

Sophos NAC DHCP Konfigurationsanleitung

Produktversion: 3.9
Stand: Dezember 2011



Inhalt

1	Einleitung.....	3
2	DHCP Enforcement im Überblick.....	4
3	Installation von DHCP Enforcement.....	5
4	DHCP Enforcement-Upgrade.....	18
5	Anhang: DHCP Enforcer Configuration Utility.....	24
6	Technischer Support.....	27
7	Rechtlicher Hinweis.....	28

1 Einleitung

Diese Anleitung beschreibt die Konfiguration von DHCP Enforcement. Anhand von DHCP Enforcement lassen sich unbekannte Endpoints identifizieren, die auf Ihr Netzwerk zugreifen. Sie können deren Sicherheitsstufe ermitteln und den Netzwerkzugriff dieser Endpoints regeln. Ferner wird die Konfiguration des NAC DHCP Enforcers und NAC-Servers erläutert. Die Anleitung bietet zudem Informationen zum Upgrade der DHCP-Enforcement-Software.

Im Einzelnen:

- Erste Installation und Konfiguration der DHCP Enforcer-Software.
- Konfiguration von DHCP mit NAC Manager.
- DHCP Enforcement-Upgrade.

Der Leitfaden richtet sich an:

- Benutzer von Sophos Enterprise Console.
- Benutzer der in Enterprise Console integrierten Version von Sophos NAC.
- Kunden, die DHCP Enforcement installieren, konfigurieren oder upgraden.

Es empfiehlt sich, zunächst die Schnellstartanleitung zu *Sophos Enterprise Console* zu Rate zu ziehen.

Begleitmaterial zu Sophos Software finden Sie hier: <http://www.sophos.de/support/docs/>.

1.1 DHCP Enforcer-Softwarevoraussetzungen

Installieren Sie die Sophos DHCP Enforcer-Software auf allen DHCP-Servern, um DHCP Enforcement in Sophos NAC zu integrieren.

Anforderungen der DHCP Enforcer Software	
Betriebssystem	<p>Folgende Windows Server-Versionen werden unterstützt:</p> <ul style="list-style-type: none"> ■ Windows Server 2003 und höher (32-Bit) ■ Windows Server 2003 SP2 und höher (64-Bit) ■ Windows Server 2003 R2 und höher (32-Bit und 64-Bit) ■ Windows Server 2008 Base und höher (32-Bit und 64-Bit) ■ Windows Server 2008 R2 Base und höher (32-Bit und 64-Bit) <p>Hinweis: Windows Server 2008 Web und Core werden nicht unterstützt.</p>
DHCP-Software	Microsoft [®] Dynamic Host Configuration Protocol (DHCP) Software

2 DHCP Enforcement im Überblick

Sophos NAC umfasst Voreinstellungen für DHCP Enforcement. Diese Voreinstellungen decken die meisten DHCP-Implementierungen ab, so dass der Konfigurationsaufwand nach der Installation von Sophos NAC minimal ist. Da jedoch keine DHCP-Implementierung der anderen gleicht, ist eine zusätzliche Konfiguration notwendig.

Hinweis: Die DHCP Enforcement-Checkliste enthält alle für die Implementierung von DHCP Enforcement erforderlichen Punkte. Stellen Sie fest, welche Anweisungen für Sie gelten:

- Wenn Sie noch nicht mit DHCP Enforcement gearbeitet haben, bietet der Abschnitt [DHCP Enforcement-Installations-Checkliste](#) (Seite 5) eine Einführung.
- Wenn Sie DHCP Enforcement zum ersten Mal in Sophos NAC 3.3, 3.5 oder 3.7 installiert haben und auf Version 3.9 upgraden, finden Sie hier [DHCP Enforcement-Upgrade-Checkliste](#) (Seite 18) entsprechende Anweisungen.

Voreinstellungen für DHCP Enforcement

Sie können die Voreinstellungen bei Bedarf in NAC Manager ändern.

- Unbekannte Endpoints können auf das Netzwerk zugreifen. Unbekannte Endpoints (Unknown Endpoints) werden nicht von Sophos Enterprise Console verwaltet. Der Compliance Agent ist nicht installiert, Exemptions gelten nicht und der Dissolvable Agent muss nicht ausgeführt werden. Die Standardeinstellung der DHCP-Server lautet „Report Only“. Ändern Sie den Modus unbekannter Endpoints in „Enforce“, um DHCP Enforcement und Quarantäne unbekannter Endpoints zu aktivieren.

Hinweis: Wenn DHCP Enforcement aktiviert ist, können unbekannte Endpoints nicht auf private IP-Adressen und das lokale Netzwerk (LAN) zugreifen.

- Bekannte Endpoints können auf das Netzwerk zugreifen. Bekannte Endpoints (Known Endpoints) werden von Sophos Enterprise Console verwaltet. Der Compliance Agent ist installiert und wird ausgeführt. Die Voreinstellung für NAC-Richtlinien lautet „Report Only“. Zum Ändern der DHCP Enforcement-Einstellungen für bekannte Endpoints müssen Sie für alle Richtlinien den Richtlinienmodus „Enforce“ wählen.

Hinweis: Bei aktiviertem DHCP Enforcement können konforme und teilkonforme Endpoints, auf denen der Agent ausgeführt wird, auf das Netzwerk zugreifen. Nicht-konformen Endpoints, auf denen der Agent ausgeführt wird, wird der Netzwerkzugriff verweigert.

Es empfiehlt sich, auf unbekanntem Endpoints DHCP Enforcement und auf bekannten Endpoints Agent Enforcement einzusetzen. DHCP Enforcement ist in Sophos NAC jedoch auch auf bekannten Endpoints möglich. Weitere Informationen zu Agent-Enforcement finden Sie in der Sophos Compliance Agent Konfigurationsanleitung.

3 Installation von DHCP Enforcement

Befolgen Sie zur Ersteinstallation von Sophos NACDHCP Enforcement die Anweisungen in diesem Abschnitt.

3.1 DHCP Enforcement-Installations-Checkliste

Die DHCP Enforcement-Installations-Checkliste enthält alle für die Implementierung von DHCP Enforcement erforderlichen Punkte. Falls nichts anderes angegeben ist, werden die Punkte der Checkliste gemäß den Anweisungen in diesem Dokument ausgeführt.

Schritt	Beschreibung	Erledigt
Installation von Sophos NAC und Compliance Agent		
1.	Installation und Konfiguration von Sophos NAC. Weitere Informationen finden Sie in der Sophos Endpoint Security and Control – Schnellstartanleitung.	
2.	Installation von Compliance Agent über Sophos Enterprise Console auf Endpoints. Weitere Informationen finden Sie in der Sophos Endpoint Security and Control – Schnellstartanleitung.	
DHCP-Server		
3.	Installation der DHCP Enforcer-Software auf allen DHCP-Servern.	
Sophos NAC Manager-Tasks		
4.	Ausführen des DHCP Configuration Wizard zur Konfiguration von Proxyserver, Korrekturserver, Dissolvable Agent- und DHCP-Enforcer-Server für Sophos NAC DHCP Enforcement.	
5.	Erstellen des DHCP Enforcer Reports, um <ul style="list-style-type: none"> ■ festzustellen, ob bekannte Endpoints bei aktiviertem DHCP Enforcement über adäquaten Netzwerkzugriff verfügen. ■ Endpoints aufzufinden, für die Ausnahmen erstellt werden müssen. 	
6.	Erstellen von Ausnahmen für Endpoints, die den Compliance Agent nicht ausführen können (z.B. Computer, die nicht unter Windows laufen). Exemptions erfassen auch Endpoints, für die keine Konformitätsprüfung erforderlich ist – z.B. Server, Router und Drucker.	
7.	Aktivieren von DHCP Enforcement.	

3.2 Installation der DHCP Enforcer-Software

Installieren Sie die DHCP Enforcer-Software auf allen Microsoft DHCP-Servern. Die DHCP Enforcer-Software enthält den DHCP Enforcer und das DHCP Enforcer Configuration Utility. Der DHCP-Server wird im Verlauf der Installation konfiguriert. Mit dem DHCP Enforcer Configuration Utility können Sie bei der Installation festgelegte DHCP Server-Einstellungen ändern. Nähere Informationen finden Sie unter *Anhang: DHCP Enforcer Configuration Utility* (Seite 24).

1. Rufen Sie <http://www.sophos.de/support/updates/> auf.
2. Geben Sie Ihre MySophos-Zugangsdaten ein.
3. Laden Sie von der Website für **Enterprise** -Downloads den NAC DHCP Enforcer-Installer herunter.
4. Führen Sie den Installer aus.

Ein Installationsassistent leitet Sie durch die Installation. Übernehmen Sie die Voreinstellungen.

Es empfiehlt sich, sich den gemeinsamen Schlüssel, den Sie auf der Seite **Sophos DHCP Enforcer** eingegeben haben, zu notieren. Der gemeinsame Schlüssel sichert den Datenfluss zwischen dem NAC-Server und dem DHCP-Server ab. Sie müssen den gemeinsamen Schlüssel eingeben, wenn Sie den DHCP Configuration Wizard mit NAC Manager ausführen.

Hinweis: Stellen Sie nach der Installation der DHCP Enforcer-Software sicher, dass der DHCP-Dienst auf allen DHCP-Servern läuft.

3.3 Tasks in NAC Manager

Wenn der DHCP Enforcer auf allen DHCP-Servern installiert wurde, konfigurieren Sie die DHCP-Server mit NAC Manager, um mit Sophos NAC arbeiten zu können. Der Konfigurationsaufwand für DHCP Enforcement in NAC Manager ist minimal. Die Voreinstellung für DHCP Enforcement lautet „Report only“. Enforcement muss aktiviert werden.

- **Unbekannte Endpoints** (Unknown Endpoints) werden nicht von Sophos Enterprise Console verwaltet. Der Compliance Agent ist nicht installiert, Exemptions gelten nicht und der Dissolvable Agent muss nicht ausgeführt werden.
- **Bekannte Endpoints** (Known Endpoints) werden von Sophos Enterprise Console verwaltet. Der Compliance Agent ist installiert und wird ausgeführt.

Hinweis: Sie müssen Exemptions für Endpoints erstellen, die den Compliance Agent nicht ausführen können (z.B. Computer, die nicht unter Windows laufen). Exemptions erfassen auch Endpoints, für die keine Konformitätsprüfung erforderlich ist – z.B. Server, Router und Drucker. Exemptions sind nur für Endpoints erforderlich, die eine dynamisch zugewiesene IP-Adresse über DHCP erhalten.

Zu den NAC Manager-Tasks gehören:

1. Ausführen des DHCP Configuration Wizard zur Konfiguration von Proxyserver, Korrekturserver, Dissolvable Agent- und DHCP-Enforcer-Server für Sophos NAC DHCP Enforcement.
2. Feststellen anhand des DHCP Enforcer-Reports in NAC Manager, ob bekannte Endpoints den erforderlichen Netzwerkzugriff erhalten, wenn DHCP Enforcement aktiviert ist. Ermitteln der Endpoints, für die Ausnahmen erstellt werden müssen.
3. Erstellen von Ausnahmen für Endpoints, die den Compliance Agent nicht ausführen können bzw. deren Konformität nicht überprüft werden muss.
4. Aktivieren von DHCP Enforcement.

3.3.1 Konfiguration mit dem DHCP Configuration Wizard

Mit dem DHCP Configuration Wizard erkennen Sie Proxyserver, Korrekturserver, Dissolvable-Agent-Server und DHCP-Server für Sophos NAC DHCP-Implementierungen. Der Assistent konfiguriert die DHCP Enforcer Access Templates automatisch mit Ihren Server-Definitionen.

Vorgehensweise

1. Melden Sie sich an NAC Manager an.
2. Klicken Sie auf **Enforce > DHCP Configuration Wizard** . Klicken Sie auf **Next**.
3. Führen Sie einen der folgenden Schritte aus:
 - Wenn Sie Proxyserver verwenden, klicken Sie auf **Yes** und dann auf **Next**. Fahren Sie mit dem nächsten Schritt fort.
 - Wenn Sie **keine** Proxyserver verwenden, klicken Sie auf **No** und dann auf **Next**. Fahren Sie mit Schritt 5 fort.

Wichtig: Wenn Sie keinen Proxyserver für den Internetzugang festlegen, können Benutzer nicht auf das Internet zugreifen und die Standard-DHCP (Internet Access DHCP Enforcer Access Template) bietet nur Korrekturzugang.
4. Geben Sie alle für den Internetzugang erforderlichen Proxyserver an und klicken Sie auf **Next**.
Führen Sie einen der folgenden Schritte aus:
 - Heben Sie die Markierung neben den Servern auf, die **nicht** als Proxyserver zum Einsatz kommen sollen.
 - Zur Auswahl weiterer Server klicken Sie auf **Add**, geben die entsprechenden Anmeldedaten ein und klicken auf **OK**. Wiederholen Sie diesen Schritt für weitere Bereiche. Nach der Einrichtung können diese Server im Bereich **Enforce > Network Resources** verwaltet werden.

Hinweis: Die ausgewählten Proxyserver ersetzen die in der Access Template „DHCP – Internet Access DHCP Enforcer“ aufgeführten Server.
5. Geben Sie alle zur Korrektur erforderlichen Korrekturserver an (z.B. Domain Controller) und klicken Sie auf **Next**.

Führen Sie einen der folgenden Schritte aus:

- Heben Sie die Markierung neben den Servern auf, die **nicht** als Korrekturserver zum Einsatz kommen sollen.
- Zur Auswahl weiterer Server klicken Sie auf **Add**, geben die entsprechenden Anmeldedaten ein und klicken auf **OK**. Wiederholen Sie diesen Schritt für weitere Bereiche. Nach der Einrichtung können diese Server im Bereich **Enforce > Network Resources** verwaltet werden.

Hinweis: Die ausgewählten Korrekturserver ersetzen die in der DHCP – Remediation Access DHCP Enforcer Access Template aufgeführten Server.

6. Führen Sie einen der folgenden Schritte aus:

- Wenn der Dissolvable Agent bereits installiert wurde, klicken Sie auf **Yes** und dann auf **Next**. Fahren Sie mit dem nächsten Schritt fort.
- Wenn der Dissolvable Agent noch **nicht** installiert wurde, klicken Sie auf **Yes** und dann auf **Next**. Fahren Sie mit Schritt 8 fort.

Hinweis: Wenn sich der Dissolvable Agent und Sophos NAC auf demselben Server befinden, ist kein weiterer Dissolvable Agent-Server erforderlich.

7. Geben Sie die Server an, auf denen der Dissolvable Agent installiert ist, damit der DHCP Enforcer den Zugriff auf sie freigeben kann. Dieser Zugriff ist zur Bekanntmachung unbekannter Endpoints im Netzwerk erforderlich. Zur Auswahl weiterer Server klicken Sie auf **Add**, geben die Serverdaten zum Dissolvable Agent ein und klicken auf **OK**. Klicken Sie auf **Next**. Nach der Einrichtung können diese Server im Bereich **Configure System > Server Settings** verwaltet werden.

8. Legen Sie die DHCP-Server fest, auf denen die DHCP Enforcer-Software installiert wird. Zur Auswahl weiterer Server klicken Sie auf **Add**, geben die entsprechenden Anmeldedaten ein und klicken auf **OK**. Wiederholen Sie diesen Schritt für weitere Bereiche. Klicken Sie auf **Next**. Nach der Einrichtung können diese Server im Bereich **Configure System > Server Settings** verwaltet werden.

Hinweis: Der Schlüssel muss mit Ihrer Eingabe bei der Installation des DHCP Enforcers auf dem Server übereinstimmen. Der gemeinsame Schlüssel sichert den Datenfluss zwischen dem NAC-Server und dem DHCP-Server ab.

9. Klicken Sie auf **Fertigstellen**.

3.3.2 Ausführen des DHCP Enforcer-Reports

Erstellen Sie den Sophos NAC DHCP Enforcer Report, um den Konformitätszustand von Endpoints vor der Aktivierung von DHCP Enforcement festzustellen. Die vorhandenen NAC-Richtlinien sind auf „Report Only“ eingestellt. Im DHCP Enforcer Report kann festgestellt werden, ob die richtige Access Template angewandt wird, wenn Enforcement aktiviert wird. Über den DHCP Enforcer Report lassen sich Geräte ausschließen und Prüfungsdetails abrufen.

Vorgehensweise

1. Melden Sie sich an NAC Manager an.
2. Klicken Sie auf **Report > Troubleshooting**.
3. Klicken Sie auf das Listenfeld **Report Type** und wählen Sie **DHCP Enforcer**.

4. Klicken Sie gegebenenfalls auf das **Pluszeichen** neben **Report Criteria** und geben Sie die entsprechende Suchoption ein oder wählen Sie sie aus. Sie können auch auf den Link **Custom Sort** klicken, um die Sortieroptionen zu erweitern. Während der Reporterstellung werden die benutzerdefinierten Sortieroptionen vorübergehend geändert.

Hinweis: Mithilfe der Symbole „*“ und „%“ ist in den meisten Feldern eine Platzhaltersuche möglich. Wenn Sie beispielsweise in das Feld **Returned User Class M%** eingeben, werden alle mit „M“ beginnenden Benutzerklassen angezeigt. Wenn Sie dagegen in das Feld nur **M** ohne % eingeben, werden nur Benutzerklassen namens „M“ angezeigt.

5. Klicken Sie auf **Run**.

Beschreibung der Felder

Feld	Beschreibung
Summary Report	
Date/Time	Datum und Uhrzeit des versuchten Netzwerkzugriffs. Hinweis: Datum und Uhrzeit werden von der Zeitzone des Webbrowsers abgeleitet, der auf NAC Manager zugreift.
MAC Address	MAC-Adresse des Geräts, durch das der Netzwerkzugriff versucht wurde. Die angezeigte MAC-Adresse ist der Netzwerkkarte zugewiesen, die mit der Anfrage des DHCP-Clients in Zusammenhang steht.
Computer Name	Name des Geräts, durch das der Netzwerkzugriff versucht wurde. Der Computername wird automatisch über den Client Request ermittelt.
Compliance State	Der dem Endpoint bei der Konformitätsprüfung zugewiesene Konformitätszustand. Es gibt drei Zustände: „Compliant“ (konform), „Partially Compliant“ (teilkonform) und „Non-Compliant“ (nicht-konform). Drei Striche (---) deuten darauf hin, dass der Agent einen Compliance State nicht gemeldet hat. Die DHCP Enforcer Access Template, die der Richtlinie zugeordnet ist, bestimmt den Netzwerkzugriff.
Template Name (Version)	Name und Version der Access Template, in der die vom DHCP Enforcer durchgeführte Maßnahme festgelegt ist. Welche Access Template verwendet wird, richtet sich nach dem Grund (Reason). Neben Ihren individuell erstellten Access Templates sind die folgenden Access Templates standardmäßig verfügbar: <ul style="list-style-type: none"> ■ DHCP - Full Access: Gestattet Vollzugriff auf das Netzwerk. ■ DHCP - Internet Access: Zugang zum Internet, jedoch kein Zugriff auf private IP-Adressen und das lokale Netzwerk (LAN). <p>Wichtig: Wenn Sie keinen Proxyserver für den Internetzugang als Netzwerkressource festgelegt haben, können die Benutzer nicht auf das Internet zugreifen und die Vorlage bietet nur Korrekturzugriff.</p>

Feld	Beschreibung
	<ul style="list-style-type: none"> ■ DHCP - Remediation Access: Sperrt den Zugriff auf das Netzwerk mit Ausnahme der Korrekturserver, jedoch nicht für Sophos NAC-Server und den Dissolvable Agent-Server.
Grund	<p>Hier wird der Grund für die Zuweisung einer bestimmten Access Template durch DHCP Enforcer angegeben. Es gibt folgende Gründe:</p> <ul style="list-style-type: none"> ■ Assessment: Der Konformitätszustand ist das Resultat einer vom Agenten durchgeführten Analyse. Die DHCP Enforcer Access Template, die der Richtlinie zugeordnet ist, bestimmt den Netzwerkzugriff. Ein Link, über den sich Details zur Konformitätsprüfung in Bezug auf diesen Eintrag abrufen lassen, wird angezeigt. ■ Default Template: Dem Endpoint kann eine Richtlinie zugewiesen sein oder er kann eine bestimmte Ausnahme sein, aber es wurde keine zugehörige Access Template gefunden. Die im Bereich Configure System > Enforcer Settings aufgeführten Default Access Templates bestimmen den Netzwerkzugriff. ■ Enforcer Override: Die Durchsetzung wurde nicht überprüft. Wenn das Kontrollkästchen Override DHCP Enforcer im Bereich Configure System > Enforcer Settings aktiviert ist, bestimmen die in diesem Bereich unter Maintenance Mode/Enforcer Override festgelegten Access Templates den Netzwerkzugriff. ■ Exempted: Der Endpoint wird basierend auf den im Bereich Enforce > Exemptions festgelegten Ausschlusskriterien von der Durchsetzung ausgenommen. Die zu den Ausnahmekriterien gehörigen Access Templates bestimmen den Netzwerkzugriff. Im Bereich Exemptions werden weitere Gründe in Klammern aufgeführt: <ul style="list-style-type: none"> ■ User Class: Die Benutzerklasse wurde als Ausnahme angegeben. ■ Vendor Class: Die Herstellerklasse wurde als Ausnahme angegeben. ■ MAC: Die MAC-Adresse wurde als Ausnahme angegeben. ■ IP Scope: Der IP-Bereich wurde als Ausnahme angegeben. ■ Maintenance Mode: Die Software befindet sich im Modus „Maintenance“ (Wartung). Die unter Maintenance Mode/Enforcer Override im Bereich Configure System > Enforcer Settings festgelegten Access Templates bestimmen den Netzwerkzugriff. ■ Policy Retrieval Error: Gemäß dem Feld Update Threshold der DHCP Richtlinie (siehe Configure System > Enforcer Settings) ist der Konformitätszustand nicht mehr aktuell. Die zu diesem Zustand gehörige DHCP Enforcer Access Template der Richtlinie bestimmt den Netzwerkzugriff. ■ Remediate: Die Richtlinie befindet sich im Modus „Remediate“ (Korrektur). Die zu diesem Richtlinienmodus gehörigen DHCP Enforcer Access Templates bestimmen den Netzwerkzugriff.

Feld	Beschreibung
	<ul style="list-style-type: none"> ■ Report Only: Die Richtlinie befindet sich im Modus „Report Only“. Die zu diesem Richtlinienmodus gehörige DHCP Enforcer Access Template bestimmt den Netzwerkzugriff. ■ Reserved: Die MAC-Adresse des Geräts, das den Netzwerkzugriff angefordert hat, ist auf dem DHCP-Server als Spezialgerät reserviert. ■ System Error: Der Enforcer ist auf einen Fehler gestoßen, der den Abschluss dieses Vorgangs verhindert hat. Die Registrierungseinstellung „SystemErrors“ auf dem NAC-Server verweigert standardmäßig den Netzwerkzugriff. ■ Template Error: Eine zugehörige Access Template wurde nicht gefunden. Die im Bereich Configure System > Enforcer Settings festgelegten Access Templates konnten nicht verwendet werden. Bei diesem Fehler wird der Netzwerkzugriff vom DHCP-Server bestimmt, der keine Benutzerklasse zurückgibt und dem Benutzer den Zugriff verweigert. ■ Unknown Endpoint: Es ist kein Eintrag zur Konformität vorhanden. Die im Bereich Configure System > Enforcer Settings unter Unknown Endpoint aufgeführten Access Templates bestimmen den Netzwerkzugriff.
Returned User Class	Hierbei handelt es sich um die DHCP-Benutzerklasse, die vom DHCP Enforcer zur Durchsetzung an den DHCP-Server übermittelt wird.
DHCP-Server	IP-Adresse des DHCP-Servers, der Netzwerkzugriff vom DHCP Enforcer anfordert. Dabei handelt es sich um den DHCP-Server, auf dem der DHCP Enforcer installiert ist.
Detailed Report	
Agent Enforcement Action	<p>Vom Endpoint ergriffene Maßnahme bezüglich IP-Adressenzuordnung. Der Endpoint veranlasst die Freigabe und die Verlängerung der Gültigkeit von IP-Adressen basierend auf der in der Richtlinie festgelegten Agent Enforcement Action. Sobald der Agent gestartet wird, erstellt er neue IP-Adressen. Wenn sich der Konformitätszustand des Endpoints sowie der Richtlinienmodus ändert und sich die in der Richtlinie des Endpoints festgelegten DHCP Enforcer Access Templates ändern, leitet der Agent eine Konformitätsprüfung ein. Es sind folgende Werte möglich:</p> <ul style="list-style-type: none"> ■ None: IP-Adressen für den Endpoint werden weder freigegeben noch verlängert. ■ Release Renew: IP-Adressen für den Endpoint werden über den DHCP-Server freigegeben und verlängert. Vor Abruf und Zuteilung der neuen IP-Adressen werden die derzeit verwendeten IP-Adressen gestrichen. ■ Drei Striche (---): Der Agent hat keine Maßnahme angegeben.
Vendor Class	Herstellerklasse des DHCP-Clients.

Feld	Beschreibung
DHCP Relay	IP-Adresse des DHCP-Relays (falls in der ursprünglichen DHCP-Anfrage vorhanden), die vom DHCP Enforcer zur Auswahl einer DHCP Enforcer Access Template verwendet wird. 0.0.0.0 bedeutet, dass ein DHCP-Relay nicht verwendet wird.
Transaction ID	Transaktionskennung, die vom DHCP-Server zurückgegeben wird. Die Transaktionskennung bringt DHCP-Client-Nachrichten mit Server-Reaktionen in Zusammenhang.

3.3.3 Erstellen von DHCP Exemptions

Von der Konformitätsprüfung ausgenommene Endpoints können den Compliance Agent nicht ausführen (z.B. Endpoints, die nicht unter Windows laufen). Exemptions erfassen auch Endpoints, für die keine Konformitätsprüfung erforderlich ist – z.B. Server, Router und Drucker. Exemptions sind nur für Endpoints erforderlich, die eine dynamisch zugewiesene IP-Adresse über DHCP erhalten. Sie müssen für diese Endpoints DHCP Exemptions erstellen, da sie sonst keinen Netzwerkzugriff erhalten, wenn Sie DHCP Enforcement aktivieren.

In NAC Manager können zwei Arten von DHCP Exemptions erstellt werden:

- **Exemptions nach DHCP-Kriterien:** Exemptions, die nach MAC-Adresse, Benutzerklasse und Herstellerklasse erstellt werden.
- **Exemptions nach IP-Bereichen:** Ausnahmen, die für Netzwerksegmente erstellt werden.

3.3.3.1 Erstellen von DHCP-Ausschlusskriterien

Auf der Seite **Exemptions** NAC Manager können Sie Exemptions erstellen, die auf DHCP-Kriterien basieren. Der gemeinsame Einsatz von Ausnahmekriterien und DHCP Enforcer Access Templates ermöglicht die Erkennung von Ausnahmen und die Bestimmung von Maßnahmen. Wenn die festgelegten Ausnahmekriterien auf einen Endpoint zutreffen, so werden die Netzwerkzugriffsrechte durch entsprechende DHCP Enforcer Access Templates geregelt.

Vorgehensweise

1. Melden Sie sich an NAC Manager an.
2. Klicken Sie auf **Enforce > Exemptions** . Klicken Sie links unten auf der Seite auf **Create Exemption**.
3. Geben Sie einen Namen und eine Beschreibung für die Exemption ein.
4. Klicken Sie auf das Listenfeld **Exemption Type** und wählen Sie **DHCP Criteria**.

5. Wählen Sie unter **Exemption Criteria** die Option **MAC Address**, **User Class** oder **Vendor Class**, geben Sie die entsprechende MAC-Adresse (oder das Präfix), die Benutzerklasse oder Herstellerklasse in die jeweiligen Felder ein und klicken Sie auf **Add**, um ein Kriterium für die Exemption zu erstellen.

Wiederholen Sie diesen Schritt für weitere Kriterien für Exemptions.

Hinweis: Bei der Angabe von Exemptions können Sie den Platzhalter * verwenden, er muss jedoch am Ende stehen. Die Angabe von AA* als MAC-Adresse schließt z.B. alle MAC-Adressen aus, die mit AA beginnen. Wenn Sie eine MAC-Adresse ohne Sternchen (*) angeben, ist die vollständige MAC-Adresse erforderlich.

6. Klicken Sie auf **Select**, um der Exemption DHCP Enforcer Access Templates zuzuordnen. Wählen Sie die Access Template **DHCP - Full Access** und klicken Sie auf **OK**.

Die Access Template **DHCP - Full Access** ist in Sophos NAC bereits vorhanden und erlaubt den Netzwerkzugriff. Sie haben für diese Exemption festgelegt, dass sie ohne eine Konformitätsprüfung von Sophos NAC auf das Netzwerk zugreift.

7. Klicken Sie auf **Save**.

3.3.3.2 Erstellen von Exemptions nach IP-Bereichen

Exemptions sind nur für Endpoints erforderlich, die eine dynamisch zugewiesene IP-Adresse über DHCP erhalten. Auf der Seite Exemptions in NAC Manager können Sie Exemptions erstellen, die auf IP-Bereichen basieren. Bei Exemptions nach IP-Bereichen (IP Scope Exemptions) handelt es sich um Exemptions, die für Netzwerksegmente erstellt werden. Exemptions nach IP-Bereichen sind hilfreich, wenn Sie Richtlinien im Unternehmen schrittweise durchsetzen möchten. Sie können Netzwerksegmente von der Konformitätsprüfung ausschließen, die noch nicht einbezogen werden sollen.

Vorgehensweise

1. Melden Sie sich an NAC Manager an.
2. Klicken Sie auf **Enforce > Exemptions**. Klicken Sie links unten auf der Seite auf **Create Exemption**.
3. Geben Sie einen Namen und eine Beschreibung für die Exemption ein.
4. Klicken Sie auf das Listenfeld **Exemption Type** und wählen Sie **IP Scope**.
5. Klicken Sie unter Exempted IP Scopes auf **Select**, um der Exemption weitere IP-Bereiche zuzuweisen, wählen Sie die entsprechenden Bereiche und klicken Sie auf **OK**.

Wenn der gewünschte IP-Bereich nicht aufgeführt wird, erstellen Sie einen neuen. Hierzu müssen Sie entweder eine neue DHCP Enforcer Access Template erstellen oder eine vorhandene DHCP Enforcer Access Template anpassen.

6. Ändern Sie bei Bedarf die Prioritätsstufe der Bereiche anhand der Pfeile.

Wenn mehrere IP-Bereiche auf eine Ausnahme zutreffen, wird der erste IP-Bereich verwendet. Es empfiehlt sich, speziellen bzw. einschränkenden IP-Bereichen eine höhere Priorität als allgemeineren IP-Bereichen zuzuordnen.

7. Klicken Sie auf **Save**.

Wichtig: Nachdem Sie Exemptions erstellt haben, können Sie ihnen auf der Listenseite **Exemptions** eine Prioritätsstufe zuordnen. Wenn mehr als eine Exemption auf einen Endpoint zutrifft, wird die erstbeste mit dem Endpoint in Zusammenhang stehende Exemption gewählt. Es empfiehlt sich, speziellen bzw. einschränkenden Exemptions eine höhere Priorität zuzuordnen als allgemeineren Exemptions.

3.3.4 Aktivieren von DHCP Enforcement

DHCP Enforcement kann für bekannte und unbekannte Endpoints aktiviert werden. Es empfiehlt sich, auf unbekanntem Endpoints DHCP Enforcement und auf bekannten Endpoints Agent Enforcement einzusetzen. DHCP Enforcement ist in Sophos NAC jedoch auch auf bekannten Endpoints möglich.

3.3.4.1 Aktivieren von DHCP Enforcement für unbekannte Endpoints

DHCP Enforcement kann für unbekannte Endpoints auf allen DHCP-Servern aktiviert werden. So können Sie die DHCP-Server festlegen, die für die Quarantäne unbekannter Endpoints zuständig sind. Über diese Funktion kann DHCP Enforcement schrittweise implementiert werden.

Vor der Aktivierung von DHCP Enforcement für unbekannte Endpoints müssen zunächst Exemptions (Ausnahmen) erstellt werden. Exemptions sind nur für Endpoints erforderlich, die eine dynamisch zugewiesene IP-Adresse über DHCP erhalten.

Vorgehensweise

1. Melden Sie sich an NAC Manager an.
2. Klicken Sie auf **Configure System > Server Settings**.
3. Klicken Sie auf den Namen des DHCP-Servers, für den DHCP Enforcement aktiviert werden soll.
4. Klicken Sie auf die Liste **Unknown Endpoint Mode** und wählen Sie die Option **Enforce** aus. Im Enforce-Modus werden unbekannte Endpoints über die „DHCP - Internet Access“-Template in Quarantäne versetzt oder erhalten Zugriff auf das Internet bzw. Korrekturserver.

Hinweis: Wenn Sie beim Ausführen des DHCP Configuration Wizard einen Proxyserver angegeben haben, können Endpoints auf das Internet zugreifen. Wenn Sie keinen Proxyserver angegeben haben, können Endpoints auf die beim DHCP Configuration Wizard angegebenen Korrekturserver zugreifen. Sie können die Access Template im Bereich **Configure System > Enforcer Settings** ändern.

5. Klicken Sie auf **Speichern**.

3.3.4.2 Aktivieren von DHCP Enforcement für bekannte Endpoints

Sie können DHCP Enforcement für bekannte Endpoints in Richtlinien aktivieren. Wenn Sie DHCP Enforcement oder Agent Enforcement für bekannte Endpoints nutzen möchten, müssen Sie in den gewünschten Richtlinien den Richtlinienmodus (Policy Mode) von Report Only zu Enforce ändern.

Wichtig: Alle Richtlinien und Richtlinienänderungen haben sofortige Gültigkeit, eine Richtlinie wird jedoch nicht auf den Endpoint übertragen, bis der Agent sie abrufen.

Vorgehensweise

1. Melden Sie sich an NAC Manager an.
2. Klicken Sie auf **Manage > Policies**. Klicken Sie dann auf die Richtlinie, die Sie aktualisieren möchten.
3. Klicken Sie auf die Liste **Policy Mode** und wählen Sie die Option **Enforce** aus.
 - **Enforce:** Endpoints werden anhand der zugewiesenen Richtlinie auf Konformität überprüft. Die Ergebnisse werden von NAC Manager in einem Report festgehalten. Es werden Meldungen angezeigt und Korrektur- und Durchsetzungsmaßnahmen anhand der für den entsprechenden Access State zutreffenden Access Templates durchgeführt. Dieser Richtlinienmodus verwendet die Access Templates, die in Schritt 5 zugewiesen werden.
4. Klicken Sie auf die Liste **Agent Enforcement Action** und wählen Sie **Release Renew**. Sie **müssen** die Option **Release Renew** für DHCP Enforcement auf unbekanntem Endpoints wählen.
5. Klicken Sie links im Network Access-Bereich auf **DHCP**. Klicken Sie auf die Registerkarte **Enforce** und überprüfen Sie die zugewiesenen Access Templates.

Hinweis: Standardmäßig enthält jede Richtlinie bereits einige Access Templates. Sorgen Sie dafür, dass die richtigen Access Templates angewandt werden. Übernehmen Sie die Zuweisungen für die Access Templates Report Only und Remediate.

Vorhandene DHCP Enforcer Access Templates

- **Policy Retrieval Error:** Gemäß dem Feld „Update Threshold“ der DHCP-Richtlinie (siehe **Configure System > Enforcer Settings**) ist der Konformitätszustand nicht mehr aktuell. Die Access Template **DHCP – Remediation Access** erlaubt ausschließlich den im DHCP Configuration Wizard angegebenen Korrekturservern den Netzwerkzugriff.
 - **Compliant:** Der Endpoint ist konform. Die Access Template **DHCP – Full Access** erlaubt konformen Endpoints den Netzwerkzugriff.
 - **Partially Compliant:** Der Endpoint ist teilweise konform. Die Access Template **DHCP – Full Access** erlaubt teilkonformen Endpoints den Netzwerkzugriff.
 - **Non-Compliant:** Der Endpoint ist nicht konform. Die Access Template **DHCP – Remediation Access** erlaubt ausschließlich den im DHCP Configuration Wizard angegebenen Korrekturservern den Netzwerkzugriff.
6. Ändern Sie bei Bedarf die Prioritätsstufe der DHCP Enforcer Access Templates anhand der Pfeile.

Wenn mehr als eine Access Template auf einen Access State zutrifft, wird die erstbeste Template gewählt. Es empfiehlt sich, speziellen bzw. einschränkenden Access Templates eine höhere Priorität zuzuordnen als allgemeineren Access Templates.
 7. Klicken Sie auf **Speichern**.

3.3.4.2.1 Verwenden vorhandener Richtlinien

Mit den vorhandenen Richtlinien können Sie die Konformität mit Sicherheitsrichtlinien sowohl auf verwalteten als auch auf nicht-verwalteten Endpoints durchsetzen.

- **Default:** Diese Standardrichtlinie wird Endpoints zugewiesen, auf denen der Compliance Agent installiert ist, und denen keine andere Richtlinie zugewiesen wurde. Standardmäßig befinden sich Richtlinien im Modus „Report Only“. Die Richtlinie kann den Endpoint nur im Modus „Remediate“ (Korrigieren) oder „Enforce“ (Durchsetzen) korrigieren.
- **Managed:** Diese Richtlinie kann für Endpoints eingesetzt werden, die von Sophos Enterprise Console verwaltet werden und auf denen ein Compliance Agent installiert ist. Standardmäßig befinden sich Richtlinien im Modus „Report Only“. Die Richtlinie kann den Endpoint nur im Modus „Remediate“ (Korrigieren) oder „Enforce“ (Durchsetzen) korrigieren.
- **Unmanaged:** Diese Richtlinie kann unternehmensexternen Endpoints zugewiesen werden. Sie führt keine Korrekturmaßnahmen auf dem Endpoint durch. Der Dissolvable Agent verwendet die Richtlinie „Unmanaged“.

Hinweis: Falls auf einem Endpoint kein Compliance Agent installiert ist und der Dissolvable Agent nicht verwendet wird, so wird der Netzwerkzugriff über die Enforcer-Einstellungen geregelt.

3.3.4.3 DHCP Enforcement in der Praxis

Das Praxiserlebnis mit DHCP Enforcement variiert bei bekannten und unbekanntem Endpoints. Gastbenutzer können über den Compliance Dissolvable Agent auf das Netzwerk zuzugreifen.

- **Unbekannte Endpoints** (Unknown Endpoints) werden nicht von Sophos Enterprise Console verwaltet. Der Compliance Agent ist nicht installiert, Exemptions gelten nicht und der Dissolvable Agent muss nicht ausgeführt werden.
- **Gast-Endpoints** können über Compliance Dissolvable Agent auf Network Access Control zugreifen.
- **Bekannte Endpoints** (Known Endpoints) werden von Sophos Enterprise Console verwaltet. Der Compliance Agent ist installiert und wird ausgeführt.

DHCP Enforcement bei unbekanntem Endpoints

Wird DHCP Enforcement auf unbekanntem Endpoints aktiviert, geschieht Folgendes:

1. Der Endpoint wird gestartet.
2. Der Netzwerkzugriff ist für unbekanntem Endpoints, auf den DHCP aktiviert ist, beschränkt. Diese Endpoints können auf das Internet oder die Korrekturserver zugreifen. Wenn Sie beim Ausführen des DHCP Configuration Wizard einen Proxyserver angegeben haben, können Endpoints auf das Internet zugreifen. Wenn Sie keinen Proxyserver angegeben haben, können Endpoints auf die beim DHCP Configuration Wizard angegebenen Korrekturserver zugreifen.

DHCP Enforcement bei Gast-Endpoints

Wenn Gast-Endpoints bei aktiviertem DHCP Enforcement auf den Compliance Dissolvable Agent zugreifen müssen, geschieht Folgendes:

1. Der Endpoint wird gestartet.

2. Der Benutzer muss die URL des Compliance Dissolvable Agents in Internet Explorer öffnen und den Compliance Dissolvable Agent ausführen.
3. Der Compliance Dissolvable Agent prüft die Konformität des Endpoints mit der NAC-Richtlinie.
4. Wird DHCP Enforcement konfiguriert und aktiviert:
 - Konforme Endpoints können auf das Netzwerk zugreifen.
 - Teilkonforme Endpoints können auf das Netzwerk zugreifen. Benutzer nicht-konformer Endpoints erhalten Meldungen des Compliance Dissolvable Agents, um die Korrektur zu ermöglichen. Wenn in der NAC-Richtlinie automatische Korrektur festgelegt wurde, werden Korrekturmaßnahmen am Endpoint vorgenommen. Standardmäßig ist die Korrektur deaktiviert. Von Korrektur der Endpoints von Gastbenutzern wird abgeraten.
 - Nicht-konforme Endpoints können auf das Netzwerk zugreifen. Diese Endpoints können auf das Internet oder die Korrekturserver zugreifen. Wenn Sie beim Ausführen des DHCP Configuration Wizard einen Proxyserver angegeben haben, können Endpoints auf das Internet zugreifen. Wenn Sie keinen Proxyserver angegeben haben, können Endpoints auf die beim DHCP Configuration Wizard angegebenen Korrekturserver zugreifen. Benutzer nicht-konformer Endpoints erhalten Meldungen des Compliance Dissolvable Agents, um die Korrektur zu ermöglichen. Wenn in der NAC-Richtlinie automatische Korrektur festgelegt wurde, werden Korrekturmaßnahmen am Endpoint vorgenommen. Standardmäßig ist die Korrektur deaktiviert. Von Korrektur der Endpoints von Gastbenutzern wird abgeraten.

DHCP Enforcement bei bekannten Endpoints

Wird DHCP Enforcement auf bekannten Endpoints aktiviert, geschieht Folgendes:

1. Der Endpoint wird gestartet und der Compliance Agent wird ausgeführt.
2. Der Compliance Agent prüft die Konformität des Endpoints mit der NAC -Richtlinie.
3. Wird DHCP Enforcement konfiguriert und aktiviert:
 - Konforme Endpoints können auf das Netzwerk zugreifen.
 - Teilkonforme Endpoints können auf das Netzwerk zugreifen. Benutzer nicht-konformer Endpoints erhalten Meldungen des Compliance Agents, um die Korrektur zu ermöglichen. Wenn in der NAC-Richtlinie automatische Korrektur des Endpoints festgelegt wurde, werden Korrekturmaßnahmen vorgenommen.
 - Nicht-konforme Endpoints können auf das Netzwerk zugreifen. Die Endpoints können auf die im DHCP Configuration Wizard angegebenen Korrekturserver zugreifen. Benutzer nicht-konformer Endpoints erhalten Meldungen des Compliance Agents, um die Korrektur zu ermöglichen. Wenn in der NAC-Richtlinie automatische Korrektur festgelegt wurde, werden Korrekturmaßnahmen am Endpoint vorgenommen.

4 DHCP Enforcement-Upgrade

Sie müssen die DHCP Enforcement-Software upgraden, um DHCP Enforcement in Sophos NAC 3.9 einsetzen zu können. Für das Upgrade müssen Sie DHCP Enforcement-Software deinstallieren und die neue Software installieren. Vor der Deinstallation der Software muss DHCP Enforcement deaktiviert und im Anschluss an die Installation wieder aktiviert werden.



Hinweis: DHCP Enforcement muss beim Upgrade deaktiviert sein. Es empfiehlt sich, DHCP Enforcement upzugraden, wenn das Netzwerk nicht voll ausgelastet ist.

4.1 DHCP Enforcement-Upgrade-Checkliste

Die DHCP Enforcement-Upgrade-Checkliste enthält alle für das Upgrade von DHCP Enforcement auf Sophos NAC 3.9 erforderlichen Punkte. Falls nichts anderes angegeben ist, werden die Punkte der Checkliste gemäß den Anweisungen in diesem Dokument ausgeführt.

Schritt	Beschreibung	Erledigt
Upgrade von Sophos NAC		
1.	Upgrade von Sophos NAC. Weitere Informationen finden Sie im Endpoint Security and Control 9.5 Upgrade-Center unter http://www.sophos.de/support/upgrades/ .	
Sophos NAC Manager-Tasks, Teil 1		
2.	Deaktivieren von DHCP Enforcement.	
DHCP-Server		
3.	Deinstallieren der vorhandenen DHCP Enforcer-Software auf allen DHCP-Servern.	
4.	<p>Installieren der neuen DHCP Enforcer-Software auf allen DHCP-Servern.</p> <p>Wichtig: Wenn Sie die DHCP Enforcer-Software auf einem DHCP-Server installieren, müssen Sie erneut einen gemeinsamen Schlüssel eingeben. Nach Möglichkeit sollten Sie den gemeinsamen Schlüssel aus der Vorgängerversion verwenden, da dieser mit dem gemeinsamen Schlüssel im NAC Manager für den gleichen DHCP-Server übereinstimmt. Wenn Sie den gemeinsamen Schlüssel aus der Vorgängerversion nicht kennen, können Sie im Zuge der Softwareinstallation einen Schlüssel erstellen. In diesem Fall müssen Sie jedoch den gemeinsamen Schlüssel in NAC Manager für den DHCP-Server anpassen.</p> <p>Hinweis: Stellen Sie nach der Installation der DHCP Enforcer-Software sicher, dass der DHCP-Dienst auf allen DHCP-Servern läuft.</p>	
Sophos NAC Manager-Tasks, Teil 2		
5.	Anpassen des gemeinsamen Schlüssels für alle DHCP-Server. (Optional)	

Schritt	Beschreibung	Erledigt
6.	Aktivieren von DHCP Enforcement.	

4.2 Deaktivieren von DHCP Enforcement

DHCP Enforcement muss beim Upgrade für unbekannte und bekannte Endpoints deaktiviert werden. Es empfiehlt sich, auf unbekanntes Endpoints DHCP Enforcement und auf bekannten Endpoints Agent Enforcement einzusetzen. DHCP Enforcement ist in Sophos NAC jedoch auch auf bekannten Endpoints möglich.

4.2.1 Deaktivieren von DHCP Enforcement für unbekannte Endpoints

Zum Deaktivieren von DHCP Enforcement für unbekannte Endpoints müssen Sie den Modus auf allen DHCP-Servern von „Enforce“ in „Report Only“ ändern.

Vorgehensweise

1. Klicken Sie auf **Configure System > Server Settings**.
2. Klicken Sie auf den Namen des DHCP-Servers, für den DHCP Enforcement deaktiviert werden soll.
3. Klicken Sie auf die Liste **Unknown Endpoint Mode** und wählen Sie die Option **Report Only** aus. Im Modus „Report Only“ wird unbekanntes Endpoints über die „DHCP - Full Access“-Template Netzwerkzugriff gewährt.
4. Klicken Sie auf **Speichern**.

4.2.2 Deaktivieren von DHCP Enforcement für bekannte Endpoints

Um DHCP Enforcement zu deaktivieren, müssen Sie den Policy Mode in den entsprechenden Richtlinien von „Enforce“ in „Report Only“ ändern.

Wichtig: Alle Richtlinien und Richtlinienänderungen haben sofortige Gültigkeit, eine Richtlinie wird jedoch nicht auf den Endpoint übertragen, bis der Agent sie abrufen.

Hinweis: Wenn Sie für bekannte Endpoints Agent Enforcement statt DHCP Enforcement einsetzen, ist dieser Schritt nicht erforderlich.

Vorgehensweise

1. Melden Sie sich an NAC Manager an.
2. Klicken Sie auf **Manage > Policies**. Klicken Sie dann auf die Richtlinie, die Sie aktualisieren möchten.
3. Klicken Sie auf die Liste **Policy Mode** und wählen Sie die Option **Report Only** aus.
 - **Report Only:** Endpoints werden anhand der zugewiesenen Richtlinie auf Konformität überprüft. Die Ergebnisse werden von NAC Manager in einem Report festgehalten. Es werden keine Meldungen angezeigt oder Korrektur- und Durchsetzungsmaßnahmen durchgeführt. Im Modus „Report Only“ wird bekannten Endpoints über die „DHCP - Full Access“-Template Netzwerkzugriff gewährt.

4. Klicken Sie auf **Speichern**.

4.3 Deinstallation der DHCP Enforcer-Software

Deinstallieren Sie die DHCP Enforcer-Software auf allen Microsoft DHCP-Servern. Die DHCP Enforcer-Software enthält den DHCP Enforcer und das DHCP Enforcer Configuration Utility.

1. Rufen Sie über das Startmenü **Systemsteuerung > Software** auf.
2. Wählen Sie **Sophos DHCP Enforcer Software** und klicken Sie auf **Entfernen**.
3. Klicken Sie auf **Ja**, um die DHCP Enforcer-Software zu entfernen.

4.4 Installation der DHCP Enforcer-Software

Installieren Sie die DHCP Enforcer-Software auf allen Microsoft DHCP-Servern. Die DHCP Enforcer-Software enthält den DHCP Enforcer und das DHCP Enforcer Configuration Utility. Der DHCP-Server wird im Verlauf der Installation konfiguriert. Mit dem DHCP Enforcer Configuration Utility können Sie bei der Installation festgelegte DHCP Server-Einstellungen ändern. Nähere Informationen finden Sie unter [Anhang: DHCP Enforcer Configuration Utility](#) (Seite 24).

1. Rufen Sie <http://www.sophos.de/support/updates/> auf.
2. Geben Sie Ihre MySophos-Zugangsdaten ein.
3. Laden Sie von der Website für **Enterprise** -Downloads den NAC DHCP Enforcer-Installer herunter.
4. Führen Sie den Installer aus.

Ein Installationsassistent leitet Sie durch die Installation. Übernehmen Sie die Voreinstellungen.

Es empfiehlt sich, sich den gemeinsamen Schlüssel, den Sie auf der Seite **Sophos DHCP Enforcer** eingegeben haben, zu notieren. Der gemeinsame Schlüssel sichert den Datenfluss zwischen dem NAC-Server und dem DHCP-Server ab. Sie müssen den gemeinsamen Schlüssel eingeben, wenn Sie den DHCP Configuration Wizard mit NAC Manager ausführen.

Hinweis: Stellen Sie nach der Installation der DHCP Enforcer-Software sicher, dass der DHCP-Dienst auf allen DHCP-Servern läuft.

4.5 Anpassen des gemeinsamen Schlüssels des DHCP-Servers

Der gemeinsame Schlüssel sichert den Datenfluss zwischen dem NAC-Server und dem DHCP-Server ab.

Wenn Sie die DHCP Enforcer-Software auf einem DHCP-Server installieren, müssen Sie erneut einen gemeinsamen Schlüssel eingeben. Nach Möglichkeit sollten Sie den gemeinsamen Schlüssel aus der Vorgängerversion verwenden, da dieser mit dem gemeinsamen Schlüssel im NAC Manager für den gleichen DHCP-Server übereinstimmt. Wenn Sie den gemeinsamen Schlüssel aus der Vorgängerversion nicht kennen, können Sie im Zuge der Softwareinstallation

einen Schlüssel erstellen. In diesem Fall müssen Sie jedoch den gemeinsamen Schlüssel in NAC Manager für den DHCP-Server anpassen.

Hinweis: Wenn Sie bei der Installation der DHCP Enforcer-Software den Schlüssel aus der Vorgängerversion verwendet haben, ist dieser Schritt nicht erforderlich.

Vorgehensweise

1. Klicken Sie auf **Configure System > Server Settings** .
2. Klicken Sie auf den Namen des DHCP-Servers, dessen Schlüssel angepasst werden muss.
3. Geben Sie den gemeinsamen Schlüssel des Servers ein.

Wichtig: Der Schlüssel muss mit Ihrer Eingabe bei der Installation der DHCP Enforcer-Software auf dem DHCP-Server übereinstimmen.

4. Klicken Sie auf **Speichern**.

4.6 Aktivieren von DHCP Enforcement

DHCP Enforcement kann für bekannte und unbekannte Endpoints aktiviert werden. Es empfiehlt sich, auf unbekanntem Endpoints DHCP Enforcement und auf bekannten Endpoints Agent Enforcement einzusetzen. DHCP Enforcement ist in Sophos NAC jedoch auch auf bekannten Endpoints möglich.

4.6.1 Aktivieren von DHCP Enforcement für unbekannte Endpoints

DHCP Enforcement kann für unbekannte Endpoints auf allen DHCP-Servern aktiviert werden. So können Sie die DHCP-Server festlegen, die für die Quarantäne unbekannter Endpoints zuständig sind. Über diese Funktion kann DHCP Enforcement schrittweise implementiert werden.

Vor der Aktivierung von DHCP Enforcement für unbekannte Endpoints müssen zunächst Exemptions (Ausnahmen) erstellt werden. Exemptions sind nur für Endpoints erforderlich, die eine dynamisch zugewiesene IP-Adresse über DHCP erhalten.

Vorgehensweise

1. Melden Sie sich an NAC Manager an.
2. Klicken Sie auf **Configure System > Server Settings** .
3. Klicken Sie auf den Namen des DHCP-Servers, für den DHCP Enforcement aktiviert werden soll.
4. Klicken Sie auf die Liste **Unknown Endpoint Mode** und wählen Sie die Option **Enforce** aus. Im Enforce-Modus werden unbekannte Endpoints über die „DHCP - Internet Access“-Template in Quarantäne versetzt oder erhalten Zugriff auf das Internet bzw. Korrekturserver.

Hinweis: Wenn Sie beim Ausführen des DHCP Configuration Wizard einen Proxyserver angegeben haben, können Endpoints auf das Internet zugreifen. Wenn Sie keinen Proxyserver angegeben haben, können Endpoints auf die beim DHCP Configuration Wizard angegebenen Korrekturserver zugreifen. Sie können die Access Template im Bereich **Configure System > Enforcer Settings** ändern.

5. Klicken Sie auf **Speichern**.

4.6.2 Aktivieren von DHCP Enforcement für bekannte Endpoints

Sie können DHCP Enforcement für bekannte Endpoints in Richtlinien aktivieren. Wenn Sie DHCP Enforcement oder Agent Enforcement für bekannte Endpoints nutzen möchten, müssen Sie in den gewünschten Richtlinien den Richtlinienmodus (Policy Mode) von Report Only zu Enforce ändern.

Wichtig: Alle Richtlinien und Richtlinienänderungen haben sofortige Gültigkeit, eine Richtlinie wird jedoch nicht auf den Endpoint übertragen, bis der Agent sie abruft.

Vorgehensweise

1. Melden Sie sich an NAC Manager an.
2. Klicken Sie auf **Manage > Policies**. Klicken Sie dann auf die Richtlinie, die Sie aktualisieren möchten.
3. Klicken Sie auf die Liste **Policy Mode** und wählen Sie die Option **Enforce** aus.
 - **Enforce:** Endpoints werden anhand der zugewiesenen Richtlinie auf Konformität überprüft. Die Ergebnisse werden von NAC Manager in einem Report festgehalten. Es werden Meldungen angezeigt und Korrektur- und Durchsetzungsmaßnahmen anhand der für den entsprechenden Access State zutreffenden Access Templates durchgeführt. Dieser Richtlinienmodus verwendet die Access Templates, die in Schritt 5 zugewiesen werden.
4. Klicken Sie auf die Liste **Agent Enforcement Action** und wählen Sie **Release Renew**. Sie **müssen** die Option **Release Renew** für DHCP Enforcement auf unbekanntem Endpoints wählen.
5. Klicken Sie links im Network Access-Bereich auf **DHCP**. Klicken Sie auf die Registerkarte **Enforce** und überprüfen Sie die zugewiesenen Access Templates.

Hinweis: Standardmäßig enthält jede Richtlinie bereits einige Access Templates. Sorgen Sie dafür, dass die richtigen Access Templates angewandt werden. Übernehmen Sie die Zuweisungen für die Access Templates Report Only und Remediate.

Vorhandene DHCP Enforcer Access Templates

- **Policy Retrieval Error:** Gemäß dem Feld „Update Threshold“ der DHCP-Richtlinie (siehe **Configure System > Enforcer Settings**) ist der Konformitätszustand nicht mehr aktuell. Die Access Template **DHCP – Remediation Access** erlaubt ausschließlich den im DHCP Configuration Wizard angegebenen Korrekturservern den Netzwerkzugriff.
- **Compliant:** Der Endpoint ist konform. Die Access Template **DHCP – Full Access** erlaubt konformen Endpoints den Netzwerkzugriff.
- **Partially Compliant:** Der Endpoint ist teilweise konform. Die Access Template **DHCP – Full Access** erlaubt teilkonformen Endpoints den Netzwerkzugriff.
- **Non-Compliant:** Der Endpoint ist nicht konform. Die Access Template **DHCP – Remediation Access** erlaubt ausschließlich den im DHCP Configuration Wizard angegebenen Korrekturservern den Netzwerkzugriff.

6. Ändern Sie bei Bedarf die Prioritätsstufe der DHCP Enforcer Access Templates anhand der Pfeile.

Wenn mehr als eine Access Template auf einen Access State zutrifft, wird die erstbeste Template gewählt. Es empfiehlt sich, speziellen bzw. einschränkenden Access Templates eine höhere Priorität zuzuordnen als allgemeineren Access Templates.

7. Klicken Sie auf **Speichern**.

5 Anhang: DHCP Enforcer Configuration Utility

Mit dem **DHCP Enforcer Configuration Utility** können Sie bei der Installation festgelegte DHCP Enforcer-Einstellungen ändern. Das Dienstprogramm wird bei der Installation des DHCP Enforcers auf dem DHCP-Server installiert. Bei mehreren DHCP-Servern müssen Sie die Einstellungen auf allen Servern ändern.

5.1 Aktualisieren des gemeinsamen Schlüssels

Vorgehensweise

Der Schlüssel muss mit Ihrer Eingabe bei der Installation des DHCP Enforcers auf dem Server übereinstimmen. Der gemeinsame Schlüssel sichert den Datenfluss zwischen dem NAC-Server und dem DHCP-Server ab.

1. Wählen Sie im Startmenü des DHCP-Servers **Sophos > NAC > Support Tools > DHCP Enforcer Configuration Utility**.

Das Dialogfeld **DHCP Enforcer Configuration Utility** wird angezeigt. Die Registerkarte **Enforcer** ist ausgewählt.

2. Klicken Sie im Dialogfeld **DHCP Enforcer Configuration Utility** auf **Edit**.
3. Geben Sie den neuen gemeinsamen Schlüssel in das Dialogfeld **DHCP Enforcer RADIUS Enforcer Server Settings** ein, bestätigen Sie die Angabe und klicken Sie auf **OK**.

5.2 Ändern der erweiterten Einstellungen

Im Folgenden wird erläutert, wie Sie mit dem DHCP Enforcer Configuration Utility Änderungen an den erweiterten Einstellungen (Advanced Settings) des DHCP Enforcers vornehmen können. In der Regel ist dies jedoch nicht erforderlich.

Vorgehensweise

1. Wählen Sie im Startmenü des DHCP-Servers **Sophos > NAC > Support Tools > DHCP Enforcer Configuration Utility**.

Das Dialogfeld **DHCP Enforcer Configuration Utility** wird angezeigt. Die Registerkarte **Enforcer** ist ausgewählt.

2. Klicken Sie im Dialogfeld **DHCP Enforcer Configuration Utility** auf die Registerkarte **Advanced**.
3. Ändern Sie die DHCP Enforcer-Einstellungen je nach Bedarf.
4. Klicken Sie auf **OK**.

Wiederholen Sie die obigen Schritte auf allen in Frage kommenden DHCP-Servern.

5.2.1 Optionen des Dienstprogramms „DHCP Enforcer Configuration Utility“

Feld	Beschreibung
Registerkarte „Enforcer“	
Access for Multiple Servers	Diese Option steht für Sophos Endpoint Security and Control nicht zur Verfügung.
Dialogfeld „DHCP Enforcer RADIUS Enforcer Server Settings“	
Klicken Sie auf die Schaltfläche zum Bearbeiten , um auf das Dialogfeld zuzugreifen.	
Hinweis: Die Dialogfeldoptionen beziehen sich auf den NAC-Server.	
Enable	Diese Option gibt an, ob der NAC-Server aktiv ist. Wenn das Feld ausgewählt ist, wird der NAC-Server für die Konformitätsprüfung von Richtlinien und Reportaktivitäten genutzt.
IP-Adresse	Dieses Feld enthält die IP-Adresse des NAC-Server.
Authentication Port	In diesem Feld ist der Authentifizierungsport des NAC-Servers angegeben.
Accounting Port	In diesem Feld ist der Kontoführungsport des NAC-Servers angegeben.
Shared Key	Dieses Feld enthält den gemeinsamen Schlüssel des DHCP-Servers. Dabei handelt es sich um den gleichen gemeinsamen Schlüssel, der bei der Installation des DHCP-Servers verwendet wurde.
Confirm Shared Key	Dieses Feld dient der Bestätigung des gemeinsamen Schlüssels des DHCP-Servers.
Dialogfeld „DHCP Enforcer Resolve IP“	
Hostname	Dieses Feld enthält den Hostnamen, wenn die IP-Adresse des NAC-Servers unbekannt ist. Nach Eingabe des Hostnamen können Sie den Hostnamen in die IP-Adresse auflösen.
Registerkarte „Advanced“	
Enable Policy Compliance	Mit diesem Feld werden Richtlinienkonformität und Reporting für alle DHCP-Anfragepakete aktiviert, mit Ausnahme der durch den reservierten Optionscode identifizierten.
Attempts	Dieses Feld gibt an, wie oft die Konformitätsprüfung einer Richtlinie für ein DHCP-Anfragepaket gestartet wird.
Timeout	Dieses Feld gibt in Sekunden an, wie lange der DHCP-Server wartet, bevor eine weitere Konformitätsprüfung für eine Richtlinie durchgeführt wird.
Default User Class	Dieses Feld gibt die zu verwendende Benutzerklasse an, wenn die in der Richtlinie definierte Benutzerklasse wegen eines Fehlers bei der Konformitätsprüfung der Richtlinie nicht abgerufen werden kann.

Feld	Beschreibung
Error	Wird diese Option aktiviert, werden Fehlermeldungen von Microsoft im Application Event Log gespeichert.
Hinweis	Wird diese Option aktiviert, werden Microsoft-Warnhinweise im Application Event Log gespeichert.
Information	Wird diese Option aktiviert, werden Hinweise zur Information von Microsoft im Application Event Log gespeichert.
Trace	Wird diese Option aktiviert, wird das Ablaufverfolgungsprotokoll von Microsoft im Application Event Log gespeichert.
Subnet Mask Override	Hier wird die Subnetzmaske für nicht-konforme Benutzer festgelegt. Die Subnetzmaske übergeht somit das Subnetz auf dem DHCP-Server, um den Netzwerkzugriff zu beschränken.
Black Hole IP Address	Es handelt sich hierbei um eine Test-IP-Adresse, über die der DHCP Enforcer gesperrte Datenbewegungen im Netzwerk beseitigen kann.
Dialogfeld „DHCP Enforcer Informs IP Address“	
IP-Adresse	Dieses Feld bestimmt die IP-Adresse des Clients, z.B. eines Remote Access Concentrators (RAC), für den Richtlinienkonformität und Reports für DHCP Inform-Pakete umgegangen werden sollen. Standardmäßig wird für DHCP Inform-Pakete die Richtlinienkonformität überprüft und Reports werden erstellt. Wird eine IP-Adresse angegeben, sind DHCP Inform-Pakte des Clients von der Richtlinienkonformitätsprüfung und Report-Erstellung ausgenommen .
Dialogfeld „DHCP Enforcer Resolve IP“	
Hostname	Die Option erkennt den Hostnamen des Clients, den Sie von der Richtlinienkonformitätsprüfung und Report-Erstellung ausnehmen möchten, wenn die IP-Adresse nicht bekannt ist. Nach Eingabe des Hostnamen können Sie den Hostnamen in die IP-Adresse auflösen.

6 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.

7 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.