RADIUS-Servergruppe“ wird angezeigt.
3. Geben Sie einen Servergruppennamen in das entsprechende Feld ein.
4. Klicken Sie auf **Hinzufügen**.
5. Geben Sie die IP-Adresse Ihres Remote-RADIUS-Servers in das entsprechende Feld ein.
6. Klicken Sie auf die Registerkarte **Authentifizierung/Kontoführung**.
7. Geben Sie den gemeinsamer geheimen Schlüssel des RADIUS-Servers in das entsprechende Feld ein und wiederholen Sie die Eingabe.
8. Ändern Sie ggf. den Authentifizierungs- und Kontoführungsport.
Hinweis: Die Standard-RADIUS-Authentifizierungs- und Kontoführungsports lauten 1812 und 1813. Wenn andere Authentifizierungs- und Kontoführungsports verwendet werden, müssen diese geändert werden. Als Authentifizierungsport wird häufig Port 1645 verwendet, und als Kontoführungsport ist Port 1646 verbreitet.
9. Klicken Sie auf die Registerkarte **Lastenausgleich**.
10. Geben Sie die Priorität Ihres Remote-RADIUS-Servers im entsprechenden Feld an.
11. Klicken Sie auf **OK**.
12. Wiederholen Sie die Schritte 4 bis 11, um weitere RADIUS-Server für die Gruppe zu erstellen.
13. Prüfen Sie die Angaben für die Remote-RADIUS-Servergruppe und klicken Sie auf **OK**.
14. Rufen Sie [Erstellen einer Verbindungsanforderungsrichtlinie](#) (Seite 46) auf.

9.8.2 Erstellen einer Verbindungsanforderungsrichtlinie

Wenn Sie Sophos NAC Advanced als RADIUS-Proxy verwenden, müssen Sie eine Verbindungsanforderungsrichtlinie erstellen.

1. Klicken Sie im Startmenü des Compliance Anwendungsservers oder eines RADIUS Enforcer-Servers auf **Verwaltung > Netzwerkrichtlinienserver** .
Der Netzwerkrichtlinienserver wird geöffnet.
2. Rechtsklicken Sie unter „Richtlinien“ auf **Verbindungsanforderungsrichtlinien** und klicken Sie anschließend auf **Neu** .
Das Fenster „Assistent für neue Verbindungsanforderungsrichtlinie“ wird angezeigt.
3. Geben Sie einen Richtliniennamen ein. Die Netzwerkverbindungsmethode sollte **Nicht angegeben** lauten.

4. Klicken Sie auf **Weiter**.
5. Klicken Sie auf **Hinzufügen**, um die entsprechenden Bedingungen für die Richtlinie festzulegen.
6. Wählen Sie die entsprechende Bedingung aus und klicken Sie auf **Hinzufügen**.
7. Geben Sie eine Wert für die Bedingung an und klicken Sie auf **OK**.

Hinweis: Wenn Sie beispielsweise im letzten Schritt den Benutzernamen angegeben haben, können Sie in diesem Schritt angeben, dass der Name „mydomain.com“ umfassen soll.

8. Klicken Sie auf **Weiter**.
9. Wählen Sie im Abschnitt **Authentifizierung** die Option **Anforderungen an folgende Remote-RADIUS-Servergruppe zur Authentifizierung weiterleiten**.
10. Wählen Sie die erstellte RADIUSservergruppe aus dem Listenfenster.
11. Klicken Sie auf **Weiter**.
12. Wählen Sie im Abschnitt **Attribut** unter **Bereichsname angeben Benutzername** aus dem Listenfeld aus und klicken Sie auf **Hinzufügen**.
13. Geben Sie in das Feld **Suchen** den/die Bereichsnamen ein, für die Sie einen Proxy verwenden, oder einen Platzhalter *****, wenn Sie für alle Bereiche einen Proxy verwenden.
14. Lassen Sie das Feld **Ersetzen durch** frei.
15. Klicken Sie auf **OK**.
16. Klicken Sie auf **Weiter**.
17. Klicken Sie auf **Fertigstellen**.
18. Rufen Sie [Prüfen der Richtlinienbedingungen](#) (Seite 47) auf.

9.8.3 Prüfen der Richtlinienbedingungen

1. Klicken Sie im Bereich „Netzwerkrichtlinienserver“ unter „Richtlinien“ auf **Verbindungsanforderungsrichtlinien**. Rechtsklicken Sie in der Richtlinienliste auf die soeben erstellte Richtlinie und wählen Sie anschließend **Eigenschaften**.

Das Eigenschaften-Fenster wird angezeigt.

2. Klicken Sie auf die Registerkarte **Bedingungen**, um die Richtlinienbedingungen für die erstellte Richtlinie zu überprüfen.
3. Sollten die Richtlinienbedingungen falsch oder unvollständig sein, klicken Sie auf **Hinzufügen** oder **Bearbeiten**, um sie zu ändern.

Hinweis: Wenn eine Richtlinienbedingung stellvertretend für alle Benutzer gelten soll, legen Sie Tag- und Uhrzeiteinschränkungen als Bedingung mit der Einstellung **24x7** fest.

4. Klicken Sie auf **OK**.
5. Rufen Sie [Ändern des Registrierungsauthentifizierungsprotokolls in der Registrierungsschnittstelle](#) (Seite 48) auf.

9.8.4 Ändern des Registrierungsauthentifizierungsprotokolls in der Registrierungsschnittstelle

Sophos NAC Advanced verwendet MSchapV2 RADIUS als Standard-Authentifizierungsprotokoll. Sollte Ihr Remote-RADIUS-Server dieses Authentifizierungsprotokoll nicht verwenden, muss das RADIUS-Authentifizierungsprotokoll in der Registrierungsschnittstelle geändert werden.

1. Suchen Sie auf dem Anwendungsserver die Datei „Web.config“ für das Registration Interface auf dem Compliance Anwendungsserver oder dem RADIUS Enforcer-Server. Wenn Sophos NAC Advanced im Standardverzeichnis installiert wurde, befindet sich die Datei unter folgendem Pfad: <lokales Laufwerk>\inetpub\wwwroot\RegistrationInterface\web.config.
2. Öffnen Sie die Datei „Web.config“ in einem Texteditor.
3. Suchen Sie den Bereich **authInterface** und den untergeordneten Bereich **radius**.
4. Geben Sie in der Zeile <add key="authType" value="mschap2"> als Wert (value) das RADIUS-Authentifizierungsprotokoll an, das von Ihrem Remote-RADIUS-Server installiert wird.

Der geänderte Abschnitt sollte wie folgt aussehen:

```
<radius>

<add key="authType" value="Ihr
Remote-RADIUS-Authentifizierungsprotokoll"/> <add
key="serverRetries" value="1"/> <add key="listRetries"
value="1"/> </radius>
```

5. Speichern und schließen Sie die Datei.
6. Auf Wunsch können Sie auch die Anweisungen im Abschnitt [Konfigurieren des RADIUS-Servers für Gruppenverknüpfungen/-profile \(optional\)](#) (Seite 48) durchführen.

9.8.5 Konfigurieren des RADIUS-Servers für Gruppenverknüpfungen/-profile (optional)

Sie können sowohl Sophos NAC Advanced als auch den RADIUS-Server für Gruppenverknüpfungen verwenden. Für beide Konfigurationen müssen Gruppen mit Sophos NAC Advanced erstellt werden. Weitere Informationen finden Sie in der Compliance Manager Hilfe.

Um Gruppenverknüpfungen/-profile des RADIUS-Servers mit Sophos NAC Advanced verwenden zu können, müssen Sie die Gruppeninformationen über ein RADIUS-Paket mit einem herstellerspezifischen Attribut (VSA) an Sophos NAC Advanced senden. Weitere Informationen zur Ausgabe von VSA finden Sie in Ihren RADIUS-Benutzerdokumenten.

Sophos Vendor-Specific Attribute (VSA)

Die Syntax des VSA basiert auf den Richtlinien, die in Abschnitt 5.26 des RADIUS-Dokuments (URL RFC2685) unter <http://www.rfc-archive.org/getrfc.php?rfc=2865> beschrieben werden.

Sophos Vendor ID

Die Vendor ID identifiziert den Hersteller. Die Sophos Vendor ID lautet 5428 (dezimal) oder 0x00001534 (hexadezimal in Netzwerkfolge).

EF-GroupID VSA

Das EF-GroupID VSA weist darauf hin, welche Gruppe zur Durchsetzung der Sitzungseinstellungen für einen authentifizierten Benutzer verwendet werden.

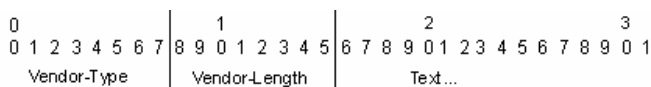
Die RADIUS Enforcer Access Templates bestimmen den Netzwerkzugriff. Zuerst werden jedoch Ausnahmen berücksichtigt. Bei Ausschluss einer Anforderung wird Netzwerkzugriff ungeachtet der Gruppe zugelassen. In der folgenden Tabelle werden die Szenarien beschrieben, wenn eine Standardrichtlinie in Compliance Manager festgelegt wird oder nicht:

Szenarien	Standardrichtlinie ist angegeben	Standardrichtlinie ist nicht angegeben
EF-GroupID VSA ist nicht vorhanden	Die Standardrichtlinie wird übernommen. Netzwerkzugriff wird ermittelt, wenn eine RADIUS Enforcer Access Template mit der Anforderung übereinstimmt. Mit der Richtlinie verbundene RADIUS Enforcer Access Templates werden zuerst analysiert. Wenn keine Übereinstimmung gefunden wird, werden die Standard RADIUS Enforcer Access Templates analysiert. Wenn keine Übereinstimmung gefunden werden kann, wird der Netzwerkzugriff verweigert.	Es wird keine Richtlinie zugewiesen. Netzwerkzugriff wird ermittelt, wenn eine RADIUS Enforcer Access Template mit der Anforderung übereinstimmt. Die Standard RADIUS Enforcer Access Templates werden zuerst analysiert. Wenn keine Übereinstimmung gefunden werden kann, wird der Netzwerkzugriff verweigert.
EF-GroupID VSA ist nicht vorhanden oder wurde nicht definiert.	Die Standardrichtlinie wird übernommen. Netzwerkzugriff wird ermittelt, wenn eine RADIUS Enforcer Access Template mit der Anforderung übereinstimmt. Mit der Richtlinie verbundene RADIUS Enforcer Access Templates werden zuerst analysiert. Wenn keine Übereinstimmung gefunden wird, werden die Standard RADIUS Enforcer Access Templates analysiert. Wenn keine Übereinstimmung gefunden werden kann, wird der Netzwerkzugriff verweigert.	Es wird keine Richtlinie zugewiesen. Netzwerkzugriff wird ermittelt, wenn eine RADIUS Enforcer Access Template mit der Anforderung übereinstimmt. Die Standard RADIUS Enforcer Access Templates werden zuerst analysiert. Wenn keine Übereinstimmung gefunden werden kann, wird der Netzwerkzugriff verweigert.
EF-GroupID VSA ist gültig	Der Benutzer wird in einer bestimmten Gruppe abgelegt und die damit verbundene Richtlinie	Der Benutzer wird in einer bestimmten Gruppe abgelegt und die damit verbundene Richtlinie

Szenarien	Standardrichtlinie ist angegeben	Standardrichtlinie ist nicht angegeben
	übernommen. Netzwerkzugriff wird ermittelt, wenn eine RADIUS Enforcer Access Template mit der Anforderung übereinstimmt. Mit der Richtlinie verbundene RADIUS Enforcer Access Templates werden zuerst analysiert. Wenn keine Übereinstimmung gefunden wird, werden die Standard RADIUS Enforcer Access Templates analysiert. Wenn keine Übereinstimmung gefunden werden kann, wird der Netzwerkzugriff verweigert.	übernommen. Netzwerkzugriff wird ermittelt, wenn eine RADIUS Enforcer Access Template mit der Anforderung übereinstimmt. Mit der Richtlinie verbundene RADIUS Enforcer Access Templates werden zuerst analysiert. Wenn keine Übereinstimmung gefunden wird, werden die Standard RADIUS Enforcer Access Templates analysiert. Wenn keine Übereinstimmung gefunden werden kann, wird der Netzwerkzugriff verweigert.

EF-GroupID VSA-Format

Das Informationsformat für den EF-GroupID VSA-Wert wird in folgender Abbildung und Tabelle dargestellt. Die Felder werden von links nach rechts übertragen.



Vendor-Typ	Vendor-Länge	Text
20 (14 hexadezimal) für EF-User-Group	>2	<p>Das Textfeld besteht aus einem oder mehreren Oktetten visuell lesbarer Zeichen. Es darf nicht auf Null enden. Der Wert des Textfelds legt eine bestimmte Benutzergruppe für die authentifizierte Sitzung des Benutzers fest.</p> <p>Benutzergruppen-ID-Textparameter:</p> <ul style="list-style-type: none"> ■ Maximal 253 Zeichen, die aus Zahlen und Buchstaben bestehen kann. Andere Zeichen sind nicht zulässig. ■ Es muss nicht auf Groß- und Kleinschreibung geachtet werden. ■ Leerzeichen sind nicht zulässig.

EF-User-Group VSA-Beispiel

Wenn z.B. das VSA auf EF-User-Group = "WestCoastSales" gesetzt ist, besteht es aus den hexadezimalen Ziffern (Netzwerkfolge), die in der folgenden Tabelle beschrieben werden:

Beschreibung	Hexadezimale Ziffern
Kopfzeile	
Geben Sie folgenden Befehl ein: RADIUS-Attribut 26 (dezimal)	1A
Länge: Einschließlich Bytes für Typ und Länge	16
MSB der Vendor-ID ist immer 00	00
Sophos Vendor-ID	00 15 34
Vendor-Typ: EF-User-Group	14
Wertinformationen	
Vendor-Länge: Einschließlich Bytes für Typ und Länge	0E
Text: "WestCoastSales" (keine Anführungszeichen)	57 65 73 74 43 6F 61 73 74 53 61 6C 65 73

9.9 Konfigurieren mehrerer Compliance Anwendungsserver (optional)

Mehrere Compliance Anwendungsserver erhöhen die Skalierbarkeit von Sophos NAC Advanced. Sie müssen alle weiteren Compliance Anwendungsserver installieren und dem primären Compliance Anwendungsserver entsprechend konfigurieren. Führen Sie zur Verwendung einer Konfigurationsdatei auf mehreren Servern bei LDAP das Password Encryption-Tool auf allen Servern aus. Das Bindekennwort wird dadurch aktualisiert und verschlüsselt. Die Verschlüsselung des Bindekennworts ist serverabhängig.

Folgende Aufgaben müssen bei mehreren Compliance Anwendungsservern durchgeführt werden:

- Exportieren und Importieren des Serverschlüssels in weitere Compliance Anwendungsserver. Weitere Informationen finden Sie unter [Export und Import des Serverschlüssels zu weiteren Compliance Anwendungsservern](#) (Seite 52).
- Konfigurieren Sie DNS Round-Robin auf Microsoft Windows[®] Server 2003, wenn andere Load Balancing-Software oder Appliances nicht aktiv sind. Weitere Informationen finden Sie unter [Konfigurieren von DNS-Round-Robin auf Windows Server 2003 oder höher](#) (Seite 52).

9.9.1 Export und Import des Serverschlüssels zu weiteren Compliance Anwendungsservern

Bei mehreren Compliance Anwendungsserver muss das öffentliche/private Schlüsselpaar auf allen betroffenen Compliance Anwendungsserver synchron sein. Weitere Informationen finden Sie in der Compliance Manager zu Hilfe.

1. Melden Sie sich auf dem primären Compliance Anwendungsserver am Compliance Manager an.
2. Klicken Sie auf **Configure System > Server Key** .
3. Exportieren Sie das öffentliche/private Schlüsselpaar.
4. Melden Sie sich auf einem anderen Compliance Anwendungsserver am Compliance Manager an und klicken Sie auf **Configure System > Server Key** .
5. Importieren Sie das öffentliche/private Schlüsselpaar.
6. Wiederholen Sie die Schritte 4 und 5 für alle weiteren Compliance Anwendungsserver.

9.9.2 Konfigurieren von DNS-Round-Robin auf Windows Server 2003 oder höher

Die Konfiguration von DNS-Round-Robin auf Microsoft Windows Server 2003 oder höher ermöglicht die Überprüfung von Endpoints über mehrere Server. Die Verwaltung beschränkt sich dabei auf nur einen Satz Gruppen, Richtlinien und Anwendungen in Sophos NAC Advanced. DNS Round Robin ermöglicht DNS-Servern die Ressourcenverteilung über mehrere Server. Dies wird als Load Balancing (Lastverteilung) bezeichnet. Dieser Abschnitt zeigt ein einfaches Beispiel zur Konfiguration der Round-Robin-Funktion von Microsoft Windows Server Domain Name Service (DNS). Andere DNS-Server mit Round-Robin sollten auf ähnliche Weise funktionieren.

Hinweis: Diese Aufgabe ist nicht erforderlich, wenn andere Load Balancing-Software aktiv ist.

1. Klicken Sie im Startmenü des Windows-Servers, auf dem der Domain Name Service aktiv ist, auf **Verwaltung > DNS** .
Das Fenster „DNS-Verwaltung“ wird angezeigt.
2. Öffnen Sie die DNS-Struktur.
3. Rechtsklicken Sie auf den Servernamen und wählen Sie dann **Eigenschaften**.
4. Klicken Sie auf die Registerkarte **Erweitert**.
5. Wählen Sie das Kontrollkästchen **Round-Robin aktivieren**.
6. Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.
7. Öffnen Sie den Ordner **Forward-Lookupzonen**, rechtsklicken Sie auf die Domäne, in der die Compliance Anwendungsserver konfiguriert werden, und wählen Sie dann **Neuer Host (A)...**

8. Geben Sie den Hostnamen und die IP-Adresse des installierten und konfigurierten primären Compliance Anwendungsservers ein und klicken Sie dann auf **Host hinzufügen**.

Hinweis: Der eingegebene Hostname wird zum Hostteil der URL, die von den Agenten verwendet werden soll. Wenn Sie beispielsweise „sophosapp“ als neuen Host hinzufügen, lautet der vollständige Domänenname „sophosapp.endpointsoftware.info“.

9. Klicken Sie auf **OK**, um den hinzugefügten Hostnamen und die IP-Adresse zu bestätigen.
10. Wiederholen Sie Schritt 8 für jeden weiteren Compliance Anwendungsserver.

Hinweis: Damit DNS-Round-Robin einwandfrei funktioniert, muss der Hostname für alle Compliance Anwendungsserver identisch sein. Wenn z.B. der Hostname des primären „sophosapp“ lautet, muss der Hostname für alle anderen Compliance Anwendungsserver ebenfalls „sophosapp“ lauten.

11. Klicken Sie auf **Fertig**, um zum Fenster „DNS-Verwaltung“ zurückzukehren.

In diesem Beispiel wird auf die Anforderung des vollständigen Domänennamens „sophosapp.endpointsoftware.info“ eine der drei IP-Adressen des Compliance Anwendungsservers ausgegeben: 10.0.224.102, 10.0.224.103 oder 63.110.105.174. Ein Agent, der mit diesem Domänennamen konfiguriert wurde, kann mit allen Compliance Anwendungsservern kommunizieren.

10 Installation des Dissolvable Agent

Der Dissolvable Agent ist für Benutzer bestimmt, auf deren Endpoints kein Agent installiert wurde oder installiert werden konnte, wie z.B. Auftragnehmer oder Besucher. Nähere Informationen zum Dissolvable Agent-Branding entnehmen Sie bitte der *Sophos NAC Advanced Agent Konfigurationsanleitung*.

10.1 Systemvoraussetzungen für den Dissolvable Agent

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

10.2 Installation des Dissolvable Agent auf einem Webserver

Um den Dissolvable Agent verwenden zu können, muss die Serverkomponente des Dissolvable Agent zunächst auf einem Windows-basierten Webserver installiert werden, auf den Benutzer Zugriff haben. Der Dissolvable Agent kann auf dem gleichen Server installiert werden wie Sophos Compliance Anwendungsserver. Sobald er installiert ist, können Benutzer den Dissolvable Agent über einen Browser herunterladen.

1. Laden Sie den Sophos Compliance Dissolvable Agent von der Sophos Website herunter. Sie können auch die Sophos Installations-CD einlegen. Die CD sollte automatisch gestartet werden.
2. Doppelklicken Sie auf die Installationsdatei für Sophos Compliance Dissolvable Agent, um die Installation des Dissolvable Agent zu starten.
3. Klicken Sie auf **Weiter**.
4. Lesen Sie den Endbenutzer-Lizenzvertrag und wählen Sie die Schaltfläche **I Accept the terms of the License Agreement**. Klicken Sie dann auf **Next**.
5. Klicken Sie auf **Change**, um das entsprechende Installationsverzeichnis zu wählen, oder übernehmen Sie die Vorgabe: c:\inetpub\wwwroot. Klicken Sie auf **Weiter**.
6. Geben Sie die IP-Adresse des Sophos NAC-Compliance Anwendungsservers oder den DNS-Namen ein.

Hinweis: Wenn Sophos NAC Advanced auf mehreren Servern installiert wurde, ist die Serveradresse die IP-Adresse bzw. der DNS-Name des Compliance Anwendungsservers – nicht des Compliance Datenbanksservers. Bei mehreren Compliance Anwendungsservern geben Sie den Hostnamen ein, der für alle Compliance Anwendungsserver gilt. Wenn die Sophos NAC-Serveradresse nach der Installation des Dissolvable Agent geändert wird, muss die Serverkomponente des Dissolvable Agent nochmals auf dem Webserver installiert und dabei die neue Sophos Compliance Anwendungsserveradresse angegeben werden.

7. Deaktivieren Sie zum Testen von Sophos NAC Advanced das Kontrollkästchen **Secure Sophos Server (use HTTPS)**.

- Die Option **Always register agent with server** ist standardmäßig nicht aktiviert. Wenn Sie möchten, dass sich Benutzer am Dissolvable Agent anmelden, müssen Sie die Option auswählen. Klicken Sie auf **Next**.

Hinweis: Wenn Sie das Kontrollkästchen „Always register agent with server“ deaktivieren, müssen Sie die Registrierungseinstellungen für den Dissolvable Agent in Compliance Manager auf „On“ einstellen.

- Klicken Sie auf **Install**.
- Klicken Sie auf **Finish**, um die Installation abzuschließen.

Hinweis:

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

Wichtig: Der Dissolvable Agent kann keine Patch-Analyse durchführen, wenn der Benutzer nicht über volle Zugriffsrechte verfügt. Der Benutzer muss sich als Administrator anmelden. Wenn dies nicht möglich ist, empfiehlt sich die Einrichtung einer separaten Richtlinie für Benutzer des Dissolvable Agent. Diese Richtlinie sollte keine Patches, jedoch das „Windows Update Profile“ enthalten. Durch dieses Profil werden der Windows-Update-Dienst installiert und automatische Updates aktiviert.

11 Deinstallation des Dissolvable Agent auf einem Webserver

Mit folgenden Schritten deinstallieren Sie die Serverkomponente von Dissolvable Agent vom Webserver: Wenn Sie den Dissolvable Agent von Ihrem Webserver deinstallieren, können Benutzer den Dissolvable Agent nicht herunterladen.

1. Rufen Sie über das Startmenü **Systemsteuerung > Software** auf.
2. Wählen Sie **Sophos Compliance Dissolvable Agent** und klicken Sie auf **Entfernen**.
3. Klicken Sie auf **Ja**, um die Entfernung des Dissolvable Agents zu bestätigen.

12 Installation des Agenten

Wenn Sie den Abschnitt *Konfiguration* in diesem Dokument durchgearbeitet haben, können Sie Compliance Agenten auf Endpoints installieren.

12.1 Systemvoraussetzungen

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

12.2 Installation des Agenten

Bei der Installation des Agenten werden die Werte einer vorherigen Installation (falls vorhanden) übernommen. Um den Agenten installieren zu können, müssen Sie am Endpoint als Administrator angemeldet sein. Nach der Installation ist die Agentenschnittstelle jedoch in jedem Benutzermodus verwendbar, so auch im eingeschränkten Benutzermodus. Nach der Installation wird der Agent in der Microsoft Windows-Systemsteuerung unter „Software“, aber nicht im Microsoft Windows-Startmenü aufgelistet.

Konfigurationsoptionen

Der Agent kann über diverse Befehlszeilenooptionen konfiguriert werden.

- Um den Quarantine Agent im Modus **Use Computer Logon** auszuführen, geben Sie den Befehl "*<vollständiger Pfad zur Installationsdatei des Agenten>*"
`AGENT_SETTINGS="Register=<Registrierungsmodus>"` ein. Wenn kein Registrierungsmodus angegeben wurde, lautet der Standard "demand".

Hinweis: Die Registrierungsmodi des Agenten lauten "demand", "nopassword" und "usecomputerlogon". Weitere Informationen finden Sie in der *Sophos NAC Advanced Praxistipps*.

- Sie können IP-Adresse, DNS-Name und Modus (HTTP oder HTTPS) des Compliance Anwendungsservers, mit dem der Agent kommuniziert, über folgenden Befehl konfigurieren:
`msiexec /i "<vollständiger Pfad zur Installationsdatei des Agenten>" AGENT_SERVER=<IP-Adresse oder DNS-Name> AGENT_SERVERMODE=<http oder https>` Wenn kein Modus angegeben wurde, wird standardmäßig HTTPS verwendet.
- Sie können die DHCP-Benutzerklasse über folgenden Befehl konfigurieren:
`msiexec /i "<vollständiger Pfad zur Installationsdatei des Agenten>" AGENT_DHCPCLASS=<Benutzerklasse>`. Die DHCP-Benutzerklasse wird zum DHCP-Enforcement verwendet, wenn der NAC DHCP Enforcer nicht genutzt wird.

Mit `msiexec /i "c:\SophosComplianceAgent.msi" AGENT_INSTALLTYPE=quarantine AGENT_SETTINGS="Register=usecomputerlogon" AGENT_SERVER=appserver AGENT_SERVERMODE=https` wird beispielsweise der Quarantine Agent mit der Registrierungseinstellung **Use Computer Logon** von einer Agenten-Installationsdatei auf Laufwerk C installiert und der Agent kommuniziert über HTTPS mit dem Compliance Anwendungsserver mit dem DNS-Namen „appserver“.

So wird der Agent installiert:

1. Laden Sie Sophos Compliance Agent von der Sophos Website herunter.
Sie können auch die Sophos Installations-CD einlegen. Die CD sollte automatisch gestartet werden.
2. Doppelklicken Sie auf die Sophos Compliance Agent-Installationsdatei.
3. Klicken Sie auf **Next**, um den Assistenten zu starten.
4. Lesen Sie den Endbenutzer-Lizenzvertrag und wählen Sie die Schaltfläche **I Accept the terms of the License Agreement**. Klicken Sie dann auf **Next**.
5. Geben Sie die IP-Adresse oder den DNS-Namen des Compliance Anwendungsservers ein.
6. Deaktivieren Sie zum Testen von Sophos NAC Advanced das Kontrollkästchen **Secure Sophos Server (use HTTPS)**. Klicken Sie auf **Weiter**.

Hinweis: Wenn Sophos NAC Advanced auf mehr als einem Server installiert wurde, ist die Serveradresse die IP-Adresse bzw. der DNS-Name des Compliance Anwendungsservers – nicht des Compliance Datenbanksservers. Bei mehreren Compliance Anwendungsservern geben Sie den Hostnamen ein, der für alle Compliance Anwendungsserver gilt.

7. Klicken Sie auf **Change**, um das entsprechende Installationsverzeichnis zu wählen, oder übernehmen Sie das Standardverzeichnis und klicken Sie dann auf **Next**.
8. Klicken Sie auf **Install**. Klicken Sie auf **Cancel**, um die Installation abzubrechen.

Hinweis: Unter Windows 2000 wird das Dialogfeld „Driver Unsigned“ angezeigt, es sei denn, Service Pack 3 oder höher wurde installiert. Dieses Verhalten wird durch die Art der Signaturerstellung im Windows Hardware Quality Lab (WHQL) verursacht. Unter Windows XP kann das Dialogfenster „Driver Unsigned“ angezeigt werden, wenn Service Pack 1 installiert wurde. Mit Service Pack 1a, Service Pack 2 oder ohne installiertem Service Pack sollte das Fenster jedoch nicht angezeigt werden.

9. Klicken Sie auf **Finish**, um die Installation abzuschließen.

Nach der Installation des Agenten muss der Endpoint möglicherweise aus folgenden Gründen neu gestartet werden:

- Sie wurden bei der Installation aufgefordert, Anwendungen zu schließen, die freigegebene Ressourcen wie XMLDOM verwenden, und Sie haben diese Anwendungen nicht geschlossen.
- Sie führen für den Quarantine Agent ein Upgrade durch, das eine neue Version von Agent Quarantine Manager (Kerneltreiber) verwendet.

13 Deinstallation des Agenten

Wichtig: Bei der Deinstallation eines Agenten wird von Windows Explorer ein Dialogfeld angezeigt, das vor der Deinstallation des Agenten zum Schließen bestimmter Anwendungen auffordert, z.B. zum Schließen eines E-Mail-Clients. Es empfiehlt sich, diese Anwendungen zu schließen, damit die Deinstallation fehlerfrei abläuft. Außerdem muss der Endpoint nach der Deinstallation des Agenten neu gestartet werden.

1. Rufen Sie über das Startmenü **Systemsteuerung > Software** auf.
2. Wählen Sie **Sophos Compliance Agent** und klicken Sie auf **Entfernen**.
3. Klicken Sie auf **Ja**, um die Entfernung des Agenten zu bestätigen.

14 Optionale Einstellungen

In diesem Abschnitt werden optionale Einstellungen für Sophos NAC Advanced aufgeführt. Bei der Implementierung von Sophos NAC Advanced können einige oder alle der folgenden Aufgaben erforderlich sein.

14.1 Prüfen/Ändern des CurrentDefsLoader-Tasks

Der Patch Loader-Prozess wird täglich zu beliebigen Zeiten ausgeführt. Dieser Task ruft die neuesten Patch-Definitionen von Sophos ab und erfordert Zugriff auf das Internet.

1. Klicken Sie auf dem Compliance Anwendungsserver im Startmenü auf **Systemsteuerung** > **Geplante Tasks** .

Das Fenster „Geplante Tasks“ wird angezeigt.

2. Doppelklicken Sie auf **Sophos NAC PatchLoader**. Das Eigenschaften-Fenster wird angezeigt.
3. Klicken Sie auf die Registerkarte **Zeitplan**.
4. Ändern Sie je nach Bedarf den Zeitpunkt des geplanten Tasks und klicken Sie auf **OK**.
5. Klicken Sie auf **OK**, um die Änderungen zu übernehmen.
6. Schließen Sie „Geplante Tasks“.

14.2 Manuelles Ausführen des Patch Loader-Tasks

Der Patch Loader-Task wird standardmäßig täglich zu beliebigen Zeiten ausgeführt. Der Patch Loader-Task kann jedoch auch manuell ausgeführt werden. Dieser Task ruft die neuesten Patch-Definitionen von Sophos ab und erfordert Zugriff auf das Internet.

1. Klicken Sie auf dem Compliance Anwendungsserver im Startmenü auf **Systemsteuerung** > **Geplante Tasks** .

Das Fenster „Geplante Tasks“ wird angezeigt.

2. Rechtsklicken Sie auf **Sophos NAC PatchLoader** und wählen Sie **Ausführen**.
3. Schließen Sie „Geplante Tasks“.

14.3 Prüfen/Ändern des Current Definition Loader-Tasks

Der Current Definition Loader-Task soll stündlich ausgeführt werden. Bei der Installation von Sophos NAC Advanced wurde der Task so eingerichtet, dass er an beliebigen Zeitpunkten ausgeführt werden kann. Er nimmt nur wenige Minuten in Anspruch und erfordert eine Internetverbindung. Dieser Task ruft die neuesten Datumsangaben der aktuellen Kennung für jede Viren- und Spywareschutzanwendung von Sophos ab.

1. Klicken Sie auf dem Compliance Anwendungsserver im Startmenü auf **Systemsteuerung** > **Geplante Tasks** .

Das Fenster „Geplante Tasks“ wird angezeigt.

2. Doppelklicken Sie auf **Sophos NAC CurrentDefsLoader**. Das Eigenschaften-Fenster wird angezeigt.

3. Klicken Sie auf die Registerkarte **Zeitplan**.
4. Klicken Sie auf **Erweitert**.
5. Ändern Sie die Zeit des geplanten Tasks und klicken Sie auf **OK**.
6. Klicken Sie auf **OK**, um die Änderungen zu übernehmen.
7. Schließen Sie „Geplante Tasks“.

14.4 Manuelles Ausführen des Current Definition Loader-Tasks

Der Current Definition Loader-Task wird stündlich ausgeführt. Er kann aber auch manuell gestartet werden. Bei der Installation von Sophos NAC Advanced wurde der Task so eingerichtet, dass er an beliebigen Zeitpunkten ausgeführt werden kann. Er nimmt nur wenige Minuten in Anspruch und erfordert eine Internetverbindung. Dieser Task ruft die neuesten Datumsangaben der aktuellen Kennung für jede Viren- und Spywareschutzanwendung von Sophos ab.

1. Klicken Sie auf dem Compliance Anwendungsserver im Startmenü auf **Systemsteuerung > Geplante Tasks**.

Das Fenster „Geplante Tasks“ wird angezeigt.

2. Rechtsklicken Sie auf **Sophos NAC CurrentDefsLoader** und wählen Sie **Ausführen**.
3. Schließen Sie „Geplante Tasks“.

14.5 Prüfen/Ändern des Report Warehouse Loader-Tasks

Der Report Warehouse Loader-Task wird standardmäßig täglich um 2.30 Uhr ausgeführt. Der Task kann jedoch auch manuell ausgeführt werden. Dieser Task sorgt dafür, dass Berichtsdaten an einem bestimmten Zeitpunkt archiviert und gelöscht werden.

1. Rufen Sie das Start-Menü von SQL Server auf.
 - Klicken Sie in SQL Server 2000 auf **Microsoft SQL Server > Enterprise Manager**. SQL Enterprise Manager wird geöffnet.
 - In SQL Server 2005 oder höher klicken Sie auf **Microsoft SQL Server 2005 (Version) > SQL Server Management Studio**. SQL Server Management Studio wird geöffnet.
2. Suchen Sie **SQL Server-Agent**.

Hinweis: In SQL Server 2000 befindet sich der SQL Server-Agent im Management-Ordner.
3. Wählen Sie unter SQL Server Agent die Option **Aufträge**.
4. Doppelklicken Sie auf den Task **Sophos NAC – LoadWH**. Das Eigenschaften-Fenster wird angezeigt.
5. Führen Sie einen der folgenden Schritte aus:
 - Klicken Sie in SQL Server 2000 auf die Registerkarte **Zeitpläne**.
 - Klicken Sie in SQL Server 2005 oder höher auf die Registerkarte **Zeitpläne**.

6. Führen Sie einen der folgenden Schritte aus:
 - Klicken Sie zum Hinzufügen eines Zeitplans auf **Neuer Zeitplan** (SQL Server 2000) bzw. **Neu** (SQL Server 2005 oder höher). Fügen Sie den Zeitplan hinzu und klicken Sie anschließend auf **OK**.
 - Klicken Sie zum Bearbeiten des vorhandenen Zeitplans auf **Bearbeiten** und klicken Sie anschließend auf **OK**.

Hinweis: Sie können den Zeitpunkt für das Verschieben archivierter Berichte ändern und/oder Sie können weitere Tasks angeben, damit Berichtsdaten mehrmals am Tag in Archivberichte verschoben werden.
7. Klicken Sie auf **OK**, um die Änderungen zu übernehmen.
8. Schließen Sie SQL Enterprise Manager bzw. SQL Server Management Studio.

14.6 Manuelles Ausführen des Report Warehouse Loader-Tasks

Der Report Warehouse Loader-Task regelt die Archivierung und Löschung von Reportdaten. Standardmäßig wird der Task täglich um 2.30 Uhr ausgeführt. Sie können den Report Warehouse Loader-Task jedoch auch manuell ausführen.

1. Rufen Sie das Start-Menü von SQL Server auf.
 - Klicken Sie in SQL Server 2000 auf **Microsoft SQL Server > Enterprise Manager** . SQL Enterprise Manager wird geöffnet.
 - In SQL Server 2005 oder höher klicken Sie auf **Microsoft SQL Server 2005 (Version) > SQL Server Management Studio** . SQL Server Management Studio wird geöffnet.
2. Suchen Sie **SQL Server-Agent**.

Hinweis: In SQL Server 2000 befindet sich der SQL Server-Agent im Management-Ordner.
3. Wählen Sie unter SQL Server Agent die Option **Aufträge**.
4. Rechtsklicken Sie auf **Sophos NAC – LoadWH** und wählen Sie **Auftrag starten**.

Hinweis: Die manuelle Ausführung des Sophos NAC-LoadWH-Tasks nimmt nicht mehr Zeit in Anspruch als die automatische Ausführung.
5. Schließen Sie SQL Enterprise Manager bzw. SQL Server Management Studio.

14.7 Deaktivieren von HTTPS zum Test außerhalb einer Arbeitsumgebung

Benutzernamen, Kennwörter und andere vertrauliche Daten werden von Sophos NAC Advanced in einer Arbeitsumgebung über HTTPS geschützt. In manchen Fällen, insbesondere zu Testzwecken, muss HTTPS unter Umständen deaktiviert werden.

1. Klicken Sie im Startmenü des Compliance Anwendungsservers auf **Verwaltung > Internetinformationsdienste (IIS)** .

IIS wird aufgerufen.
2. Öffnen Sie den Ordner **Websites** und dann den Ordner **Standardwebsite**.

3. Rechtsklicken Sie auf **RegistrationInterface** und wählen Sie **Eigenschaften**.
Das Fenster „Eigenschaften von RegistrationInterface“ wird angezeigt.
4. Klicken Sie auf die Registerkarte **Verzeichnissicherheit**.
5. Klicken Sie im Bereich **Sichere Kommunikation** auf **Bearbeiten**.
Das Fenster „Sichere Kommunikation“ wird angezeigt.
6. Deaktivieren Sie das Kontrollkästchen **Sicheren Kanal voraussetzen (SSL)**.
7. Klicken Sie auf **OK**, um zum Fenster „Eigenschaften von RegistrationInterface“ zurückzukehren, und klicken Sie dann auf **OK**, um zu IIS zurückzukehren.
8. Wiederholen Sie die Schritte 2 bis 6 für „PolicyInterface“, „ReportInterface“ und „ServerStatusInterface“.
9. Schließen Sie „IIS“.

15 Technischer Support

Technischen Support zu Sophos Produkten können Sie wie folgt abrufen:

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

16 Rechtlicher Hinweis

Copyright © 2011 Sophos Limited. Alle Rechte vorbehalten. Diese Publikation darf weder elektronisch oder mechanisch reproduziert, elektronisch gespeichert oder übertragen, noch fotokopiert oder aufgenommen werden, es sei denn, Sie verfügen entweder über eine gültige Lizenz, gemäß der die Dokumentation in Übereinstimmung mit dem Lizenzvertrag reproduziert werden darf, oder Sie verfügen über eine schriftliche Genehmigung des Urheberrechtsinhabers.

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

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 license

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

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

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

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

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

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

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

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

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

Original SSLeay license

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

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

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

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

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

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

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

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

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

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

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

OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

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