

Sophos NAC Manager Hilfe

Produktversion: 3.9
Stand: Dezember 2011



Inhalt

1 NAC Manager im Überblick.....	3
2 Manage-Bereich im Überblick.....	12
3 Enforce-Bereich im Überblick.....	45
4 Report-Bereich im Überblick.....	58
5 Konfigurationsbereich im Überblick.....	79
6 Logging Tool.....	86
7 Maintenance Mode Tool.....	91
8 Glossar.....	93
9 Technischer Support.....	99
10 Rechtlicher Hinweis.....	100

1 NAC Manager im Überblick

Die Online-Hilfe enthält Anweisungen und Informationen zur Bedienung von NAC Manager.

Einschränkung:

1.1 Implementierung von Network Access Control

Dieser Abschnitt bietet Tipps zur Implementierung von Network Access Control.

Prozessablauf	Schritte
Sie können die Computer über Sophos Enterprise Console mit Sophos NAC schützen.	<ol style="list-style-type: none"> 1. Starten Sie in Sophos Enterprise Console den Assistenten zum Schützen von Computern.
Ermitteln des aktuellen Konformitätszustands mit den Reports von NAC Manager.	<ol style="list-style-type: none"> 1. Bestimmen Sie den Konformitätszustand der Benutzer anhand der Reports in NAC Manager. Hinweis: Die Reports in NAC Manager bieten einen Überblick über die tatsächliche Konformität einzelner Benutzer mit der verwalteten Richtlinie. 2. Mit den Reports in NAC Manager können Sie feststellen, ob die Benutzerbenachrichtigungen angemessen sind. Hinweis: Benutzer können die Meldungen erst dann einsehen, wenn Sie den Richtlinienmodus in „Remediate“ oder „Enforcement“ ändern. Dies wird in den folgenden Schritten durchgeführt.
Aktualisieren der Profile von NAC Manager nach Belieben.	<ol style="list-style-type: none"> 1. Ändern Sie die Profile von Sophos Anti-Virus und/oder Sophos Client Firewall. Überprüfen Sie, ob in die Profile die korrekten Einstellungen für Betriebssysteme, Benachrichtigungen und Korrekturmaßnahmen aufweisen. 2. Ermitteln Sie anhand der Reports in NAC Manager, ob die Profilaktualisierung wie gewünscht erfolgte.
Implementieren der Korrekturrichtlinie.	<ol style="list-style-type: none"> 1. Aktualisieren Sie die „Managed“-Richtlinie. Ändern Sie den Richtlinienmodus von Report Only in Remediate. 2. Ermitteln Sie anhand der Reports in NAC Manager den aktuellen Unternehmenskonformitätszustand. Hinweis: Im Laufe der Zeit sollten Endpoints, die nicht oder nur teilweise konform sind, korrigiert und somit konform werden.

Prozessablauf	Schritte
Bedarfsabhängiges Erstellen und Aktualisieren von Access Templates.	<ol style="list-style-type: none"> 1. Erstellen oder aktualisieren Sie Access Templates. Hinweis: Wenn der Netzwerkzugriff über Agent Enforcement durchgesetzt werden soll, erstellen oder aktualisieren Sie Agent Enforcer Access Templates. Wenn der Netzwerkzugriff über DHCP Enforcement durchgesetzt werden soll, erstellen oder aktualisieren Sie DHCP Enforcer Access Templates. Weitere Informationen finden Sie unter Praxistipps: Access Templates (Seite 46). 2. Anhand der Reports in NAC Manager können Sie feststellen, ob den Endpoints der gewünschte Netzwerkzugriff gewährt wird.
Implementieren der Durchsetzungsrichtlinie.	<ol style="list-style-type: none"> 1. Aktualisieren Sie die „Managed“-Richtlinie. Ändern Sie den Richtlinienmodus von Remediate in Enforce. 2. Ermitteln Sie anhand der Reports in NAC Manager den aktuellen Unternehmenskonformitätszustand. Hinweis: Im Laufe der Zeit müssen nicht-konforme Endpoints korrigiert werden, damit den Benutzern nicht der Zugriff auf Netzwerkressourcen verweigert wird.

1.2 Anmeldung an NAC Manager

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

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

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

Beim ersten Aufruf von NAC Manager müssen Sie das Kennwort ändern. Notieren Sie sich dieses Kennwort: Bis Sie andere Benutzerkonten angelegt haben, können Sie nur über dieses Kennwort auf NAC Manager zugreifen. Weitere Informationen finden Sie unter [Erstellen eines Kontos](#) (Seite 80).

1.3 Aufrufen der Startseite

Die Startseite enthält folgende Bedienelemente.
















- **Current Compliance:** Grafische Ansicht der aktuellen Konformitätszustände aller Endpoint-Agenten, die in den letzten sieben Tagen im Report verzeichnet wurden. Weitere Informationen finden Sie unter [Erstellen von Compliance Reports](#) (Seite 59).
- **Compliance Trend:** Grafische Ansicht von Übereinstimmungs-Trends der letzten sieben Tage. Weitere Informationen finden Sie unter [Erstellen von Compliance Reports](#) (Seite 59).







- **Server Task Status:** Status jedes Ladeprozesses nach Server sortiert. Wenn ein Ladeprozess nicht ausgeführt werden kann, klicken Sie auf den Link **Error**, um ausführliche Fehlerangaben zu erhalten. Es gibt folgende Ladeprozesse:
 - **Current Definition Loader:** Ruft die neuesten Signaturdaten zu Virenschutz- und Spywareschutzanwendungen von Sophos ab.
 - **Report Warehouse Loader:** Regelt die Löschung von Reportdaten.

1.4 Symbole in NAC Manager

Die Symbole in NAC Manager stellen Maßnahmen oder sonstige Versinnbildlichungen dar. In der folgenden Tabelle werden alle Symbole beschrieben.

Symbol	Beschreibung
Allgemeine Funktionen	
	Erhöht die Priorität eines Listenelements.
	Verringert die Priorität eines Listenelements.
	Löscht ein Listenelement. Das Löschen von Listenelementen, z.B. von Profilen, muss bestätigt werden. Das Löschen von Einstellungen eines Elements, z.B. die Fähigkeiten, muss nicht bestätigt werden.
	Markiert ein Element oder eine Aufgabe als verpflichtend. Dies bedeutet, dass das Element bzw. die Aufgabe abgeschlossen werden muss, bevor Sie eine andere Aufgabe durchführen oder die Daten auf der Seite speichern können.
	Dieses Symbol kennzeichnet ein freigegebenes Element. Durch Klicken auf das Symbol kann ein Element gesperrt werden. Nur Systemadministratoren und Administratoren können Elemente sperren.
	Dieses Symbol kennzeichnet ein gesperrtes Element. Durch Klicken auf das Symbol geben Sie ein Element frei (d.h. die Sperrung wird aufgehoben). Systemadministratoren können alle Elemente freigeben. Administratoren können nur solche Elemente freigeben, die sie selbst gesperrt haben.
	Dieses Symbol kennzeichnet ein gesperrtes Element, das nicht vom angemeldeten Benutzer freigegeben werden kann. Dabei kann es sich z.B. um spezielle Netzwerkressourcen handeln, die von einem anderen Benutzer gesperrt worden sind.
	Dieses Symbol kennzeichnet einen Fehler auf der Seite, der korrigiert werden muss, bevor eine weitere Aufgabe ausgeführt werden kann oder Änderungen auf der Seite gespeichert werden können.
	Dieses Symbol kennzeichnet eine Informationsmeldung über eine erfolgreich durchgeführte oder gespeicherte Maßnahme.

Symbol	Beschreibung
	Dieses Symbol kennzeichnet einen externen Link, der eine Verknüpfung außerhalb von NAC Manager darstellt.
	Dieses Symbol kennzeichnet ein vorhandenes Element, das nicht geändert werden kann, z.B. eine Standard-Anwendung oder eine Standard-Netzwerkressource. Einige Standard-Elemente lassen sich jedoch als neue Elemente speichern, die Sie ändern können.
Konformitätszustände von Vorlagen	
	Dieses Symbol kennzeichnet Access Templates, die für konforme Endpoints vorgesehen sind.
	Dieses Symbol kennzeichnet Access Templates, die für teilkonforme Endpoints vorgesehen sind.
	Dieses Symbol kennzeichnet Access Templates, die für nicht-konforme Endpoints vorgesehen sind.
Accounts	
	Dieses Symbol kennzeichnet ein aktiviertes Konto. Durch Klicken auf das Symbol wird das Konto deaktiviert.
	Dieses Symbol kennzeichnet ein deaktiviertes Konto. Durch Klicken auf das Symbol wird das Konto aktiviert.
Profile und Richtlinien	
	Dieses Symbol kennzeichnet ein von Quarantine Agent unterstütztes Profil, eine Anwendung oder eine Fähigkeit.
	Dieses Symbol kennzeichnet ein von Dissolvable Agent unterstütztes Profil, eine Anwendung oder eine Fähigkeit.
	Dieses Symbol kennzeichnet ein von Windows 7 unterstütztes Profil, eine Anwendung oder eine Fähigkeit.
	Dieses Symbol kennzeichnet ein von Windows Vista unterstütztes Profil, eine Anwendung oder eine Fähigkeit.
	Dieses Symbol kennzeichnet ein von Windows XP unterstütztes Profil, eine Anwendung oder eine Fähigkeit.
	Dieses Symbol kennzeichnet ein von Windows 2000 unterstütztes Profil, eine Anwendung oder eine Fähigkeit.
	Dieses Symbol kennzeichnet ein von Windows Server 2008 unterstütztes Profil, eine Anwendung oder eine Fähigkeit.
	Dieses Symbol kennzeichnet ein von Windows Server 2003 unterstütztes Profil, eine Anwendung oder eine Fähigkeit.

Symbol	Beschreibung
	Dieses Symbol kennzeichnet eine Korrekturmaßnahme, die von manchen Betriebssystemen nicht unterstützt wird. Klicken Sie auf das Symbol, um die nicht unterstützten Betriebssysteme anzuzeigen.
	Die betreffende Fähigkeit wird zwar von Windows 7 unterstützt, nicht jedoch die zugehörige Korrekturmaßnahme.
	Die betreffende Fähigkeit wird zwar von Windows Vista unterstützt, nicht jedoch die zugehörige Korrekturmaßnahme.
	Die betreffende Fähigkeit wird zwar von Windows XP unterstützt, nicht jedoch die zugehörige Korrekturmaßnahme.
	Die betreffende Fähigkeit wird zwar von Windows 2000 unterstützt, nicht jedoch die zugehörige Korrekturmaßnahme.
	Die betreffende Fähigkeit wird zwar von Windows Server 2008 unterstützt, nicht jedoch die zugehörige Korrekturmaßnahme.
	Die betreffende Fähigkeit wird zwar von Windows Server 2003 unterstützt, nicht jedoch die zugehörige Korrekturmaßnahme.
Anwendungsprofile	
	Dieses Symbol kennzeichnet eine Meldung, die für die Bedingung definiert wurde. Diese Meldung wird auf dem Endpoint nur dann angezeigt, wenn die Bedingung erfüllt ist.
Exemptions	
	Dieses Symbol kennzeichnet eine MAC-Adresse in einer DHCP-Exemption.
	Dieses Symbol kennzeichnet eine Herstellerklasse in einer DHCP-Exemption.
	Dieses Symbol kennzeichnet eine Benutzerklasse in einer DHCP-Exemption.
	Dieses Symbol kennzeichnet einen IP-Bereich in einer DHCP-Exemption.
Reports	
	Ruft den Agent Enforcer Report zu einem ausgewählten Agent Session Report-Eintrag auf.
	Ruft den DHCP Enforcer Report zu einem ausgewählten Agent Session Report-Eintrag auf.
	Ruft Details über Compliance Assessment in Bezug auf Compliance Detail, Agent Session oder Non-Compliance Detail Report-Eintrag auf.

1.5 Situationen, in denen sich das Anlegen von Arbeitskopien (Save as New) empfiehlt

In diesem Abschnitt wird erläutert, wann sich das Anlegen von Arbeitskopien über die Schaltfläche „Save as new“ anbietet.

Typ	Beschreibung
Über die Funktion „Save As New“ können Sie ein vorhandenes Profil oder eine Access Template unter einem neuen Namen speichern und Änderungen vornehmen.	Wenn Sie das vorhandene Profil oder die vorhandene Access Template nicht ändern möchten oder können, können Sie sie so kopieren.
Über die Schaltfläche „Save as New“ können Sie ein Profil oder eine Access Template ändern, das bzw. die bereits auf Richtlinien übertragen wurde, wenn die Änderungen nicht sofort übertragen werden sollen.	Wenn Sie ein vorhandenes Profil oder eine Access Template ändern, das bzw. die bereits in einer oder mehreren Richtlinien verwendet wird, werden die Änderungen sofort wirksam und beim nächsten Abruf der Richtlinie übertragen. Wenn die Änderungen nicht sofort übernommen werden sollen, speichern Sie daher die Richtlinie, das Profil oder die Access Template zunächst unter einem anderen Namen, um eine Arbeitskopie zu erhalten.

1.6 Speichern eines Elements als neues Element

Sie können ein Element unter einem anderen Namen speichern und somit eine Arbeitskopie anlegen, wenn Sie vorhandene Einstellungen wiederverwenden möchten.

Es empfiehlt sich, ein Element unter einem neuen Namen abzuspeichern und somit eine Arbeitskopie anzulegen, bevor Sie Änderungen an den Systemeinstellungen vornehmen. Zu den Elementen, die unter einem neuen Namen abgespeichert werden können, gehören Agent Configuration Templates, Profile, Access Templates, Netzwerkressourcen und Ausnahmen.

Vorgehensweise

1. Klicken Sie auf den entsprechenden Namen des Bereichs: **Manage**, **Enforce** oder **Configure System**.
2. Klicken Sie auf den Bereichsnamen des wiederzuverwendenden Elements.
3. Klicken Sie in der Liste auf den Namen des gewünschten Elements.
4. Klicken Sie auf **Save As New**. Geben Sie nun im Dialogfeld einen neuen Namen für das Element ein und klicken Sie auf **OK**.

Weitere Informationen zum Erstellen oder Aktualisieren von Elementeneinstellungen finden Sie im entsprechenden Kapitel.

1.7 Anzeigen oder Suchen von Listenelementen

In NAC Manager können Sie Listenelemente anzeigen oder nach bestimmten Elementen suchen.

In jedem NAC Manager-Bereich können Sie jederzeit eine Liste der erstellten oder hinzugefügten Elemente anzeigen, nähere Informationen zu einem Element abrufen, ein Element aktualisieren oder löschen. Außerdem können Sie umfangreiche Listen über die Suchoptionen in bestimmten Bereichen kürzen.

Vorgehensweise

1. Klicken Sie auf den entsprechenden Namen des Bereichs: **Manage**, **Enforce** oder **Configure System**.
2. Klicken Sie auf den Bereichsnamen des anzuzeigenden Elements.

Hinweis: Damit die Namen der Anwendungen in der **Applications**-Listenseite einwandfrei angezeigt werden, muss auf dem Computer, auf dem NAC Manager ausgeführt wird, Unterstützung für ostasiatische Sprachen (über **Systemsteuerung** > **Ländereinstellungen**) installiert sein.

3. Wenn Sie sich in **Manage** > **Profiles or Applications** befinden, können Sie in der Liste anhand der Suchkriterien nach bestimmten Elementen suchen. Geben Sie die entsprechenden Suchoptionen ein bzw. wählen Sie sie aus und klicken Sie auf **Search**.

Hinweis: Die Suchwerte für Listenelemente müssen **nicht** hundertprozentig übereinstimmen und es wird **nicht** zwischen Groß- und Kleinschreibung unterschieden. Mithilfe der Symbole * und % ist in den meisten Feldern außerdem eine Platzhaltersuche möglich. Wenn Sie beispielsweise in das Feld Name ein M% eingeben, werden alle mit „M“ beginnenden Namen angezeigt. Wenn Sie dagegen in das Feld Name nur M ohne % eingeben, werden nur Namen namens „M“ angezeigt.

4. Führen Sie einen der folgenden Schritte aus:
 - Zum Sortieren der Liste klicken Sie auf die entsprechende Spaltenüberschrift.
 - Zum Abrufen näherer Informationen zu einem Element oder zum Aktualisieren eines Elements klicken Sie auf den Namen des Elements.
 - Zum Löschen eines Elements markieren Sie das Kästchen neben den entsprechenden Elementen und klicken Sie auf **Delete**. Überprüfen Sie im Dialogfeld die Auswahl der zu löschenden Elemente und klicken Sie auf **OK**.

1.8 Löschen von Elementen

Durch das Löschen von Elementen in NAC Manager werden sie aus der Software entfernt. Es können nur Elemente gelöscht werden, die nicht von einem anderen Element verwendet werden. So können Sie beispielsweise keine Netzwerkressourcen löschen, die einer Agent Enforcer Access Template zugeteilt wurden. Elemente können auch über das Mülleimersymbol gelöscht werden.

Vorgehensweise

1. Klicken Sie auf den entsprechenden Namen des Bereichs: **Manage**, **Enforce** oder **Configure System**.
2. Klicken Sie auf den Bereichsnamen des zu löschenden Elements.
3. Markieren Sie das Kontrollkästchen neben jedem zu löschenden Element.
4. Klicken Sie auf **Delete**.
5. Klicken Sie zur Bestätigung im Dialogfeld auf **OK**.

1.9 Situationen, in den sich das Sperren von Elementen anbietet

In diesem Abschnitt wird erläutert, wann sich das Sperren von Elementen anbietet.

Tipp	Beschreibung
<p>Sie können Richtlinien, Profile, Access Templates und Netzwerkressourcen sperren, um sie vor unbeabsichtigten Änderungen zu schützen.</p>	<p>Durch das Sperren dieser Elemente von NAC Manager schützen Sie sie vor unbeabsichtigten Änderungen. Administratoren können nur Elemente freigeben, die sie selbst gesperrt haben. Systemadministratoren können alle Elemente freigeben.</p> <p>Hinweis: Wenn Sie sichergehen möchten, dass eine gesamte Richtlinie vor Änderungen geschützt ist, sperren Sie neben der eigentlichen Richtlinie auch alle zugehörigen Profile, Access Templates und Netzwerkressourcen.</p>

1.10 Sperren und Freigeben von Elementen in NAC Manager

Wenn Sie ein Element in einer Software sperren, können andere Administratoren es nicht aktualisieren.

Systemadministratoren können alle Elemente freigeben. Administratoren können nur solche Elemente freigeben, die sie selbst gesperrt haben.

Vorgehensweise

1. Klicken Sie auf den entsprechenden Namen des Bereichs: **Manage**, **Enforce** oder **Configure System**.
2. Klicken Sie auf den Bereichsnamen der zu sperrenden oder freizugebenden Elemente.
3. Klicken Sie neben den gewünschten Elementen jeweils auf das **Sperren**-Symbol oder auf das **Freigeben**-Symbol.

Neben jedem Konto wird nun das Symbol des aktuellen Zustands angezeigt.

Hinweis: Einige Elemente, wie Standard-Anwendungen und Standard-Netzwerkressourcen, können weder gesperrt noch freigegeben werden.

1.11 Rechtsklick-Funktionen

Auf allen Listenseiten und in anderen Bereichen stehen Funktionen zur Verfügung, die sich per Rechtsklick anzeigen lassen.

Vorgehensweise

1. Klicken Sie auf den entsprechenden Namen des Bereichs: **Manage**, **Enforce** oder **Configure System**.
2. Klicken Sie auf den Bereichsnamen des gewünschten Elements.
3. Rechtsklicken Sie auf den Namen des Links und wählen Sie die gewünschte Funktion aus. Weitere Informationen zu Bereichen und Funktionen entnehmen Sie bitte der folgenden Tabelle.

Kontextmenüs

Bereich in NAC Manager	Beschreibung
Alle Bereiche	In allen Listen stehen folgende Funktionen zur Auswahl: Edit, View (für Standardelemente, die nicht bearbeitet werden können), Copy, Rename, Delete, Lock/Unlock und View Audit Data. Hinweis: Einige Funktionen sind jedoch nicht für bestimmte Listenelemente verfügbar.
Listenseiten: Agent Configuration Templates, Profiles, Applications, Agent Enforcer Access Templates, DHCP Enforcer Access Templates, Network Resources	Die links aufgezählten Listenseiten bieten neben den oben genannten Funktionen: View Usage Details (zeigt Details zu den Richtlinien, Profilen oder Access Templates an, in denen das ausgewählte Element vorkommt).
Accounts	Die Accounts-Listenseite bietet neben den oben genannten Funktionen: Copy und Lock/Unlock und Enable/Disable.

2 Manage-Bereich im Überblick

Der Manage-Bereich enthält alle Komponenten zur Verwaltung von Richtlinien. Die im Folgenden aufgeführten Bereiche erreichen Sie über das Manage-Menü:

Bereich und Aktion	Beschreibung
Applications	
Verwenden von Standardanwendungstypen.	Anwendungstypen dienen der Kategorisierung von Anwendungen und Festlegung von Standard-Richtlinien für alle unter einer Kategorie zusammengefassten Anwendungen. Standard-Anwendungstypen sind bereits in der Software verfügbar.
Verwenden von Standardanwendungen.	Unter Applications (Anwendungen) sind Programme zu verstehen, die von Sophos NAC erkannt werden. Standard-Anwendungen sind bereits in der Software verfügbar. Anwendungen sind an einen Anwendungstyp gebunden, der beim Hinzufügen des Anwendungsprofils zur Richtlinie eine Bewertungsmethode festlegt.
Agent Configuration Templates	
Erstellen von Agent Configuration Templates.	In Agent Configuration Templates sind optionale Einstellungen zur Funktionsweise des Agenten auf Endpoints festgelegt.
Profiles	
Erstellen von Profilen für Betriebssysteme und/oder Anwendungen oder Übernehmen von vorhandenen Profilen.	<p>In Profilen (Profiles) lassen sich Elemente festlegen, die auf dem Endpoint analysiert bzw. überprüft werden sollen, z.B. Betriebssysteme und Anwendungen. Nach der Erstellung können Profile über Richtlinien verwaltet und priorisiert werden.</p> <p>Tipps:</p> <ul style="list-style-type: none"> ■ Nutzen Sie vorhandene Profile als Vorlage. Sie können die vorhandenen Profile als neue Profile speichern und daraufhin u.a. die Meldungen an Ihre Bedürfnisse anpassen, weitere Bedingungen einrichten, Konformitätszustände ändern, Korrekturmaßnahmen aktivieren. Oder ziehen Sie die Profile einfach nur als Vorlage für die Erstellung eigener Profile heran. ■ Mit den vorhandenen Patch Manager-Profilen können Sie die Konformität mit Sicherheitsrichtlinien sowohl auf verwalteten als auch auf nicht verwalteten Endpoints durchsetzen. Weitere Informationen finden Sie unter Einsatz vorhandener Patch Manager-Profile (Seite 28).
Richtlinien	
Ändern der Richtlinien.	Anhand von Policies (Richtlinien) wird, basierend auf den Profilbewertungen am Endpoint, der gesamte Zugriff auf das Unternehmensnetzwerk kontrolliert. Über Richtlinien wird die Konfiguration verwaltet, in der Konformitätszustand, angezeigte Meldungen sowie durchgeführte Korrektur- und Durchsetzungsmaßnahmen eines Endpoints festgehalten sind.

Bereich und Aktion	Beschreibung
	<p>Tipps:</p> <ul style="list-style-type: none"> ■ Einer Richtlinie können beliebig viele Profile zugewiesen werden. ■ Es muss jedoch mindestens ein Betriebssystemprofil enthalten sein. ■ Richtlinien müssen für jedes auf einem Endpoint zu bewertende Betriebssystem das entsprechende Betriebssystemprofil enthalten. ■ Mit den vorhandenen Richtlinien können Sie die Konformität mit Sicherheitsrichtlinien sowohl auf verwalteten als auch auf nicht verwalteten Endpoints durchsetzen. Weitere Informationen finden Sie unter Vorhandene Richtlinien (Seite 15).

2.1 Praxistipps: Richtlinien

Dieser Abschnitt enthält Praxistipps zu Richtlinien.

Auswahl des passenden Richtlinienmodus

Wichtig: Sie müssen sicherstellen, dass der Richtlinie die richtigen Access Templates für die Modi „Report Only“ und „Remediate“ zugeordnet sind. Wenn Sie eine Enforcer Access Template verwenden, die den Netzwerkzugriff im Modus „Report Only“ oder „Remediate“ verhindert, wird allen Endpoints ungeachtet ihres Konformitätszustands der Zugriff verweigert. Um einen Konformitätszustand durchzusetzen, müssen Sie den Richtlinienmodus auf „Enforce“ setzen.

Typ	Beschreibung
Verwenden Sie zur Konformitätsprüfung von Unternehmen den Modus „Report Only“.	Der Modus „Report Only“ bietet die Möglichkeit zur Berichterstellung (auch Reporting genannt) über den Konformitätszustand Ihres Unternehmens. Dieser Modus fordert dem Benutzer am wenigsten Aufmerksamkeit ab.
Verwenden Sie zum Reporting und zur Anpassung von Endpoints an die geltenden Richtlinien den Modus „Remediate“.	Der Modus „Remediate“ bietet Unternehmen die Möglichkeit zur Erstellung von Endpoint-Reports und zur Korrektur der Endpoints, falls sie von den geltenden Richtlinien abweichen. Auf diese Weise kann Richtlinienkonformität noch vor der Durchsetzung von Maßnahmen erreicht werden.
Verwenden Sie zum Reporting, zur Korrektur und zur Durchsetzung von Netzwerkkonformität den Modus „Enforce“. Wenn bestimmte Endpoints nicht mit der Richtlinie übereinstimmen, wird ihnen der Netzwerkzugriff verweigert.	Der Modus „Enforce“ bietet Unternehmen die Möglichkeit zum Reporting, zur Korrektur und zur Durchsetzung von Netzwerkkonformität. Die in der Richtlinie ausgewählten (Agent und/oder DHCP) Access Templates bestimmen den Netzwerkzugriff. Wenn mehr als eine Access Template auf einen Zustand (Access State) zutrifft, wird die erstbeste Template gewählt.

Quarantine Override nur, wenn Netzwerkzugriff erforderlich ist

Tipp	Beschreibung
Setzen Sie die Option „Quarantine Override“ nur dann auf true , wenn der Netzwerkzugriff für das Unternehmen unerlässlich und das Sicherheitsrisiko vernachlässigbar ist.	Wenn Sie die Quarantäne über diese Option außer Kraft setzen, kann der Quarantänezustand eines Endpoints selbst dann aufgehoben werden, wenn er nicht konform ist.

Ausstatten von Richtlinien nur mit erforderlichen Profilen

Tipp	Beschreibung
Statten Sie Richtlinien nur mit den erforderlichen Profilen aus. Entfernen Sie überholte Profile aus Richtlinien.	Zur übersichtlicheren Verwaltung und Pflege Ihrer Richtlinien sollten Sie nur die absolut notwendigen Profile zu Viren- und Spywareschutz, persönlicher Firewall und Betriebssystemen in den Richtlinien behalten.

Erstellen und Priorisieren von Profilen in Richtlinien

Tipp	Beschreibung
Betriebssystemprofile sollten einer Richtlinie vor dem Priorisieren zugewiesen werden.	<p>Richtlinien müssen für jedes zu bewertende Betriebssystem das entsprechende Betriebssystemprofil enthalten. Weisen Sie dem wichtigsten Betriebssystem die höchste Priorität zu.</p> <p>Wenn ein bestimmtes Betriebssystem nicht auf dem Endpoint installiert ist, wird das Betriebssystemprofil der höchsten Priorität zur Ermittlung des Konformitätszustands und der erforderlichen Maßnahmen verwendet. Daraufhin werden keine weiteren Profile für diese Richtlinie analysiert.</p> <p>Beispiel: Wenn Windows XP und Windows 2000 als erforderliche Betriebssysteme definiert wurden und Windows XP als bevorzugtes Betriebssystem gilt, weisen Sie der Richtlinie beide Betriebssystemprofile zu, priorisieren Sie Windows XP und stellen Sie sicher, dass die ELSE-Bedingung im Windows-XP-Profil auf „Non-Compliant“ gesetzt ist und dass in ihr eine Meldung für Benutzer nicht konformer Endpoints vorgesehen ist. Wenn in diesem Umfeld auf einem Endpoint kein erforderliches Betriebssystem installiert ist, so gilt der Endpoint als nicht konform und es wird eine entsprechende Meldung auf diesem Endpoint angezeigt. Keine weiteren Profile in der Richtlinie werden analysiert.</p>

Tipp	Beschreibung
Weisen Sie einer Richtlinie die passenden Anwendungsprofile zu und legen Sie eine Priorität fest.	Wenn Ihre Richtlinie z.B. mehr als ein Virenschutzprofil enthält, weisen Sie dem wichtigsten Virenschutzprogramm die höchste Priorität zu.

Überprüfen der zugewiesenen Access Templates

Tipp	Beschreibung
Entfernen Sie überholte und nicht verwendete Access Templates aus Richtlinien.	Richtlinien sollten nur Access Templates für verwendete Enforcement-Methoden enthalten. Auf diese Weise lassen sich Netzwerkzugriffsprobleme ungeachtet des Richtlinienmodus einfacher beheben.
Überprüfen Sie, ob der Richtlinie die korrekten Access Templates zugewiesen wurden.	<p>Standardmäßig enthält jede Richtlinie bereits einige Access Templates. Stellen Sie sicher, dass jedem Access State die richtigen Access Templates zugeordnet wurden.</p> <p>Sie müssen die Access Templates Ihren Anforderungen gemäß priorisieren oder löschen. Wenn mehr als eine Access Template auf einen Access State zutrifft, wird die erstbeste Template gewählt.</p> <p>Wichtig:</p> <ul style="list-style-type: none"> ■ Wenn Sie eine Enforcer Access Template verwenden, die den Netzwerkzugriff im Modus „Report Only“ oder „Remediate“ verhindert, wird allen Endpoints ungeachtet ihres Konformitätszustands der Zugriff verweigert. Um einen Konformitätszustand durchzusetzen, müssen Sie den Richtlinienmodus auf „Enforce“ setzen. ■ Wenn Sie aus einem Access State alle Agent Enforcer Access Templates entfernen, lassen Sie jeglichen ausgehenden Datenverkehr für diesen Access State zu.

2.2 Vorhandene Richtlinien

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

Bei der Konformitätsbewertung des Endpoints ruft der Agent die Richtlinie ab, die für die Gruppe des Endpoints in Sophos Enterprise Console gilt. Weitere Informationen finden Sie unter [Aktualisieren von Richtlinien](#) (Seite 16).

- **Default:** Diese Standardrichtlinie wird Endpoints zugewiesen, auf denen der Sophos 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 ist für Endpoints vorgesehen, auf denen Sophos Enterprise Console installiert ist und die von Sophos Compliance Agent verwaltet werden. 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 Agent installiert ist und der Dissolvable Agent nicht verwendet wird, so wird der Netzwerkzugriff über die Enforcer-Einstellungen geregelt. Weitere Informationen finden Sie unter [Festlegen von Enforcer-Einstellungen](#) (Seite 81).

2.3 Aktualisieren von Richtlinien

Anhand von Richtlinien wird, basierend auf den Profilbewertungen am Endpoint, der gesamte Zugriff auf das Unternehmensnetzwerk kontrolliert. Über Richtlinien wird die Konfiguration verwaltet, in der Konformitätszustand, angezeigte Meldungen sowie durchgeführte Korrektur- und Durchsetzungsmaßnahmen eines Endpoints festgehalten sind.

Wichtig: Alle Richtlinien und Richtlinienänderungen haben im Netzwerk sofortige Gültigkeit, aber die Richtlinie wird erst dann auf den Endpoint übertragen, wenn der Agent sie abruft.

Vorgehensweise

1. Klicken Sie auf **Manage > Policies**. Klicken Sie dann auf die Richtlinie, die Sie aktualisieren möchten. Weitere Informationen zu definierten Richtlinien finden Sie unter [Vorhandene Richtlinien](#) (Seite 15).
2. Klicken Sie auf das Listenfeld **Policy Mode**, um den Richtlinienmodus auszuwählen. Der Richtlinienmodus bestimmt die bei der Konformitätsprüfung zu verwendenden Access Templates. Es gibt drei Richtlinienmodi: „Report Only“, „Remediate“ und „Enforce“. Weitere Informationen finden Sie unter [Glossar](#) (Seite 93).
3. Klicken Sie links im Agenten auf **Settings**.
4. Legen Sie ggf. die Continuous Agent-Einstellungen fest. Diese Einstellungen gelten nur für Endpoints, auf denen der Quarantine Agent läuft:
 - **Policy Refresh Interval:** Hier legen Sie fest, wie häufig der Agent die Richtlinie abruft. Die Vorgabe lautet 4 Stunden.
 - **Assess and Enforce Interval:** Hier legen Sie fest, wie häufig der Agent die Konformität des Endpoints überprüft. Die Vorgabe lautet vier Stunden.
 - **Report Interval:** Hier legen Sie fest, wie häufig der Agent Report-Daten an den Server sendet. Die Vorgabe lautet acht Stunden.

5. Wählen Sie ggf. die Agent Configuration Template in den Configuration Settings.

Wenn keine Configuration Template ausgewählt wird, verwendet der Agent die Voreinstellungen. Diese Einstellungen gelten nur für Endpoints, auf denen der Quarantine Agent läuft: Mehr dazu erfahren Sie unter [Erstellen von Agent Configuration Templates](#) (Seite 20) und [Anzeigen der Agenten-Einstellungen](#) (Seite 20).

6. Legen Sie ggf. die Quarantine Agent-Einstellungen fest. Diese Einstellungen gelten nur für Endpoints, auf denen der Quarantine Agent läuft:

- **Quarantine Override:** Hier legen Sie fest, ob die Quarantäne eines Endpoints außer Kraft gesetzt werden kann. Wenn „Quarantine Override“ auf „True“ eingestellt ist, darf der Benutzer die Agentenquarantäne außer Kraft setzen. Diese Option ermöglicht das Entfernen von Endpoints aus der Quarantäne, selbst wenn sie nicht konform sind. Wenn der Wert auf „False“ gesetzt ist, kann die Agenten Quarantäne nicht außer Kraft gesetzt werden und der Endpoint bleibt so lange in Quarantäne, bis Richtlinienkonformität gegeben ist.

7. Legen Sie ggf. die DHCP Agent Settings fest. Diese Einstellungen gelten nur für DHCP Enforcement:

- **Agent Enforcement Action:** Hiermit bestimmen Sie die Abrufmethode neuer IP-Adressen für den Endpoint. Sobald der Agent gestartet wird, erstellt er neue IP-Adressen. Wenn sich der Konformitätszustand des Endpoints 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:

- **None:** IP-Adressen für den Endpoint werden weder freigegeben noch verlängert. Wählen Sie **None**, wenn Sie DHCP Enforcement **nicht** durchführen.

- **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 derzeitig verwendeten IP-Adressen gestrichen. Sie **müssen** die Option **Release Renew** für DHCP Enforcement wählen.

Hinweis: Wenn auf einem Endpoint der Dissolvable Agent unter Windows Vista oder Windows 7 ausgeführt wird und neue IP-Adressen freigegeben und/oder verlängert werden müssen, fordert der Agent den Benutzer entweder zur Anmeldung als Administrator oder zu einem Neustart des Endpoints auf.

8. Führen Sie einen der folgenden Schritte aus:

- Klicken Sie im linken unteren Seitenbereich auf **Add Profiles**, um der Richtlinie weitere Profiltypen zuzuweisen. Klicken Sie zur Auswahl des Profiltyps auf das Listenfeld **Profile Type** und markieren Sie jeweils das Kontrollkästchen neben den Profilen, die der Richtlinie zugewiesen werden sollen. Klicken Sie anschließend auf **OK**. Wiederholen Sie diese Schritte bei Bedarf, um der Richtlinie weitere Profile zuzuweisen.

Wichtig: Einer Richtlinie können beliebig viele Profile zugewiesen werden. Es muss jedoch mindestens ein Betriebssystemprofil enthalten sein. Richtlinien müssen für jedes auf einem Endpoint zu bewertende Betriebssystem das entsprechende Betriebssystemprofil enthalten.

- Klicken Sie zum Entfernen von Profilen aus der Richtlinie Sie im Profil-Bereich (links) auf den entsprechenden Profiltyp und dann auf das **Mülleimersymbol** neben den zu entfernenden Profilen.
9. Wenn Sie mehrere Betriebssysteme oder Anwendungsprofile nutzen, können Sie mit den Pfeiltasten die Priorität der Profile aller Typen für die Bewertung festlegen.
Es gibt drei Arten von Richtlinienverhalten: „Required“, „Best“ und „All“. Weitere Informationen finden Sie unter [Glossar](#) (Seite 93).
 10. Klicken Sie im Netzwerkzugriffsbereich (links) auf den Enforcer-Typ, für den die Access Templates überprüft oder geändert werden sollen. Wenn Sie Access Templates für einen bestimmten Access State hinzufügen möchten, klicken Sie auf die entsprechende Richtlinie, wählen Sie **Select**, aktivieren Sie die Kontrollkästchen neben den Access Templates und Access States, für die die Vorlagen zutreffen, und klicken Sie auf **OK**. Sie können auch die aktuellen Access Templates beibehalten oder löschen.
Je nach Ihrer Netzwerkconfiguration müssen Sie mehr als einen Enforcer-Typ festlegen. Weitere Informationen zu regulären Ausdrücken finden Sie unter [Anzeigen von Richtlinienmodi und Access States](#) (Seite 18).
Hinweis: Je nach den in NAC Manager vorhandenen Access Templates und deren Konformitätszuständen wird jede Richtlinie in der Regel automatisch mit Access Templates für alle Access States ausgestattet. Stellen Sie sicher, dass jedem Access State die richtigen Access Templates zugeordnet wurden. Sie können außerdem die Einstellungen der vorhandenen Access Templates ändern oder völlig neue Access Templates erstellen und sie anstelle der vorhandenen Access Templates in die Profile aufnehmen. Wenn Sie aus einem Zugriffszustand alle Agent Enforcer Access Templates entfernen, lassen Sie jeglichen ausgehenden Verkehr für diesen Zustand zu. Mehr dazu erfahren Sie unter [Erstellen von Agent Enforcer Access Templates](#) (Seite 48) und [Erstellen von DHCP Enforcer Access Templates](#) (Seite 49).
 11. 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.
 12. Klicken Sie auf **Save**.

2.4 Anzeigen von Richtlinienmodi und Access States

In der folgenden Tabelle werden die Access States aller Richtlinienmodi nach Enforcer-Typ sortiert aufgelistet und erläutert.

Weitere Informationen finden Sie unter [Aktualisieren von Richtlinien](#) (Seite 16).

Richtlinienmodus	Beschreibung und Access States
Report Only	Endpoints werden anhand der zugewiesenen Richtlinie auf Konformität überprüft. Die Ergebnisse von NAC Manager werden in einem Report festgehalten. Es werden keine Meldungen angezeigt oder Korrektur- und

Richtlinienmodus	Beschreibung und Access States
	<p>Durchsetzungsmaßnahmen durchgeführt. Wählen Sie eine Enforcer Access Template, die Datenverkehr vom Endpoint zulässt.</p> <p>Wichtig: Wenn Sie eine Enforcer Access Template verwenden, die den Netzwerkzugriff im Modus „Report Only“ oder „Remediate“ verhindert, wird allen Endpoints ungeachtet ihres Konformitätszustands der Zugriff verweigert. Zum Durchsetzen eines Konformitätszustands müssen Sie den Richtlinienmodus auf „Enforce“ setzen.</p>
Remediate	<p>Endpoints werden anhand der zugewiesenen Richtlinie auf Konformität überprüft. Die Ergebnisse von NAC Manager werden in einem Report festgehalten. Es werden Meldungen angezeigt und Korrekturmaßnahmen durchgeführt. Es werden jedoch keine Durchsetzungsmaßnahmen durchgeführt. Wählen Sie eine Enforcer Access Template, die Datenverkehr vom Endpoint zulässt.</p> <p>Wichtig: Wenn Sie eine Enforcer Access Template verwenden, die den Netzwerkzugriff im Modus „Report Only“ oder „Remediate“ verhindert, wird allen Endpoints ungeachtet ihres Konformitätszustands der Zugriff verweigert. Zum Durchsetzen eines Konformitätszustands müssen Sie den Richtlinienmodus auf „Enforce“ setzen.</p>
Enforcement	<p>Endpoints werden anhand der zugewiesenen Richtlinie auf Konformität überprüft. Die Ergebnisse von NAC Manager werden in einem Report festgehalten. Es werden Meldungen angezeigt und Korrektur- und Durchsetzungsmaßnahmen anhand der für den entsprechenden Access State zutreffenden Access Templates durchgeführt. Wenn der Endpoint einen in der zugewiesenen Richtlinie festgelegten Access States aufweist, wird der Netzwerkzugriff von den entsprechenden Access Templates geregelt.</p> <p>Mögliche Zustände des Agenten:</p> <ul style="list-style-type: none"> ■ No Agent Tray: Der Agent läuft nicht auf dem Endpoint. Dieser Zustand kann von Agent Enforcer gemeldet werden, wenn der Benutzer nicht an Windows angemeldet ist oder das Programm „Agent Tray“ nicht mehr läuft. ■ User Override: Der Benutzer hat die Quarantäne des Agenten auf dem Endpoint außer Kraft gesetzt. ■ Policy Retrieval Error: Eine bestimmte Richtlinie konnte nicht für den Endpoint abgerufen werden. Dieser Zustand kann vorliegen, wenn der Agent eine Richtlinie nicht vom NAC-Server herunterladen kann oder der Konformitätszustand des Endpoints gemäß dem Feld Agent Policy Update Threshold (unter Configure System > Enforcer Settings) abgelaufen ist. <p>Enforcer State:</p> <ul style="list-style-type: none"> ■ Policy Retrieval Error: Gemäß dem Feld Update Threshold der DHCP Richtlinie (siehe Configure System > Enforcer Settings) ist der Konformitätszustand nicht mehr aktuell.

Richtlinienmodus	Beschreibung und Access States
	<p>Mögliche Konformitätszustände:</p> <ul style="list-style-type: none"> ■ Compliant: Die Konformitätsprüfung hat den Endpoint für richtlinienkonform befunden. ■ Partially Compliant: Die Konformitätsprüfung hat den Endpoint für teilweise richtlinienkonform befunden. ■ Non-Compliant: Die Konformitätsprüfung hat den Endpoint für nicht richtlinienkonform befunden.

2.5 Erstellen von Agent Configuration Templates

Agent Configuration Templates enthalten optionale Einstellungen für Administratoren zur Funktionsweise des Agenten auf Endpoints. Agent Configuration Templates gelten nur für Endpoints, auf denen der Quarantine Agent läuft.

Nach der Einrichtung von Agent Configuration Templates können Sie sie Richtlinien zuweisen. Daraufhin können Agenten die zugewiesene Richtlinie bei der nächsten Bewertung abfragen und die Einstellungen auf dem Endpoint durchsetzen. Weitere Informationen finden Sie unter [Aktualisieren von Richtlinien](#) (Seite 16).

Vorgehensweise

1. Öffnen Sie **Manage > Agent Configuration Templates**. Klicken Sie links unten auf der Seite auf **Create Agent Configuration Template**.
2. Geben Sie einen Namen und eine Beschreibung für die Agent Configuration Template ein.
3. Klicken Sie nun auf **Select**, markieren Sie die Kontrollkästchen neben den Agenten-Einstellungen, die der Agent Configuration Template hinzugefügt werden sollen, klicken Sie auf **OK** und geben Sie die Werte an, wo zutreffend.

Die Agenten-Einstellungen definieren die Funktionen für die Ausführung des Agenten auf dem Endpoint. Weitere Informationen zu den Agenten-Einstellungen und verfügbaren Werten finden Sie unter [Anzeigen der Agenten-Einstellungen](#) (Seite 20).

4. Klicken Sie auf **Save**.

Hinweis: Wenn die Agent Configuration Template erstellt ist, können Sie über ein Rechtsklickmenü auf der **Agent Configuration Template**-Listenseite oder beim Bearbeiten der Vorlage durch Klicken auf den Link **View Usage Details** die Richtlinien anzeigen, die auf dieser Vorlage basieren.

2.6 Anzeigen der Agenten-Einstellungen

In der folgenden Tabelle werden die Agenten-Einstellungen beschrieben.

Weitere Informationen zum Erstellen von Agent Configuration Templates finden Sie unter [Erstellen von Agent Configuration Templates](#) (Seite 20).

Einstellung	Beschreibung und mögliche Werte	Vorgabe
Log Lifetime	<p>Hier wird die Aufbewahrungsdauer von Agenten-Protokollen auf dem Endpoint in Stunden festgelegt. Nach Ablauf der Aufbewahrungsdauer wird der Protokollinhalt gelöscht, sodass die Protokolle wieder leer sind. Beim Start eines Agenten werden alle Protokolle gelöscht, deren Datum den festgelegten Wert überschritten hat.</p> <p>Hinweis: Protokollierung beeinträchtigt die Leistung. Aus diesem Grund empfiehlt es sich, die Protokollierung nur zur Fehlersuche zu aktivieren und danach wieder zu deaktivieren. Die Protokolldateien für Windows 2000 und Windows XP befinden sich im Verzeichnis <Laufwerk>:\Dokumente und Einstellungen\Alle Benutzer\Anwendungsdaten\Sophos Compliance Agent\Logs. Die Protokolldateien für Windows Vista und Windows 7 befinden sich im Verzeichnis <Laufwerk>:\Programmdateien\Sophos\Sophos Compliance Agent\Logs.</p>	24
Logging	<p>Diese Einstellung legt die Protokollierungsstufe des Agenten fest. Es sind folgende Werte möglich:</p> <ul style="list-style-type: none"> ■ Log Error and Warning: Fehler- und Warnmeldungen. ■ Log All Messages: Fehler- und Warnmeldungen sowie Informationen. ■ Log All Messages and Brief Trace: Fehler- und Warnmeldungen, Informationen und kurze Ablaufverfolgungsmeldungen. <p>Hinweis: Protokollierung beeinträchtigt die Leistung. Aus diesem Grund empfiehlt es sich, die Protokollierung nur zur Fehlersuche zu aktivieren und danach wieder zu deaktivieren. Die Protokolldateien für Windows 2000 und Windows XP befinden sich im Verzeichnis <Laufwerk>:\Dokumente und Einstellungen\Alle Benutzer\Anwendungsdaten\Sophos Compliance Agent\Logs. Die Protokolldateien für Windows Vista und Windows 7 befinden sich im Verzeichnis <Laufwerk>:\Programmdateien\Sophos\Sophos Compliance Agent\Logs.</p>	Log Error and Warning
Max Attempts	<p>Hier lässt sich die maximale Anzahl der vom Agenten unternommenen Verbindungsversuche mit dem NAC-Server für einen bestimmten Vorgang (d.h. Richtlinie abrufen und bewerten/durchsetzen/korrigieren, Bericht erstellen) festlegen. Der Agent versucht beim ersten Aufruf und bei jeder planmäßigen Konformitätsprüfung, die Verbindung erneut herzustellen – dies geschieht nicht bei Konformitätsprüfungen, die vom Benutzer eingeleitet werden.</p>	10
Retry Delay	<p>Hier wird die Zeit in Sekunden festgelegt, die der Agent wartet, bis er eine weitere Verbindungsaufnahme zum NAC-Server versucht. Der Agent versucht beim ersten Aufruf und bei jeder planmäßigen Konformitätsprüfung, die Verbindung erneut herzustellen – dies geschieht nicht bei Konformitätsprüfungen, die vom Benutzer eingeleitet werden.</p>	15
Save Proxy Password	<p>Das Proxy-Kennwort, das für künftige Proxy-Authentifizierungs-Anfragen verwendet werden soll, wird gespeichert. Mögliche Werte sind Do Not Save und Save.</p>	Save

Einstellung	Beschreibung und mögliche Werte	Vorgabe
Save Proxy Username	Der Proxy-Benutzername, der für künftige Proxy-Authentifizierungs-Anfragen verwendet werden soll, wird gespeichert. Mögliche Werte sind Do Not Save und Save .	Save
Show Errors In Results	Hier legen Sie fest, ob Fehlermeldungen im Dialogfeld Results angezeigt oder ausgeblendet werden sollen. Mögliche Werte sind Show und Hide . Wenn Sie Show wählen, werden Fehlermeldungen im Dialogfeld Results angezeigt und in der Datei „errors.htm“ auf dem Endpoint gespeichert. Wenn Sie Hide wählen, werden Fehlermeldungen lediglich in der Datei „errors.htm“ gespeichert. Die Datei für Windows 2000 und Windows XP befindet sich im Verzeichnis <Laufwerk>:\Dokumente und Einstellungen\Alle Benutzer\Anwendungsdaten\Sophos Compliance Agent\Data. Die Datei für Windows Vista und Windows 7 befindet sich im Verzeichnis <Laufwerk>:\Programmdaten\Sophos\Sophos Compliance Agent\Data.	Show
Show Exit	Diese Einstellung bestimmt, ob die Menüoption Exit angezeigt oder ausgeblendet werden soll. Mögliche Werte sind Show und Hide .	Hide
Show Extended Errors	Hier legen Sie fest, ob die im Zusammenhang mit Verbindungsproblemen des NAC-Server entstehenden ausführlichen Fehlermeldungen im Dialogfeld Results angezeigt oder ausgeblendet werden sollen. Mögliche Werte sind Show und Hide . Wenn Sie Show wählen, werden ausführliche Fehlermeldungen im Dialogfeld Results angezeigt und in der Datei „errors.htm“ auf dem Endpoint gespeichert. Die Datei für Windows 2000 und Windows XP befindet sich im Verzeichnis <Laufwerk>:\Dokumente und Einstellungen\Alle Benutzer\Anwendungsdaten\Sophos Compliance Agent\Data. Die Datei für Windows Vista und Windows 7 befindet sich im Verzeichnis <Laufwerk>:\Programmdaten\Sophos\Sophos Compliance Agent\Data.	Show
Show Logging	Diese Einstellung legt fest, ob im Produktinfofeld das Kontrollkästchen Protokollierung aktivieren angezeigt wird. Mögliche Werte sind Show und Hide .	Show

2.7 Praxistipps: Profile

Dieser Abschnitt enthält Praxistipps zu Profilen.

Erstellen einsatzbereiter Profile über vorhandene Profile

Tip	Beschreibung
Nutzen Sie vorhandene Profile als Vorlage.	Einsatzbereiche: <ul style="list-style-type: none"> ■ Für Demonstrationen, Pilotprojekte oder Machbarkeitstests können Sie die vorhandenen Profile verwenden.

Tipp	Beschreibung
	<ul style="list-style-type: none"> ■ Für die Einführung in die Arbeitsumgebung kopieren Sie die vorhandenen Profile (durch Anlegen einer Arbeitskopie) und passen die Meldungen an, fügen weitere Bedingungen hinzu, ändern die Maßnahmen usw. Oder nutzen Sie die Profile einfach bei der Erstellung neuer Profile als Vorlage.

Auswahl weiterer Fähigkeiten für Profile

Bei den Fähigkeiten handelt es sich um die Funktionen einer Anwendung, die auf Konformität überprüft werden können. Sophos NAC stellt zunächst anhand einer „Installed“-Fähigkeit sicher, dass ein Betriebssystem oder eine Anwendung installiert ist. Sobald die Installation einer Anwendung von der Software bestätigt wurde, werden weitere Fähigkeiten auf dem Endpoint überprüft.

Hinweis: Die verfügbaren Anwendungsfähigkeiten hängen vom Softwaredesign der Anwendung ab. Einige Fähigkeiten stehen für bestimmte Betriebssysteme, auf denen die Anwendung unterstützt wird, oder für alle Versionen einer Anwendung, nicht zur Verfügung. Nicht verfügbare Fähigkeiten werden nicht angezeigt. Wenn eine Fähigkeit nur auf bestimmten Betriebssystemen verfügbar ist, werden nur diese Betriebssysteme angezeigt.

Tipp	Beschreibung
Wählen Sie weitere Fähigkeiten aus, mit denen die Anwendung getestet werden kann, um sicherzustellen, dass der Endpoint adäquat geschützt ist.	Wenn eine Anwendung installiert ist, heißt dies nicht unbedingt, dass sie den Endpoint aktiv schützt. Es empfiehlt sich, den Endpoint auf weitere Fähigkeiten, wie „Last Scan Grace Period“ und „Signature Grace Period“, zu untersuchen, um optimalen Schutz zu gewährleisten.
Verwenden Sie Fähigkeiten, die Ihre Unternehmenssicherheitsrichtlinien unterstützen.	Zum Beispiel könnte in Ihrem Unternehmen eine Richtlinie in Kraft sein, die einmal pro Woche für eine Virenschutzanwendung eine Systemüberprüfung erfordert. Oder es ist eine Sicherheitsrichtlinie in Kraft, die eine Echtzeitüberprüfung als ausreichenden Schutz betrachtet. In ersterem Fall empfiehlt sich die Aufnahme einer „Scan“-Fähigkeit in das Profil, in letzterem Fall nicht .
Verwenden Sie die Fähigkeiten „Grace Period“ („Last Scan Grace Period“ und „Signature Grace Period“) und „Date“ („Last Scan Date“ und „Signature Date“).	Wenn Sie über „Grace Period“ das Profil einrichten, brauchen Sie sich nicht mehr damit beschäftigen – minimaler Wartungsaufwand. Die Fähigkeiten „Grace Period“ und „Date“ sollten nicht gleichzeitig eingesetzt werden, es sei denn, die Bedingungen wurden vorher gründlich getestet. Das Ergebnis ist unvorhersehbar.

Tipp	Beschreibung
Für die sicherste Endpoint-Analyse verwenden Sie alle verfügbaren Fähigkeiten.	Verwenden Sie möglichst alle verfügbaren Fähigkeiten (mit Ausnahme von „Grace Period“ und „Date“), um die sicherste Endpoint-Prüfung zu erzielen. Schließen Sie Fähigkeiten nur aus dem Profil aus, wenn sie sich negativ auf die Sophos NAC-Installation oder Ihre Geschäftsabläufe auswirken.

Festlegen von Bedingungen und Konformitätszuständen

Tipp	Beschreibung
Wenn Netzwerkzugriff erwünscht ist, weisen Sie Bedingungen Konformitätszustände zu.	<ul style="list-style-type: none"> ■ Verwenden Sie „compliant“, um Netzwerkzugriff zu erlauben. ■ Mit „partially compliant“ schränken Sie den Netzwerkzugriff ein oder aktivieren die Quarantänefunktion. Oder Sie gewähren vollen Netzwerkzugriff und senden gleichzeitig Meldungen an die teilkonformen Endpoints und führen Korrekturmaßnahmen durch. ■ Anhand von „non-compliant“ kann der Netzwerkzugriff verweigert oder eingeschränkt werden, Meldungen können ausgegeben und Korrekturmaßnahmen ergriffen werden. <p>Der Konformitätszustand des Endpoints wird über die in der Richtlinie festgelegten Profile ermittelt. Der geringste Konformitätszustand bestimmt den gesamten Konformitätszustand. Wenn Sophos NAC beispielsweise feststellt, dass ein Endpoint mit dem Virenschutzprofil konform ist, jedoch nicht mit dem Firewall-Profil, wird der Gesamtzustand für nicht-konform befunden.</p>
Fügen Sie eine neue Bedingung hinzu, um mehr als einen Wert zu testen, einen anderen Konformitätszustand zu setzen oder basierend auf dem Konformitätszustand eine andere Meldung/Korrekturmaßnahme festzulegen.	Zum Beispiel können Sie über die Fähigkeit „Grace Period“ bestimmen, dass einem Endpoint, dessen Signaturdatei seit 5 Tagen veraltet ist, erst dann der Netzwerkzugriff verweigert wird, wenn die Signaturdatei seit 10 Tagen veraltet ist. Fügen Sie in diesem Fall eine neue Bedingung hinzu: Wenn der Endpoint innerhalb von 5 Tagen konform ist, soll eine Warnmeldung angezeigt und Netzwerkzugriff gewährt werden. Fügen Sie eine weitere Bedingung für folgenden Fall hinzu: Wenn der Endpoint innerhalb von 10 Tagen teilweise konform ist, soll eine Warnmeldung angezeigt und Netzwerkzugriff gewährt werden. Wenn die Signaturdatei des Endpoints mehr als 10 Tage veraltet ist, wird eine Warnmeldung angezeigt und Netzwerkzugriff verweigert.

Tipp	Beschreibung
<p>Bringen Sie mehrere Bedingungen in die Reihenfolge, in der sie bewertet werden sollen.</p>	<p>Wenn eine Bedingung erfüllt ist, werden der zugehörige Konformitätszustand, die zugehörige Meldung und die zugehörige Korrekturmaßnahme verwendet, und keine weiteren Bedingungen für diese Fähigkeit werden analysiert.</p> <p>Eine teilkonforme Bedingung, die Sie über eine nicht-konforme Bedingung einordnen, wird zuerst analysiert, und nur nicht-konformen Endpoints wird der Netzwerkzugriff verweigert.</p>
<p>Stellen Sie sicher, dass die Konformitätszustände, Meldungen und Korrekturmaßnahmen zur ausgewählten Bedingung passen.</p>	<p>In Fähigkeiten werden Bedingungen und Konformitätszustände in einer Standardreihenfolge angezeigt. Wenn Sie eine Bedingung ändern, stellen Sie sicher, dass die Konformitätsbedingungen zur Bedingung passen, die analysiert werden soll. Außerdem möchten Sie den jeweiligen Endpoints beim Ändern der Reihenfolge von Bedingungen und Konformitätszuständen womöglich andere Meldungen und Korrekturmaßnahmen zuweisen.</p> <p>Zum Beispiel kann die Standardreihenfolge bewirken, dass ein Endpoint als konform („compliant“) gilt, wenn eine Firewall aktiviert ist, und als nicht-konform („non-compliant“) gilt, wenn dies nicht der Fall ist. Wenn Sie die Bedingung durch „Not Enabled“ deaktivieren, sollten Sie auch die entsprechenden Konformitätszustände so ändern, dass der Endpoint im Fall einer deaktivierten Firewall als „Non-Compliant“ eingestuft wird. Als ELSE-Bedingung (d.h. die Firewall ist „Enabled“) sollte der Endpoint auf „Compliant“ gesetzt werden.</p>
<p>Machen Sie Gebrauch von Bedingungen und Konformitätszuständen, die Ihre Sicherheitsrichtlinien komplementieren.</p>	<p>Zum Beispiel könnte in Ihrem Unternehmen eine Sicherheitsrichtlinie in Kraft sein, die einen Endpoint als nicht konform einstuft, wenn Echtzeitschutz deaktiviert ist; oder es ist eine Sicherheitsrichtlinie in Kraft, die einen Endpoint bei deaktiviertem Echtzeitschutz als teilkonform einstuft. In ersterem Fall würden Sie sicherstellen, dass der Endpoint als nicht-konform („non-compliant“) eingestuft und der Netzwerkzugriff verweigert wird. In letzterem Fall würden Sie sich auf die Korrektur des teilkonformen Endpoints konzentrieren, ohne den Netzwerkzugriff einzuschränken oder zu verweigern.</p>
<p>Bei Versionsfähigkeiten stellen Sie sicher, dass die Versionsnummer die richtige Anzahl an Kennwerten aufweist.</p>	<p>Wenn Sie beispielsweise eine Bedingung mit == 8 anlegen und auf dem Endpoint Version 8.1 installiert wurde, vergleicht die Software Version 8.1 mit dem in der Bedingung festgelegten Kennwert (nämlich 8). Die Bedingung ist somit erfüllt. Wenn Sie jedoch eine Bedingung mit == 8.0 anlegen und die auf dem Endpoint installierte Version lautet 8.1, vergleicht die Software Version 8.1 mit den beiden</p>

Tipp	Beschreibung
	Kennwerten (nämlich 8 und 0) in der Bedingung. In diesem Fall ist die Bedingung nicht erfüllt.
Bei Virenschutz- und Spywareschutzanwendungen testen Sie die Verwendung des Operators == (gleich) in den Datumsfähigkeiten.	Wenn Sie für eine Viren- oder Spywareschutzanwendung ein Profil definieren und eine Datumsfähigkeit („Last Scan Date“ und „Signature Date“) mit dem Operator == (gleich) angeben, muss das Datum vom Endpoint im Format MM/TT/JJJJ zurückgegeben werden. Wenn die Anwendung das Datum im Format MM/TT/JJJJ HH:MM:SS zurückgibt, kann die Erkennung fehlschlagen, auch wenn das Datum am Endpoint mit dem in der Bedingung angegebenen Wert identisch ist. Um dieses Problem zu vermeiden, verwenden Sie bei der Definition von Daten den Operator >= (größer gleich) oder <= (kleiner gleich) anstelle von == (gleich). Testen Sie eine Richtlinie, bevor Sie sie installieren, um sicherzustellen, dass die Erkennung durch Verwendung des Operators == nicht fehlschlägt.

Erstellen von Meldungen

Eine Meldung wird nur dann angezeigt, wenn bestimmte Bedingungen erfüllt sind. Je nach Richtlinie können mehrere Meldungen angezeigt werden. Sie sollten Meldungen stets auf Richtigkeit, Informationsgehalt und Angemessenheit testen.

Wichtig: Bedenken Sie, dass auch unternehmensfremde Endpoints eine Verbindung zum Netzwerk herstellen können. Da auf diesen Endpoints andere oder inkompatible Sicherheitssoftware installiert sein kann, müssen die Meldungen in diesem Fall mit besonderer Sorgfalt formuliert werden. Die vorhandene Richtlinie „Unmanaged“ ist speziell für nicht verwaltete Endpoints konzipiert. Passen Sie diese Richtlinie sowie die entsprechenden Profile und Meldungen an, damit auch nicht verwaltete Endpoints adäquat abgedeckt werden.

Tipp	Beschreibung
Erstellen Sie Meldungen und unterdrücken Sie sie im Richtlinienmodus „Report Only“.	Erstellen Sie ein Profil mit Meldungen, die nahezu einsatzbereit sind. Meldungen lassen sich über den Richtlinienmodus „Report Only“ unterdrücken. Wenn Meldungen angezeigt und Korrekturmaßnahmen durchgeführt werden sollen, jedoch keine Konformität durchgesetzt werden soll, können Sie zum Modus „Remediate“ migrieren. Wenn auch Konformität durchgesetzt werden soll, migrieren Sie zum Modus „Enforce“. Weitere Informationen finden Sie unter Implementierung von Network Access Control (Seite 3).
Nutzen Sie Meldungen, um auf das Zutreffen bestimmter Bedingungen aufmerksam zu machen.	Erstellen Sie zum Beispiel eine Meldung, die anzeigt, dass die Antivirensignatur veraltet ist und dass Sophos NAC die Signatur sofort aktualisiert.

Tipp	Beschreibung
Verfassen Sie Meldungen zunächst in englischer Sprache und übersetzen Sie sie daraufhin nach Bedarf in andere Sprachen.	Der Agent wählt zur Ausgabe von Meldungen die am besten passende Sprache aus. Eine Meldung wird auf Englisch angezeigt, wenn keine Übersetzung in die Sprache des jeweiligen Betriebssystems vorhanden ist. Sollte keine englische Meldung vorhanden sein und die Meldung kann nicht in einer anderen Sprache angezeigt werden, wird ein leeres Meldungsfenster angezeigt. Meldungen werden in NAC Manager außerdem auf Englisch angezeigt. Wenn keine Meldung auf Englisch vorhanden ist, wird ein leeres Meldungsfenster angezeigt.

Korrekturmaßnahmen

Die verfügbaren Korrekturmaßnahmen hängen vom Softwaredesign der Anwendung ab. Einige Korrekturmaßnahmen stehen für bestimmte Betriebssysteme, auf denen die Anwendung unterstützt wird, oder für alle Versionen einer Anwendung, nicht zur Verfügung. Wenn eine Korrekturmaßnahme nur auf bestimmten Betriebssystemen unterstützt wird, werden die Betriebssysteme, auf denen die Maßnahme nicht zur Verfügung steht, entsprechend gekennzeichnet.

Tipp	Beschreibung
Wählen Sie Korrekturmaßnahmen und unterdrücken Sie sie im Richtlinienmodus „Report Only“.	Erstellen Sie ein Profil mit Korrekturmaßnahmen, die nahezu einsatzbereit sind. Korrekturmaßnahmen lassen sich über den Richtlinienmodus „Report Only“ unterdrücken. Wenn Meldungen angezeigt und Korrekturmaßnahmen durchgeführt werden sollen, jedoch keine Konformität durchgesetzt werden soll, können Sie zum Modus „Remediate“ migrieren. Wenn auch Konformität durchgesetzt werden soll, migrieren Sie zum Modus „Enforce“. Weitere Informationen finden Sie unter Implementierung von Network Access Control (Seite 3).
Erstellen Sie bei der Auswahl von Korrekturmaßnahmen eine Bedingung mit dem Access State „Partially Compliant“.	Wenn Sie nur Bedingungen mit den Zuständen „Compliant“ und „Non-Compliant“ erstellen, greifen die Korrekturmaßnahmen erst dann, wenn ein Endpoint nicht mehr konform ist. Weisen Sie einer Bedingung jedoch den Zustand „Partially Compliant“ zu, können auf Endpoints Korrekturmaßnahmen durchgeführt werden, damit sie stets auf dem aktuellen Stand sind. Sie werden nur als „Non-Compliant“ eingestuft, wenn sie erheblich veraltet sind.
Verwenden Sie möglichst alle verfügbaren Korrekturmaßnahmen, um die sicherste Endpoint-Überprüfung zu erzielen.	Schließen Sie Korrekturmaßnahmen nur dann aus dem Profil aus, wenn sie Probleme verursachen.

Tipp	Beschreibung
Vermeiden Sie Korrekturmaßnahmen, wenn sie die Arbeit auf einem Endpoint gravierend beeinträchtigen.	<p>Wenn Sie Korrekturmaßnahmen vermeiden möchten, gibt es mehrere Möglichkeiten: a) Erstellen Sie separate Profile für bestimmte Benutzer, die keine Korrekturmaßnahmen enthalten. b) Deaktivieren Sie Korrekturmaßnahmen in vorhandenen Profilen vorübergehend. c) Setzen Sie den Richtlinienmodus der jeweiligen Endpoints auf „Report Only“.</p> <p>Sie sollten die negativen Auswirkungen von Korrekturmaßnahmen auf den Endpoints untersuchen und den Störungsgrad in jedem Fall abwägen.</p>

2.8 Erstellen von Profilen

In Profilen (Profiles) lassen sich Elemente festlegen, die auf dem Endpoint analysiert bzw. überprüft werden sollen, z.B. Betriebssysteme und Anwendungen. In Profilen werden Bedingungen, Konformitätszustände, Meldungen und Korrekturmaßnahmen definiert. Nach der Erstellung können Profile über Richtlinien verwaltet und priorisiert werden.

Sie können Profile für bestimmte Elemente einrichten und diesen (je nach Elementtyp) zugehörige Service-Packs oder Anwendungsfähigkeiten zuordnen. Sie können auch mehrere Profile für dasselbe Betriebssystem oder dieselbe Anwendung einrichten, wenn Sie für ein Element unterschiedliche Konformitätszustände, Meldungen oder Korrekturmaßnahmen festlegen möchten.

2.9 Hinweise zu Profilen

Für die Profilerstellung gelten folgende Grundsätze:

- Einer Richtlinie können beliebig viele Profile zugewiesen werden.
- Es muss jedoch mindestens ein Betriebssystemprofil enthalten sein.
- Richtlinien müssen für jedes auf einem Endpoint zu bewertende Betriebssystem das entsprechende Betriebssystemprofil enthalten.
- Einem Profil darf nur ein Betriebssystem oder eine Anwendung zugeordnet sein.
- Betriebssysteme und Anwendungen können hingegen mehreren Profilen angehören.

2.10 Einsatz vorhandener Patch Manager-Profile

Mit den vorhandenen Patch Manager-Profilen können Sie die Konformität mit Patches sowohl auf verwalteten als auch auf nicht-verwalteten Endpoints durchsetzen.

Wenn Sie den Patch Agent mit Enterprise Console kombinieren, können Sie die Ergebnisse der Patch-Analyse in die Ergebnisse der Überprüfungen von NAC integrieren. Das vordefinierte Sophos Patch Agent-Profil kann auf NAC-Richtlinien übertragen werden. Wenn Sie diese Funktion nicht verwenden, können Sie dennoch mit dem Windows Update-Profil nach Betriebssystem-Updates suchen.

Richtlinien „Default“ und „Managed“

Das folgende Profil wird automatisch den Richtlinien „Default“ und „Managed“ zugeordnet. Dieses Profil ist für den Quarantine Agent und für bekannte Benutzer bestimmt.

- **Windows Update Profile:** Dieses Profil sorgt dafür, dass das Dienstprogramm „Windows Update“ auf allen verwalteten Endpoints installiert wird. Wenn auf einem Endpoint keine automatischen Updates aktiviert sind, werden durch die Korrekturmaßnahme auf dem Endpoint automatische Updates aktiviert.

Hinweis: Das Sophos Patch Agent-Profil wird nicht automatisch zu den Richtlinien hinzugefügt. Da die „Behavior“-Einstellung „Best“ lautet und sowohl das Windows-Update- als auch das Sophos Patch Agent-Profil enthalten ist, kann ein Computer auch als richtlinienkonform gelten, wenn er nicht über alle Patches verfügt, sofern das Windows Update-Tool installiert ist und automatische Updates aktiviert wurden. Wenn Sie das Sophos Patch Agent-Profil in die Richtlinien aufnehmen möchten, empfiehlt sich, das Windows Update-Profil zu entfernen oder die „Behavior“-Einstellung „All“ auszuwählen.

Unmanaged-Richtlinie

Das folgende Profil wird automatisch der Richtlinie „Unmanaged“ zugeordnet. Dieses Profil ist für den Dissolvable Agent und für temporäre Benutzer bestimmt.

- **Windows Update Profile for Unmanaged Endpoints:** Dieses Profil sorgt dafür, dass das Dienstprogramm „Windows Update“ auf allen nicht verwalteten Endpoints installiert wird. Falls auf einem Endpoint automatische Updates nicht aktiviert sind, weist eine Meldung darauf hin, dass zum Erreichen des Konformitätszustands automatische Updates aktiviert sein müssen.

2.11 Erstellen von Betriebssystemprofilen

Die Seite „Profiles“ ermöglicht Ihnen das Erstellen von Betriebssystemprofilen für die Integration in Richtlinien. Mit Betriebssystemprofilen können Sie Betriebssysteme sowie Service-Packs, die auf dem Endpoint analysiert werden sollen, verwalten und nach Prioritätsstufe sortieren. In Profilen lassen sich Bedingungen zur Ermittlung des Konformitätszustands des Endpoints festlegen und Meldungen für den Endpoint einrichten.

Vorgehensweise

1. Klicken Sie auf **Manage > Profiles**. Klicken Sie links unten auf der Seite auf **Create Profile**.
2. Geben Sie einen Namen und eine Beschreibung für das Profil ein.
3. Klicken Sie auf **Select Profile Item**.
4. Wählen Sie aus dem Listenfeld **Profile Type** die Option **Operating System** und dann das Betriebssystem, für das Sie dieses Profil erstellen möchten. Klicken Sie auf **OK**.

Wichtig: Betriebssystemprofile sind für Richtlinien erforderlich. Falls eins der erforderlichen Betriebssysteme nicht auf dem Endpoint installiert ist, wird der Status der ELSE-Bedingungsübereinstimmung des Betriebssystemprofils mit höchster Priorität verwendet, um den Konformitätsstatus und die Maßnahmen für den Betriebssystemprofiltyp festzustellen. Keine weiteren Profile dieser Richtlinie werden analysiert.

5. Klicken Sie ggf. auf die Listenfelder in der Spalte **Compliance State**, um die Konformitätszustände für folgende Betriebssystembedingungen zu ändern. Weitere Informationen finden Sie unter *Ermitteln des Konformitätszustands* (Seite 43).
 - **Installed:** Wenn dieses Betriebssystem installiert ist, wird der Konformitätszustand auf die Richtlinienüberprüfung des Endpoints übertragen und evtl. zuvor eingerichtete Meldungen werden angezeigt.
 - **Else:** Wenn keins der Betriebssysteme installiert ist, wird der Konformitätszustand des Betriebssystemprofils mit der höchsten Priorität auf die Richtlinienüberprüfung des Endpoints übertragen und evtl. zuvor eingerichtete Meldungen werden angezeigt.

6. Klicken Sie ggf. auf die Listenfelder in der Spalte **Message** und wählen Sie **Show Message**, um für eine Bedingung eine Meldung zu erstellen. Klicken Sie dann auf das **Message**-Symbol, geben Sie die Meldung in den gewünschten Sprachen (maximal acht) ein und klicken Sie auf **OK**.

Diese Meldung wird auf dem Endpoint nur dann angezeigt, wenn die Bedingung erfüllt ist.

Hinweis: Der Agent wählt zur Ausgabe von Meldungen auf einem Endpoint die am besten passende Sprache aus. Es empfiehlt sich, eine Meldung auf Englisch (Standardsprache) für den Fall zu erstellen, dass eine Nachricht in einer anderen Sprache nicht angezeigt werden kann. So erhält der Benutzer des Endpoints immer eine Nachricht. Ältere Versionen des Agenten können Meldungen nur in englischer Sprache (Standardsprache) anzeigen. Weitere Informationen zu Meldungen finden Sie in der *Sophos Compliance Agent Konfigurationsanleitung*.

7. Klicken Sie auf **Add Service Packs**.

Hinweis: Service-Packs werden nur analysiert, wenn das zugehörige Betriebssystem auf dem Endpoint installiert ist.

8. Markieren Sie die gewünschten Service-Packs für die Aufnahme ins Profil und klicken Sie auf **OK**.
9. Klicken Sie ggf. auf die Listenfelder in der Spalte **Compliance State**, um die Konformitätszustände für jede Service-Pack-Bedingung zu ändern.

- **Installed:** Wenn dieses Service-Pack installiert ist, wird der zugeordnete Konformitätszustand auf die Richtlinienüberprüfung des Endpoints übertragen und evtl. zuvor eingerichtete Meldungen werden angezeigt.
- **Else:** Wenn keins der Service-Packs installiert ist, wird der Konformitätszustand des Service-Packs mit der höchsten Priorität (also das aktuellste) auf die Richtlinienüberprüfung des Endpoints übertragen und evtl. zuvor eingerichtete Meldungen werden angezeigt.

10. Klicken Sie ggf. auf die Listenfelder in der Spalte **Message** und wählen Sie **Show Message**, um für eine Bedingung eine Meldung zu erstellen. Klicken Sie dann auf das **Message**-Symbol, geben Sie die Meldung in den gewünschten Sprachen (maximal acht) ein und klicken Sie auf **OK**.

Diese Meldung wird auf dem Endpoint nur dann angezeigt, wenn die Bedingung erfüllt ist.

11. Klicken Sie auf **Save**.

Hinweis: Wenn das Profil erstellt ist, können Sie über ein Rechtsklickmenü auf der Profil-Listenseite oder beim Bearbeiten der Vorlage durch Klicken auf den Link **View Usage Details** die Richtlinien anzeigen, die dieses Profil verwenden.

2.12 Erstellen von Anwendungsprofilen

Die Seite „Profile“ ermöglicht Ihnen das Erstellen von Anwendungsprofilen für die Integration in Richtlinien. Mit Anwendungsprofilen können Sie Anwendungen sowie zugehörige Fähigkeiten, die auf dem Endpoint analysiert werden sollen, verwalten und nach Prioritätsstufe sortieren. In Profilen lassen sich Bedingungen zur Ermittlung des Konformitätszustands des Endpoints festlegen und Meldungen oder Korrekturmaßnahmen für den Endpoint einrichten.

Vorgehensweise

1. Klicken Sie auf **Manage > Profiles**. Klicken Sie links unten auf der Seite auf **Create Profile**.
2. Geben Sie einen Namen und eine Beschreibung für das Profil ein.
3. Klicken Sie auf **Select Profile Item**.
4. Wählen Sie aus der Liste **Profile Type** einen Profiltyp aus und geben Sie die entsprechenden Suchoptionen ein oder wählen Sie sie aus. Klicken Sie auf **Search**.
5. Wählen Sie die Anwendung, für die das Profil erstellt werden soll, und klicken Sie auf **OK**.

Hinweis: Damit die Namen der Anwendungen einwandfrei angezeigt werden, muss auf dem Computer, auf dem NAC Manager ausgeführt wird, Unterstützung für ostasiatische Sprachen (über **Systemsteuerung > Ländereinstellungen**) installiert sein.

6. Klicken Sie ggf. auf die Listenfelder in der Spalte **Compliance State**, um die Konformitätszustände für folgende Anwendungsbedingungen zu ändern. Weitere Informationen finden Sie unter [Ermitteln des Konformitätszustands](#) (Seite 43).
 - **Installed:** Wenn diese Anwendung installiert ist, wird der Konformitätszustand auf die Richtlinienüberprüfung des Endpoints übertragen und evtl. zuvor eingerichtete Meldungen werden angezeigt.
 - **Else:** Wenn diese Anwendung nicht installiert ist, wird der Konformitätszustand auf die Richtlinienüberprüfung des Endpoints übertragen und evtl. zuvor eingerichtete Meldungen werden angezeigt.

7. Klicken Sie ggf. auf die Listenfelder in der Spalte **Message** und wählen Sie **Show Message**, um für eine Bedingung eine Meldung zu erstellen. Klicken Sie dann auf das **Message**-Symbol, geben Sie die Meldung in den gewünschten Sprachen (maximal acht) ein und klicken Sie auf **OK**.

Diese Meldung wird auf dem Endpoint nur dann angezeigt, wenn die Bedingung erfüllt ist.

Hinweis: Der Agent wählt zur Ausgabe von Meldungen auf einem Endpoint die am besten passende Sprache aus. Es empfiehlt sich, eine Meldung auf Englisch (Standardsprache) für den Fall zu erstellen, dass eine Nachricht in einer anderen Sprache nicht angezeigt werden kann. So erhält der Benutzer des Endpoints immer eine Nachricht. Ältere Versionen des Agenten können Meldungen nur in englischer Sprache (Standardsprache) anzeigen. Weitere Informationen zu Meldungen finden Sie in der *Sophos Compliance Agent Konfigurationsanleitung*.

8. Klicken Sie auf **Add Capabilities**.

Unter Capabilities sind die Funktionen einer Anwendung zu verstehen, die im Rahmen einer Konformitätsbewertung getestet werden können. Dazu zählen Bewertungsregeln, die sich aus Bedingungen, Konformitätszuständen, Meldungen und Korrekturmaßnahmen (falls vorhanden) zusammensetzen.

Fähigkeiten werden nur analysiert, wenn die Anwendung auf dem Endpoint installiert ist.

9. Markieren Sie die gewünschten Fähigkeiten für die Aufnahme ins Profil und klicken Sie auf **OK**.

Näheres zu Fähigkeiten erfahren Sie unter [Anzeigen von Anwendungsfähigkeiten und Bedingungen](#) (Seite 33).

10. Führen Sie für jede Fähigkeit einen oder alle der folgenden Schritte aus:

- a) Klicken Sie auf die Listenfelder in der Spalte **Condition**, um Bedingungen auszuwählen oder geben Sie in die jeweiligen Felder Bedingungsparameter ein.

Weitere Informationen zu Bedingungen, die nur für bestimmte Anwendungsfähigkeiten gelten, finden Sie unter [Anzeigen von Anwendungsfähigkeiten und Bedingungen](#) (Seite 33).

- b) Klicken Sie auf die Listenfelder in der Spalte **Compliance State**, um den Konformitätszustand einer Bedingung zu ändern.
- c) Klicken Sie auf die Listenfelder in der Spalte **Message** und wählen Sie **Show Message**, um eine Meldung für eine Bedingung zu erstellen. Klicken Sie dann auf das **Message**-Symbol, geben Sie die Meldung in den gewünschten Sprachen (maximal acht) ein und klicken Sie auf **OK**.

Diese Meldung wird auf dem Endpoint nur dann angezeigt, wenn die Bedingung erfüllt ist.

- d) Aktivieren Sie in der Spalte **Remediation Action** das gewünschte Kontrollkästchen, um Korrekturmaßnahmen auszuwählen, die Sie einer Bedingung zuordnen möchten.

Diese Maßnahme wird auf dem Endpoint nur dann durchgeführt, wenn die Bedingung erfüllt ist. Korrekturmaßnahmen stehen nicht für alle Anwendungen oder

Anwendungsfähigkeiten zur Verfügung. Es stehen folgende Korrekturmaßnahmen zur Auswahl:

- **Enable:** Aktiviert auf dem Endpoint Echtzeitschutz für Viren- oder Spywareschutzanwendungen, aktiviert die Firewall für Firewall-Anwendungen oder ermöglicht automatische Updates für Patch Manager-Anwendungen. Diese Maßnahme steht nur für die Anwendungsfähigkeit „Real-Time Protection“ oder „Enabled“ zur Auswahl.
- **Update:** Aktualisiert die Signaturdatei auf dem Endpoint. Diese Maßnahme steht nur für die Fähigkeit „Signature Date“ oder „Signature Grace Period“ zur Auswahl.
- **Scan:** Leitet eine Überprüfung auf dem Endpoint ein. Diese Maßnahme steht nur für die Fähigkeit „Scan Date“ oder „Signature Grace Period“ zur Auswahl.
- **Apply:** Die Sophos Enterprise Console-Richtlinie wird auf Sophos Anti-Virus auf dem Endpoint angewandt. Diese Maßnahme ist für die SEC Policy-Fähigkeit verfügbar.

- e) Klicken Sie auf **New Condition**, um der Anwendungsfähigkeit weitere Bedingungen zuzuweisen.

Die verfügbaren Bedingungen richten sich nach den in Schritt 9 ausgewählten Fähigkeiten. Wenn Sie keine Fähigkeiten mit zusätzlichen Bedingungen ausgewählt haben, wird diese Schaltfläche nicht angezeigt. Wenn Sie zusätzliche Bedingungen ausgewählt haben, können Sie die Priorität der Bedingungen für die Endpoint-Analyse durch Klicken auf die Pfeilsymbole ändern.

11. Klicken Sie auf **Save**.

Hinweis: Wenn das Profil erstellt ist, können Sie über ein Rechtsklickmenü auf der Profil-Listenseite oder beim Bearbeiten der Vorlage durch Klicken auf den Link **View Usage Details** die Richtlinien anzeigen, die dieses Profil verwenden.

2.13 Anzeigen von Anwendungsfähigkeiten und Bedingungen

In der folgenden Tabelle werden die Bedingungen für jede Anwendungsfähigkeit nach Profiltyp sortiert aufgeführt und erklärt.

Weitere Informationen zur Erstellung von Anwendungsprofilen finden Sie unter [Erstellen von Anwendungsprofilen](#) (Seite 31).

Hinweis: Die verfügbaren Anwendungsfähigkeiten und Korrekturmaßnahmen hängen vom Softwaredesign der Anwendung ab. Einige Fähigkeiten und Korrekturmaßnahmen stehen für bestimmte Betriebssysteme, auf denen die Anwendung unterstützt wird, oder für alle Versionen einer Anwendung nicht zur Verfügung. Nicht verfügbare Fähigkeiten werden nicht angezeigt. Wenn eine Fähigkeit auf einigen Betriebssystemen nicht unterstützt wird, werden nur die kompatiblen Betriebssysteme angezeigt. Wenn eine Korrekturmaßnahme nur auf bestimmten Betriebssystemen unterstützt wird, werden die Betriebssysteme, auf denen die Maßnahme nicht zur Verfügung steht, entsprechend gekennzeichnet.

Sophos Anti-Virus

Hinweis: Sophos Anti-Virus bietet neben den Antiviren-, Anti-Spyware-, HIPS- und IDS-Anwendungsfähigkeiten die folgenden Fähigkeiten. Welche Fähigkeiten zur Verfügung stehen, hängt von der Softwareversion ab.

Anwendungsfähigkeit	Beschreibung und mögliche Bedingungen
Adware/PUA	<p>Enthält die Bedingungen zur Erkennung von Adware und PUAs auf dem Endpoint. Es sind folgende Bedingungen möglich:</p> <ul style="list-style-type: none"> ■ Detected/Not Detected: Legt fest, ob die Adware oder eine PUA erkannt bzw. nicht erkannt wird und enthält den zugehörigen Konformitätszustand und die jeweils auszugebende Meldung, wenn die Bedingung erfüllt ist. ■ Else: Enthält den Konformitätszustand und die Meldung für eine nicht erfüllte Bedingung.
Controlled Applications	<p>Hiermit wird ermittelt, ob auf dem Endpoint eine Controlled Application erkannt wird. Controlled Applications werden in der Sophos Enterprise Console-Richtlinie festgelegt. Es sind folgende Bedingungen möglich:</p> <ul style="list-style-type: none"> ■ Detected/Not Detected: Legt fest, ob die Controlled Application erkannt bzw. nicht erkannt wird und enthält den zugehörigen Konformitätszustand und die jeweils auszugebende Meldung, wenn die Bedingung erfüllt ist. ■ Else: Enthält den Konformitätszustand und die Meldung für eine nicht erfüllte Bedingung.
Von SEC verwaltet	<p>Bestimmt, ob Sophos Anti-Virus von Sophos Enterprise Console verwaltet oder als Einzelplatzprodukt installiert wird. Es sind folgende Bedingungen möglich:</p> <ul style="list-style-type: none"> ■ Yes/No: Legt fest, ob Sophos Anti-Virus von Sophos Enterprise Console verwaltet wird und enthält den zugehörigen Konformitätszustand und die jeweils auszugebende Meldung, wenn die Bedingung erfüllt ist. ■ Else: Enthält den Konformitätszustand und die Meldung für eine nicht erfüllte Bedingung.
SEC Policy	<p>Bestimmt, ob Sophos Anti-Virus der Sophos Enterprise Console-Richtlinie entspricht. Es sind folgende Bedingungen möglich:</p> <ul style="list-style-type: none"> ■ Conforms/Does Not Conform: Legt fest, ob Sophos Anti-Virus mit der Sophos Enterprise Console-Richtlinie übereinstimmt und enthält den zugehörigen Konformitätszustand und die jeweils vorzunehmende Maßnahme, wenn die Bedingung erfüllt ist. ■ Else: Enthält den Konformitätszustand, die Meldung und die Maßnahme für eine erfüllte/nicht erfüllte Bedingung.

Anwendungsfähigkeit	Beschreibung und mögliche Bedingungen
Suspicious Behavior	<p>Hiermit wird ermittelt, ob auf dem Endpoint verdächtiges Verhalten erkannt wird. Es sind folgende Bedingungen möglich:</p> <ul style="list-style-type: none"> ■ Detected/Not Detected: Legt fest, ob verdächtiges Verhalten erkannt bzw. nicht erkannt wird und enthält den zugehörigen Konformitätszustand und die jeweils auszugebende Meldung, wenn die Bedingung erfüllt ist. ■ Else: Enthält den Konformitätszustand und die Meldung für eine nicht erfüllte Bedingung.
Suspicious File	<p>Hiermit wird ermittelt, ob auf dem Endpoint verdächtige Dateien erkannt werden. Es sind folgende Bedingungen möglich:</p> <ul style="list-style-type: none"> ■ Detected/Not Detected: Legt fest, eine verdächtige Datei erkannt bzw. nicht erkannt wird, und enthält den zugehörigen Konformitätszustand und die jeweils auszugebende Meldung, wenn die Bedingung erfüllt ist. ■ Else: Enthält den Konformitätszustand und die Meldung für eine nicht erfüllte Bedingung.
Viren/Spyware	<p>Hiermit wird festgestellt, ob auf dem Endpoint ein Virus oder Spyware erkannt wurde. Es sind folgende Bedingungen möglich:</p> <ul style="list-style-type: none"> ■ Detected/Not Detected: Legt fest, ob ein Virus oder Spyware erkannt bzw. nicht erkannt wird, und enthält den zugehörigen Konformitätszustand und die jeweils auszugebende Meldung, wenn die Bedingung erfüllt ist. ■ Else: Enthält den Konformitätszustand und die Meldung für eine nicht erfüllte Bedingung.

Anti-Spyware oder Anti-Virus

Anwendungsfähigkeit	Beschreibung und mögliche Bedingungen
Last Scan Date	<p>Ermittelt, ob das Datum der letzten Anwendungsüberprüfung dem in der Bedingung festgelegten Datum entspricht. Diese Fähigkeit kann anstelle der Fähigkeit „Last Scan Grace Period“ verwendet werden. Es sind folgende Bedingungen möglich:</p> <ul style="list-style-type: none"> ■ Date: Hier ist das Datum der letzten Überprüfung auf dem Endpoint angegeben. Dazu werden Konformitätszustand, Meldung und Maßnahme aufgelistet, die bei erfüllter Bedingung gelten. Es gibt folgende Operatoren: == (gleich), != (nicht gleich), < (kleiner als), <= (kleiner gleich), > (größer als), >= (größer gleich). ■ Else: Konformitätszustand, Meldung und Maßnahme bei nicht erfüllter Bedingung.

Anwendungsfähigkeit	Beschreibung und mögliche Bedingungen
Last Scan Grace Period	<p>Ermittelt, ob das Datum der letzten Anwendungsüberprüfung gemäß dem in der Bedingung festgelegten Zeitraum aktuell ist. Diese Fähigkeit kann anstelle der Fähigkeit „Last Scan Date“ verwendet werden. Es sind folgende Bedingungen möglich:</p> <ul style="list-style-type: none"> ■ Within: Hier wird der Zeitraum festgelegt, in dem sich das letzte Überprüfungsdatum auf dem Endpoint befinden muss, um als aktuell zu gelten. Dazu werden Konformitätszustand, Meldung und Maßnahme aufgelistet, die bei erfüllter Bedingung zutreffen. ■ Else: Konformitätszustand, Meldung und Maßnahme, wenn das Datum nicht im festgelegten Zeitraum liegt.
Real-Time Protection	<p>Hiermit wird ermittelt, ob die Anwendung den Endpoint aktiv schützt. Es sind folgende Bedingungen möglich:</p> <ul style="list-style-type: none"> ■ Enabled/Disabled: Aktivierung bzw. Deaktivierung des Echtzeitschutzes der Anwendung auf dem Endpoint. Zeigt Konformitätszustand, Meldung und Maßnahme im Falle zutreffender Bedingung an. ■ Else: Konformitätszustand, Meldung und Maßnahme, wenn keine der beiden Bedingungen zutrifft.
Signature Date	<p>Ermittelt, ob das Datum der Signaturdatei der Anwendung dem in der Bedingung festgelegten Datum entspricht. Diese Fähigkeit kann anstelle der Fähigkeit „Signature Grace Period“ verwendet werden. Es sind folgende Bedingungen möglich:</p> <ul style="list-style-type: none"> ■ Date: Hier ist das Datum der Signaturdatei auf dem Endpoint angegeben. Dazu werden Konformitätszustand, Meldung und Maßnahme aufgelistet, die bei erfüllter Bedingung gelten. Es gibt folgende Operatoren: == (gleich), != (nicht gleich), < (kleiner als), <= (kleiner gleich), > (größer als), >= (größer gleich). ■ Else: Konformitätszustand, Meldung und Maßnahme bei nicht erfüllter Bedingung.
Signature Grace Period	<p>Ermittelt, ob das Datum der Signaturdatei der Anwendung gemäß dem in der Bedingung festgelegten Zeitraum aktuell ist. Diese Fähigkeit kann anstelle der Fähigkeit „Signature Date“ verwendet werden. Es sind folgende Bedingungen möglich:</p> <ul style="list-style-type: none"> ■ Within: Hier ist der Zeitraum in Tagen festgelegt, in dem sich das Datum der Signaturdatei auf dem Endpoint befinden muss, um als aktuell zu gelten. Dazu werden Konformitätszustand, Meldung und Maßnahme aufgelistet, die bei erfüllter Bedingung zutreffen. ■ Else: Konformitätszustand, Meldung und Maßnahme, wenn das Datum nicht im festgelegten Zeitraum liegt.

Anwendungsfähigkeit	Beschreibung und mögliche Bedingungen
Version	<p>Ermittelt, ob die Version der Anwendung auf dem Endpoint die Bedingung erfüllt.</p> <p>Hinweis: Die Version wird auf dem Endpoint anhand der in der Bedingung angegebenen Kennwerte analysiert. Wenn Sie beispielsweise eine Bedingung mit == 8 anlegen und auf dem Endpoint Version 8.1 installiert wurde, vergleicht die Software Version 8.1 mit dem in der Bedingung festgelegten Kennwert (nämlich 8). Die Bedingung ist somit erfüllt. Wenn Sie jedoch eine Bedingung mit == 8.0 anlegen und die auf dem Endpoint installierte Version 8.1 lautet, vergleicht die Software Version 8.1 mit den beiden Kennwerten (nämlich 8 und 0) in der Bedingung. In diesem Fall ist die Bedingung nicht erfüllt.</p> <ul style="list-style-type: none"> ■ Wenn die Anwendung die Versionsnummer im Profil abgelegt hat, sind folgende Bedingungen im Profil verfügbar: <ul style="list-style-type: none"> ■ Version: Hier ist die Version der Anwendung auf dem Endpoint angegeben. Dazu werden Konformitätszustand und Meldung aufgelistet, die bei erfüllter Bedingung gelten. Es gibt folgende Operatoren: == (gleich), != (nicht gleich), < (kleiner als), <= (kleiner gleich), > (größer als), >= (größer gleich). Die Version muss im Format <i>N.n.n.n</i> angegeben werden und ist auf vier Kennwerte beschränkt. ■ Else: Enthält den Konformitätszustand und die Meldung bei nicht erfüllter Versionsbedingung. ■ Wenn die Versionsnummer der Anwendung in den Anwendungserkennungsregeln definiert wurde, sind folgende Bedingungen im Profil verfügbar: <ul style="list-style-type: none"> ■ Pass/Fail: Hiermit wird festgelegt, ob die Analyse auf dem Endpoint positiv (pass) oder negativ (fail) verläuft, wenn die Endpoint-Anwendungsversion mit der Versionsnummer übereinstimmt, die in den Anwendungserkennungsregeln definiert ist. Ist die Bedingung erfüllt, liegt der hier angegebene Konformitätszustand vor und es wird die hier eingerichtete Meldung ausgegeben. ■ Else: Enthält den Konformitätszustand und die Meldung für eine nicht erfüllte Bedingung.

Assessment, HIPS oder IDS

Anwendungsfähigkeit	Beschreibung und mögliche Bedingungen
Running	<p>Hiermit wird ermittelt, ob die ausführbaren Dienste auf dem Endpoint laufen. Es sind folgende Bedingungen möglich:</p> <ul style="list-style-type: none"> ■ Running/Not Running: Der Dienst läuft bzw. läuft nicht auf dem Endpoint. Der Konformitätszustand, die Meldung und die Maßnahme im Falle zutreffender Bedingung werden angezeigt. ■ Else: Konformitätszustand, Meldung und Maßnahme, wenn keine der beiden Bedingungen zutrifft.
Version	<p>Ermittelt, ob die Version der Anwendung auf dem Endpoint die Bedingung erfüllt.</p> <p>Hinweis: Die Version wird auf dem Endpoint anhand der in der Bedingung angegebenen Kennwerte analysiert. Wenn Sie beispielsweise eine Bedingung mit == 8 anlegen und auf dem Endpoint Version 8.1 installiert wurde, vergleicht die Software Version 8.1 mit dem in der Bedingung festgelegten Kennwert (nämlich 8). Die Bedingung ist somit erfüllt. Wenn Sie jedoch eine Bedingung mit == 8.0 anlegen und die auf dem Endpoint installierte Version 8.1 lautet, vergleicht die Software Version 8.1 mit den beiden Kennwerten (nämlich 8 und 0) in der Bedingung. In diesem Fall ist die Bedingung nicht erfüllt.</p> <ul style="list-style-type: none"> ■ Wenn die Anwendung die Versionsnummer im Profil abgelegt hat, sind folgende Bedingungen im Profil verfügbar: <ul style="list-style-type: none"> ■ Version: Hier ist die Version der Anwendung auf dem Endpoint angegeben. Dazu werden Konformitätszustand und Meldung aufgelistet, die bei erfüllter Bedingung gelten. Es gibt folgende Operatoren: == (gleich), != (nicht gleich), < (kleiner als), <= (kleiner gleich), > (größer als), >= (größer gleich). Die Version muss im Format <i>N.n.n.n</i> angegeben werden und ist auf vier Kennwerte beschränkt. ■ Else: Enthält den Konformitätszustand und die Meldung bei nicht erfüllter Versionsbedingung. ■ Wenn die Versionsnummer der Anwendung in den Anwendungserkennungsregeln definiert wurde, sind folgende Bedingungen im Profil verfügbar: <ul style="list-style-type: none"> ■ Pass/Fail: Hiermit wird festgelegt, ob die Analyse auf dem Endpoint positiv (pass) oder negativ (fail) verläuft, wenn die Endpoint-Anwendungsversion mit der Versionsnummer übereinstimmt, die in den Anwendungserkennungsregeln definiert ist. Ist die Bedingung erfüllt, liegt der hier angegebene Konformitätszustand vor und es wird die hier eingerichtete Meldung ausgegeben. ■ Else: Enthält den Konformitätszustand und die Meldung für eine nicht erfüllte Bedingung.

Firewall

Anwendungsfähigkeit	Beschreibung und mögliche Bedingungen
Enabled	<p>Hiermit wird ermittelt, ob die Anwendung den Endpoint aktiv schützt. Es sind folgende Bedingungen möglich:</p> <ul style="list-style-type: none"> ■ Enabled/Disabled: Aktivierung bzw. Deaktivierung der Firewall auf dem Endpoint. Zeigt Konformitätszustand, Meldung und Maßnahme im Falle zutreffender Bedingung an. ■ Else: Konformitätszustand, Meldung und Maßnahme, wenn keine der beiden Bedingungen zutrifft.
Running	<p>Hiermit wird ermittelt, ob die ausführbaren Dienste auf dem Endpoint laufen. Es sind folgende Bedingungen möglich:</p> <ul style="list-style-type: none"> ■ Running/Not Running: Der Dienst läuft bzw. läuft nicht auf dem Endpoint. Der Konformitätszustand, die Meldung und die Maßnahme im Falle zutreffender Bedingung werden angezeigt. ■ Else: Konformitätszustand, Meldung und Maßnahme, wenn keine der beiden Bedingungen zutrifft.
Version	<p>Ermittelt, ob die Version der Anwendung auf dem Endpoint die Bedingung erfüllt.</p> <p>Hinweis: Die Version wird auf dem Endpoint anhand der in der Bedingung angegebenen Kennwerte analysiert. Wenn Sie beispielsweise eine Bedingung mit == 8 anlegen und auf dem Endpoint Version 8.1 installiert wurde, vergleicht die Software Version 8.1 mit dem in der Bedingung festgelegten Kennwert (nämlich 8). Die Bedingung ist somit erfüllt. Wenn Sie jedoch eine Bedingung mit == 8.0 anlegen und die auf dem Endpoint installierte Version 8.1 lautet, vergleicht die Software Version 8.1 mit den beiden Kennwerten (nämlich 8 und 0) in der Bedingung. In diesem Fall ist die Bedingung nicht erfüllt.</p> <ul style="list-style-type: none"> ■ Wenn die Anwendung die Versionsnummer im Profil abgelegt hat, sind folgende Bedingungen im Profil verfügbar: <ul style="list-style-type: none"> ■ Version: Hier ist die Version der Anwendung auf dem Endpoint angegeben. Dazu werden Konformitätszustand und Meldung aufgelistet, die bei erfüllter Bedingung gelten. Es gibt folgende Operatoren: == (gleich), != (nicht gleich), < (kleiner als), <= (kleiner gleich), > (größer als), >= (größer gleich). Die Version muss im Format <i>N.n.n.n</i> angegeben werden und ist auf vier Kennwerte beschränkt. ■ Else: Enthält den Konformitätszustand und die Meldung bei nicht erfüllter Versionsbedingung.

Anwendungsfähigkeit	Beschreibung und mögliche Bedingungen
	<ul style="list-style-type: none"> ■ Wenn die Versionsnummer der Anwendung in den Anwendungserkennungsregeln definiert wurde, sind folgende Bedingungen im Profil verfügbar: <ul style="list-style-type: none"> ■ Pass/Fail: Hiermit wird festgelegt, ob die Analyse auf dem Endpoint positiv (pass) oder negativ (fail) verläuft, wenn die Endpoint-Anwendungsversion mit der Versionsnummer übereinstimmt, die in den Anwendungserkennungsregeln definiert ist. Ist die Bedingung erfüllt, liegt der hier angegebene Konformitätszustand vor und es wird die hier eingerichtete Meldung ausgegeben. ■ Else: Enthält den Konformitätszustand und die Meldung für eine nicht erfüllte Bedingung.

Fixed Device Encryption

Anwendungsfähigkeit	Beschreibung und mögliche Bedingungen
Full Disk Encryption	<p>Hiermit wird ermittelt, ob die Festplatten eines Endpoints verschlüsselt sind. Es sind folgende Bedingungen möglich:</p> <ul style="list-style-type: none"> ■ All Drives/At Least 1 Drive/No Drives: Hier wird angegeben, ob alle Laufwerke (All Drives), mindestens ein Laufwerk (At Least 1 Drive) oder keine Laufwerke (No Drives) auf dem Endpoint verschlüsselt sind. Wenn eine dieser Bedingungen zutrifft, werden jeweils der zugehörige Konformitätszustand und die zugehörige Meldung angezeigt. ■ Else: Hier werden Konformitätszustand und Meldung für den Fall, dass keine Bedingung zutrifft, angezeigt.
Pre-boot Authentication	<p>Hier wird bestimmt, ob die Anwendung einen Endpoint bereits vor dem Hochfahren des Systems authentifiziert. Es sind folgende Bedingungen möglich:</p> <ul style="list-style-type: none"> ■ Enabled/Temporarily Disabled/Disabled: Diese Bedingung bestimmt, ob „Pre-boot Authentication“ auf dem Endpoint aktiviert (enabled), vorübergehend deaktiviert (temporarily disabled) oder deaktiviert (disabled) ist. Es wird jeweils der Konformitätszustand, die Meldung und die Maßnahme angezeigt. ■ Else: Hier werden Konformitätszustand, Meldung und Maßnahme für den Fall, dass keine Bedingung zutrifft, angezeigt.
Version	<p>Ermittelt, ob die Version der Anwendung auf dem Endpoint die Bedingung erfüllt.</p> <p>Hinweis: Die Version wird auf dem Endpoint anhand der in der Bedingung angegebenen Kennwerte analysiert. Wenn Sie beispielsweise eine Bedingung mit == 8 anlegen und auf dem Endpoint Version 8.1 installiert wurde,</p>

Anwendungsfähigkeit	Beschreibung und mögliche Bedingungen
	<p>vergleicht die Software Version 8.1 mit dem in der Bedingung festgelegten Kennwert (nämlich 8). Die Bedingung ist somit erfüllt. Wenn Sie jedoch eine Bedingung mit == 8.0 anlegen und die auf dem Endpoint installierte Version 8.1 lautet, vergleicht die Software Version 8.1 mit den beiden Kennwerten (nämlich 8 und 0) in der Bedingung. In diesem Fall ist die Bedingung nicht erfüllt.</p> <ul style="list-style-type: none"> ■ Wenn die Anwendung die Versionsnummer im Profil abgelegt hat, sind folgende Bedingungen im Profil verfügbar: <ul style="list-style-type: none"> ■ Version: Hier ist die Version der Anwendung auf dem Endpoint angegeben. Dazu werden Konformitätszustand und Meldung aufgelistet, die bei erfüllter Bedingung gelten. Es gibt folgende Operatoren: == (gleich), != (nicht gleich), < (kleiner als), <= (kleiner gleich), > (größer als), >= (größer gleich). Die Version muss im Format <i>N.n.n.n</i> angegeben werden und ist auf vier Kennwerte beschränkt. ■ Else: Enthält den Konformitätszustand und die Meldung bei nicht erfüllter Versionsbedingung. ■ Wenn die Versionsnummer der Anwendung in den Anwendungserkennungsregeln definiert wurde, sind folgende Bedingungen im Profil verfügbar: <ul style="list-style-type: none"> ■ Pass/Fail: Hiermit wird festgelegt, ob die Analyse auf dem Endpoint positiv (pass) oder negativ (fail) verläuft, wenn die Endpoint-Anwendungsversion mit der Versionsnummer übereinstimmt, die in den Anwendungserkennungsregeln definiert ist. Ist die Bedingung erfüllt, liegt der hier angegebene Konformitätszustand vor und es wird die hier eingerichtete Meldung ausgegeben. ■ Else: Enthält den Konformitätszustand und die Meldung für eine nicht erfüllte Bedingung. <p>Hinweis: Die Versionsbedingung im Sophos SafeGuard 5.x-Profil wird erfüllt, wenn entweder SafeGuard 5.x oder 6.x erkannt wird.</p>

Patch Manager

Anwendungsfähigkeit	Beschreibung und mögliche Bedingungen
Enabled	<p>Hiermit wird ermittelt, ob die Anwendung den Endpoint aktiv schützt. Die Fähigkeit wird für den Patch Agent und das Windows Update-Tool angeboten. Es sind folgende Bedingungen möglich:</p> <ul style="list-style-type: none"> ■ Enabled/Disabled: Diese Bedingung bestimmt, ob die Patch-Analyse auf dem Endpoint aktiviert (enabled) oder deaktiviert (disabled) ist. Bei erfüllter Bedingung wird jeweils der Konformitätszustand und die

Anwendungsfähigkeit	Beschreibung und mögliche Bedingungen
	<p>Meldung angezeigt. Aktivierung bzw. Deaktivierung automatischer Updates für den Windows-Update-Dienst auf dem Endpoint. Zeigt Konformitätszustand, Meldung und Maßnahme im Falle zutreffender Bedingung an.</p> <ul style="list-style-type: none"> ■ Else: Konformitätszustand, Meldung und Maßnahme, wenn keine der beiden Bedingungen zutrifft.
Patched	<p>Der Endpoint verfügt über alle Patches. Es sind folgende Bedingungen möglich:</p> <ul style="list-style-type: none"> ■ Patched/Not Patched: Anzeige, ob der Endpoint gepatcht ist oder nicht. Zeigt Konformitätszustand, und Meldung im Falle zutreffender Bedingung an. ■ Else: Konformitätszustand und die Meldung für eine nicht erfüllte Bedingung "Patched/Not Patched".
Version	<p>Ermittelt, ob die Version der Anwendung auf dem Endpoint die Bedingung erfüllt.</p> <p>Hinweis: Die Version wird auf dem Endpoint anhand der in der Bedingung angegebenen Kennwerte analysiert. Wenn Sie beispielsweise eine Bedingung mit == 8 anlegen und auf dem Endpoint Version 8.1 installiert wurde, vergleicht die Software Version 8.1 mit dem in der Bedingung festgelegten Kennwert (nämlich 8). Die Bedingung ist somit erfüllt. Wenn Sie jedoch eine Bedingung mit == 8.0 anlegen und die auf dem Endpoint installierte Version 8.1 lautet, vergleicht die Software Version 8.1 mit den beiden Kennwerten (nämlich 8 und 0) in der Bedingung. In diesem Fall ist die Bedingung nicht erfüllt.</p> <ul style="list-style-type: none"> ■ Version: Hier ist die Version der Anwendung auf dem Endpoint angegeben. Dazu werden Konformitätszustand und Meldung aufgelistet, die bei erfüllter Bedingung gelten. Es gibt folgende Operatoren: == (gleich), != (nicht gleich), < (kleiner als), <= (kleiner gleich), > (größer als), >= (größer gleich). Die Version muss im Format <i>N.n.n.n</i> angegeben werden und ist auf vier Kennwerte beschränkt. ■ Else: Enthält den Konformitätszustand und die Meldung bei nicht erfüllter Versionsbedingung.

Removable Device Encryption

Anwendungsfähigkeit	Beschreibung und mögliche Bedingungen
Version	<p>Ermittelt, ob die Version der Anwendung auf dem Endpoint die Bedingung erfüllt.</p> <p>Hinweis: Die Version wird auf dem Endpoint anhand der in der Bedingung angegebenen Kennwerte analysiert. Wenn Sie beispielsweise eine Bedingung</p>

Anwendungsfähigkeit	Beschreibung und mögliche Bedingungen
	<p>mit == 8 anlegen und auf dem Endpoint Version 8.1 installiert wurde, vergleicht die Software Version 8.1 mit dem in der Bedingung festgelegten Kennwert (nämlich 8). Die Bedingung ist somit erfüllt. Wenn Sie jedoch eine Bedingung mit == 8.0 anlegen und die auf dem Endpoint installierte Version 8.1 lautet, vergleicht die Software Version 8.1 mit den beiden Kennwerten (nämlich 8 und 0) in der Bedingung. In diesem Fall ist die Bedingung nicht erfüllt.</p> <ul style="list-style-type: none"> ■ Wenn die Anwendung die Versionsnummer im Profil abgelegt hat, sind folgende Bedingungen im Profil verfügbar: <ul style="list-style-type: none"> ■ Version: Hier ist die Version der Anwendung auf dem Endpoint angegeben. Dazu werden Konformitätszustand und Meldung aufgelistet, die bei erfüllter Bedingung gelten. Es gibt folgende Operatoren: == (gleich), != (nicht gleich), < (kleiner als), <= (kleiner gleich), > (größer als), >= (größer gleich). Die Version muss im Format <i>N.n.n.n</i> angegeben werden und ist auf vier Kennwerte beschränkt. ■ Else: Enthält den Konformitätszustand und die Meldung bei nicht erfüllter Versionsbedingung. ■ Wenn die Versionsnummer der Anwendung in den Anwendungserkennungsregeln definiert wurde, sind folgende Bedingungen im Profil verfügbar: <ul style="list-style-type: none"> ■ Pass/Fail: Hiermit wird festgelegt, ob die Analyse auf dem Endpoint positiv (pass) oder negativ (fail) verläuft, wenn die Endpoint-Anwendungsversion mit der Versionsnummer übereinstimmt, die in den Anwendungserkennungsregeln definiert ist. Ist die Bedingung erfüllt, liegt der hier angegebene Konformitätszustand vor und es wird die hier eingerichtete Meldung ausgegeben. ■ Else: Enthält den Konformitätszustand und die Meldung für eine nicht erfüllte Bedingung. <p>Hinweis: Die Versionsbedingung im Sophos SafeGuard Data Exchange-Profil wird erfüllt, wenn entweder Data Exchange 5.x oder 6.x erkannt wird.</p>

2.14 Ermitteln des Konformitätszustands

Der Konformitätszustand wird anhand der Konformität des Endpoints mit den Richtlinienprofilen ermittelt. Die Software überprüft die Profilbedingungen gemäß dem zugewiesenen Richtlinienverhalten für den Profiltyp. Die Ergebnisse dieser Überprüfung werden auf die Richtlinienebene übertragen. Die Konformität wird dabei anhand des am wenigsten konformen Zustands ermittelt. Sobald der Konformitätszustand ermittelt wurde,

kann der Netzwerkzugriff darauf basierend mithilfe der Access Templates der Richtlinie durchgesetzt werden.

- **Compliant:** Wenn die Bedingung bei der Analyse erfüllt wird, ist Konformität gegeben.
- **Partially Compliant:** Wenn die Bedingung bei der Analyse erfüllt wird, ist Teilkonformität gegeben.
- **Non-Compliant:** Wenn die Bedingung bei der Analyse erfüllt wird, ist keine Konformität gegeben.

3 Enforce-Bereich im Überblick

Im Enforce-Bereich sind alle Komponenten enthalten, die für die Einrichtung von Netzwerkressourcen, Netzwerkzugriffseinstellungen und Ausnahmen erforderlich sind. Die im folgenden aufgeführten Bereiche erreichen Sie über das Enforce-Menü:

Bereich und Aktion	Beschreibung
DHCP Configuration Wizard	
Starten des DHCP Configuration Wizard.	Mit dem DHCP Configuration Wizard erkennen Sie Web-Proxyserver, Korrekturserver und DHCP-Enforcer-Server für Sophos NAC DHCP-Implementierungen. Der Assistent konfiguriert die DHCP Enforcer Access Templates automatisch mit Ihren Server-Definitionen.
Netzwerkressourcen	
Erstellen von Netzwerkressourcen.	Bei Netzwerkressourcen handelt es sich um Anwendungen oder Geräte, die zur Korrektur von Endpoints oder solchen Endpoints, auf die Endpoints in Quarantäne nicht zugreifen dürfen sollen, erforderlich sind. Netzwerkressourcen können zu Agent Enforcer oder DHCP Enforcer Access Templates hinzugefügt werden. Hinweis: Netzwerkressourcen kommen bei Client-basierter Quarantäne über den Quarantine Agent oder beim DHCP Enforcement zum Einsatz.
Agent Enforcer Access Templates	
Erstellen von Agent Enforcer Access Templates.	In Agent Enforcer Access Templates wird der Zugriffsstatus aller Endpoints auf Netzwerkressourcen bei der Durchführung einer Client-basierten Quarantäne verzeichnet. Nach der Erstellung können Agent Enforcer Access Templates Richtlinien zugewiesen werden, um den Zugriff je nach dem Konformitätszustand des Agenten auf dem Endpoint durchzusetzen. Hinweis: Agent Enforcer Access Templates gelten nur für Endpoints, auf denen der Quarantine Agent läuft.
DHCP Enforcer Access Templates	
Erstellen von DHCP Enforcer Access Templates.	Mit DHCP Enforcer Access Templates können Sie die zur Unterstützung von DHCP Enforcement erforderlichen Zugriffsdaten festlegen. DHCP Enforcer Access Templates können Richtlinien, Exemptions und Enforcer-Einstellungen zugewiesen werden. Hinweis: DHCP Enforcer Access Templates kommen nur bei Sophos NAC DHCP-Implementierungen zum Einsatz.
Exemptions	
Erstellen von Exemptions.	In Exemptions (Ausnahmen) sind Endpoints basierend auf diversen Kriterien festgehalten, die bei Verbindung mit dem Netzwerk nicht auf Konformität überprüft werden müssen. Hierzu zählen Endpoints, auf denen entweder der Agent nicht ausgeführt werden kann (z.B. Endpoints, die nicht unter Windows

Bereich und Aktion	Beschreibung
	<p>laufen), oder für die keine Konformitätsprüfung erforderlich ist – z.B. Server, Router und Drucker.</p> <p>Hinweis: Exemptions betreffen ausschließlich DHCP Enforcement.</p>
Deaktivieren oder Aktivieren von Exemptions.	<p>Exemptions können durch den Systemadministrator aktiviert und deaktiviert werden. Durch das Deaktivieren einer Exemption wird der Endpoint auf Konformität überprüft. Wenn eine Exemption deaktiviert ist und auf dem Endpoint nicht Sophos Compliance Agent installiert ist, wird der Endpoint als unbekannt eingestuft. Das Aktivieren einer Exemption verhindert die Konformitätsprüfung eines Endpoints.</p>

3.1 Praxistipps: Access Templates

Dieser Abschnitt enthält Praxistipps zu Access Templates. Access Templates bestimmen, auf welche Weise Endpoints Netzwerkzugriff erhalten. Sophos NAC unterstützt Agent- und DHCP-Enforcement. Wenn in NAC Manager Access Templates auf die Access States (konform, teilkonform, nicht konform) übertragen werden, wird der Netzwerkzugriff im Rahmen der Richtlinienüberprüfung durchgesetzt.

Erstellen einer einsatzbereiten Access Template

Tipp	Beschreibung
Erstellen Sie eine Access Template, die nahezu einsatzbereit ist.	<p>Verwenden Sie in der Richtlinie die Einstellung „Policy Mode“, um die Auswirkungen auf den Endpoints allmählich zu verstärken. Auf diese Weise können Sie Enforcement über eine einfache Einstellung erreichen, ohne aufwändige Änderungen an den Access Templates vornehmen zu müssen. Weitere Informationen finden Sie unter Praxistipps: Richtlinien (Seite 13).</p>

Nutzen vorhandener Access Templates als Vorlage

Tipp	Beschreibung
Nutzen Sie vorhandene Access Templates als Vorlage.	<p>Einsatzbereiche:</p> <ul style="list-style-type: none"> ■ Für Demonstrationen, Pilotprojekte oder Machbarkeitstests können Sie die vorhandenen Access Templates verwenden. ■ Für die Einführung in die Arbeitsumgebung kopieren Sie die vorhandenen Access Templates (durch Anlegen einer Arbeitskopie) und passen die Einstellungen an.

Priorisieren von Netzwerkressourcen, Access Templates und Exemptions

Verwenden Sie Prioritätsstufen zur Implementierung des gewünschten Netzwerkzugriffs.

Tipp	Beschreibung
<p>Ordnen Sie speziellen bzw. einschränkenden Netzwerkressourcen, Access Templates und Exemptions eine höhere Priorität zu als allgemeinen Netzwerkressourcen.</p>	<ul style="list-style-type: none"> ■ Netzwerkressourcen: Wenn einem Endpoint mehr als eine Netzwerkressource zugewiesen ist, bestimmt die erste passende Netzwerkressource den Netzwerkzugriff. Ausführbare Netzwerkressourcen werden vor Port-/Protokoll-Netzwerkressourcen analysiert. ■ Access Templates: Wenn mehr als eine Access Template auf einen Zustand (Access State) zutrifft, wird die erstbeste Template gewählt. Die speziellen bzw. einschränkenden Access Templates bieten eine bestimmte IP-Adresse oder einen einschränkenden IP-Adressenbereich. Im Gegensatz dazu bieten die allgemeineren Access Templates einen umfangreicheren IP-Adressenbereich. ■ Exemptions: Wenn einem Endpoint mehr als eine Exemption zugewiesen ist, bestimmt die erste passende Exemption den Netzwerkzugriff. Wenn außerdem einer bestimmten Exemption mehr als eine Access Template zugewiesen ist, wird die erste Template verwendet, die die übereinstimmende IP-Adresse des DHCP-Servers oder DHCP-Relays enthält.

Festlegen der Konformitätszustände der Templates

Tipp	Beschreibung
<p>Wählen Sie für die Access Templates keine widersprüchlichen Konformitätszustände.</p>	<p>Durch Auswahl von „Compliant“ erstellen Sie z.B. eine Access Template, die Netzwerkzugriff ermöglicht. Durch Auswahl von „Non-Compliant“ erstellen Sie eine Access Template, die den Netzwerkzugriff auf Korrekturserver beschränkt.</p>

Festlegen von Access Templates für den Default Access State

Tipp	Beschreibung
<p>Legen Sie Access Templates für den Default Access State (Standard-Zugriffszustand) fest. Dieser Tipp ist nur für DHCP-Enforcement relevant.</p>	<p>Wenn Sie DHCP Enforcement einsetzen, geben Sie die gewünschten Access Templates für den Default Access State auf der Seite Configure System > Enforcer Settings in NAC Manager an. Der Default Access State ist als Notlösung bei der Zuweisung von Access Templates zu betrachten. Die dem Default Access</p>

Tipp	Beschreibung
	State zugeordneten Access Templates sollten daher alle erforderlichen IP-Adressen enthalten. Ordnen Sie den speziellen bzw. einschränkenden Access Templates eine höhere Priorität zu und kennzeichnen Sie die Access Template der niedrigsten Priorität mit „ANY - Deny All settings“.

Testen von Access Templates auf korrekte Enforcement-Einstellungen

Tipp	Beschreibung
<p>Nehmen Sie Access Templates in eine Richtlinie auf, um herauszufinden, ob einem Endpoint die richtige Access Template zugeordnet wurde.</p> <p>Weitere Informationen zum Testen von Richtlinien oder Einführen von Sophos NAC finden Sie unter Implementierung von Network Access Control (Seite 3).</p>	<p>Überprüfen Sie in jeder Access Template, ob für die Access States die richtigen Durchsetzungsmaßnahmen (Enforcement Actions) eingerichtet sind. Überprüfen Sie, ob die Exemptions tatsächlich ausgeschlossen sind. Im Agent Enforcer-, DHCP Enforcer- oder DHCP Exemption-Report von NAC Manager erfahren Sie, welche Access Template aus welchem Grund einem Endpoint zugeordnet wurde und welche Durchsetzungsmaßnahme ergriffen wurde.</p>

3.2 Erstellen von Agent Enforcer Access Templates

In Agent Enforcer Access Templates wird der Zugriffsstatus aller Endpoints auf Netzwerkressourcen während der Durchführung einer clientbasierten Quarantäne-Durchsetzung verzeichnet. Agent Enforcer Access Templates gelten nur für Endpoints, auf denen der Quarantine Agent läuft.

Die in der Agent Enforcer Access Template festgelegten Netzwerkressourcen regeln den Netzwerkzugriff des Endpoints. Wenn ein Endpoint beispielsweise mit einer bestimmten Richtlinie nicht konform ist, wird die dem Konformitätszustand der Richtlinie zugeordnete Agent Enforcer Access Template übertragen, woraufhin Netzwerkressourcen entweder zugelassen oder abgewiesen werden. Weitere Informationen zu Netzwerkressourcen finden Sie unter [Erstellen von Netzwerkressourcen](#) (Seite 53). Wenn Sie eine Access Template erstellt haben, lässt sie sich Richtlinien zuweisen. Weitere Informationen finden Sie unter [Aktualisieren von Richtlinien](#) (Seite 16).

Vorgehensweise

1. Klicken Sie auf **Enforce > Agent Enforcer Access Templates** . Klicken Sie unten links auf der Seite auf **Create Agent Enforcer Access Template**.
2. Geben Sie einen Namen und eine Beschreibung für die Agent Enforcer Access Template ein.
3. Markieren Sie das Kontrollkästchen neben den Konformitätszuständen der Templates, um zu bestimmen, wie die Agent Enforcer Access Template zugewiesen oder für die Auswahl in den Richtlinien gekennzeichnet werden soll.

4. Führen Sie einen der folgenden Schritte aus:
 - Klicken Sie auf **Select**, um einer Access Template vorhandene Netzwerkressourcen zuzuordnen, wählen Sie die entsprechenden Netzwerkressourcen und klicken Sie auf **OK**.
 - Klicken Sie auf **Create**, um für die Access Template neue Netzwerkressourcen einzurichten, füllen Sie die Felder mit den erforderlichen Informationen aus und klicken Sie auf **Save**. Wiederholen Sie diesen Schritt, wenn Sie weitere Netzwerkressourcen für die Access Template erstellen möchten. Weitere Informationen finden Sie unter [Erstellen von Netzwerkressourcen](#) (Seite 53).
5. Wählen Sie das Zugriffsverhalten für jede Netzwerkressource. Es gibt folgende Optionen:
 - **Deny**: Weist jeglichen vom Endpoint abgehenden, an die Netzwerkressource gerichteten Datenverkehr ab.
 - **Permit**: Lässt jeglichen vom Endpoint abgehenden, an die Netzwerkressource gerichteten Datenverkehr zu.
6. Ändern Sie bei Bedarf die Prioritätsstufe der Netzwerkressourcen anhand der Pfeile.

Wenn einem Endpoint mehr als eine Netzwerkressource zugewiesen ist, bestimmt die erste passende Netzwerkressource den Netzwerkzugriff für die Endpoint-Sitzung. Es empfiehlt sich, speziellen bzw. einschränkenden Netzwerkressourcen eine höhere Priorität zuzuordnen als allgemeineren Netzwerkressourcen. Ausführbare Netzwerkressourcen werden vor Port-/Protokoll-Netzwerkressourcen analysiert.
7. Klicken Sie auf **Save**.

Hinweis: Klicken Sie auf den Link **View Template Details**, um die nach Priorität sortierten Anwendungen und Netzwerkressourcen in Zusammenhang mit der Agent Enforcer Access Template anzuzeigen. Wenn die Agent Enforcer Access Template erstellt ist, können Sie über ein Rechtsklickmenü auf der **Agent Enforcer Access Template**-Listenseite oder beim Bearbeiten der Vorlage durch Klicken auf den Link **View Usage Details** die Richtlinien anzeigen, die auf dieser Vorlage basieren.

3.3 Erstellen von DHCP Enforcer Access Templates

Mit DHCP Enforcer Access Templates können Sie die zur Unterstützung von DHCP-Durchsetzung erforderlichen Zugriffsdaten festlegen. DHCP Enforcer Access Templates kommen nur bei Sophos NAC DHCP-Implementierungen zum Einsatz.

Zur ersten Konfiguration des DHCP Enforcers empfiehlt sich der DHCP Configuration Wizard. Weitere Informationen finden Sie unter [Der DHCP Configuration Wizard](#) (Seite 51). Bei umfangreicheren DHCP-Konfigurationen können Sie entweder neue DHCP Enforcer Access Templates erstellen oder vorhandene übernehmen.

Die in der DHCP Enforcer Access Template festgelegten Netzwerkressourcen regeln den Netzwerkzugriff des Endpoints. Wenn ein Endpoint beispielsweise mit einer bestimmten Richtlinie nicht konform ist, wird die dem Konformitätszustand der Richtlinie zugeordnete DHCP Enforcer Access Template, die mit der IP-Adresse des DHCP-Servers oder des DHCP-Relays übereinstimmt, übertragen, woraufhin Netzwerkressourcen entweder zugelassen oder abgewiesen werden. Weitere Informationen zu Netzwerkressourcen finden Sie unter

[Erstellen von Netzwerkressourcen](#) (Seite 53). Wenn Sie eine Access Template erstellt haben, lässt sie sich Richtlinien, Ausnahmen und Enforcer-Einstellungen zuweisen. Mehr dazu erfahren Sie unter [Aktualisieren von Richtlinien](#) (Seite 16), [Erstellen von Ausnahmen](#) (Seite 55) und [Festlegen von Enforcer-Einstellungen](#) (Seite 81).

Vorgehensweise

1. Klicken Sie auf **Enforce > DHCP Enforcer Access Templates** . Klicken Sie links unten auf der Seite auf **Create DHCP Enforcer Access Template**.
2. Geben Sie einen Namen und eine Beschreibung für die DHCP Enforcer Access Template ein.
3. Markieren Sie das Kontrollkästchen neben den Konformitätszuständen der Templates, um zu bestimmen, wie die DHCP Enforcer Access Template zugewiesen oder für die Auswahl in der Richtlinie, den Ausnahmen und den Enforcer-Einstellungen gekennzeichnet werden soll.
4. Wählen Sie **Full Access**, um Endpoints Vollzugriff auf das Netzwerk zu gewähren. Wenn nur bestimmte Netzwerkressourcen freigegeben werden sollen, wählen Sie **Restricted** (Eingeschränkter Zugriff). Wenn Sie den Zugriff einschränken, geben Sie lediglich den Zugriff auf die angegebenen Netzwerkressourcen, den NAC-Server und den Dissolvable Agent-Server frei. Der Zugriff auf andere Ressourcen ist gesperrt.
5. Wenn Sie im vorigen Schritt eingeschränkten Zugriff gewählt haben, können Sie das Kontrollkästchen **Prevent LAN Access** (LAN-Zugriff verhindern) auswählen. Durch diese Option wird Endpoints der Zugriff auf das lokale Netzwerk (LAN) verweigert. Führen Sie ferner einen der folgenden Schritte durch, um die Netzwerkressourcen anzugeben, auf die zugegriffen werden darf:
 - Klicken Sie auf **Select**, um einer Access Template vorhandene Netzwerkressourcen zuzuordnen, wählen Sie die entsprechenden Netzwerkressourcen und klicken Sie auf **OK**. Es stehen nur Port-/Protokoll-Netzwerkressourcen mit bestimmten IP-Adressenbereichen (nicht ANY) zur Auswahl.
 - Klicken Sie auf **Create**, um für die Access Template neue Netzwerkressourcen einzurichten, füllen Sie die Felder mit den erforderlichen Informationen aus und klicken Sie auf **Save**. Wiederholen Sie diesen Schritt, wenn Sie weitere Netzwerkressourcen für die Access Template erstellen möchten. Weitere Informationen finden Sie unter [Erstellen von Netzwerkressourcen](#) (Seite 53).

Wichtig: Wenn Sie keinen Proxyserver für den Internetzugang als Netzwerkressource festlegen, können Benutzer nicht auf das Internet zugreifen und die Standard-DHCP (Internet Access DHCP Enforcer Access Template) bietet nur Korrekturzugang. Weitere Informationen finden Sie unter [Der DHCP Configuration Wizard](#) (Seite 51).

Hinweis: Wenn Sophos Enterprise Console auf einem anderen Server als Sophos NAC installiert wurde, müssen Sie eine Netzwerkressource für den Sophos Enterprise Console-Server erstellen und ihn Ihrer DHCP Enforcer Access Template zuweisen, um den Zugang darauf zu gewähren.

Hinweis: Jede DHCP Enforcer Access Template gestattet eine bestimmte Anzahl von Host-Routen und Netzwerk-Routen, die durch die IP-Adresse/-Subnetz-Ziele in den Netzwerkressourcen festgelegt werden. Wenn der Grenzwert überschritten wird, können Sie dieses Problem durch Löschen der Netzwerkressourcen aus der Access Template oder durch Löschen der Routen aus den Netzwerkressourcen in der Access Template beheben.

6. Über **Advanced Options** (unten links auf der Seite) können Sie weitere DHCP-Optionen auswählen. Es stehen folgende erweiterte Optionen zur Auswahl:

- **User Class:** Diese Option ermöglicht die Übernahme der Benutzerklasse des DHCP-Clients oder die Ersetzung durch eine andere Benutzerklasse. Sie können den DHCP-Server für die Vergabe von IP-Adressen basierend auf der Benutzerklasse konfigurieren. Die Benutzerklasse wird Endpoints vor der Zuweisung der IP-Adresse basierend auf dem Konformitätszustand des Endpoints, dem die Vorlage zugewiesen ist, zugewiesen.

Wichtig:

- Die Benutzerklasse erfordert ein alphanumerisches Format, bei dem zwischen Groß- und Kleinschreibung unterschieden wird. Sie muss einer DHCP-Benutzerklasse auf dem DHCP-Server entsprechen.
- Wenn der Quarantine Agent bei der Eingabe einer -Benutzerklasse die Richtlinie noch nicht nach dem Policy Refresh Interval angerufen hat, verwendet der Agent nicht die jeweilige Benutzerklasse und kann die entsprechenden IP-Adressen so lange nicht abrufen, bis die entsprechende Richtlinie abgerufen ist.
- **Lease Duration:** Mit dieser Option können Sie entweder die Lease-Einstellungen des DHCP-Servers übernehmen oder besondere Lease-Einstellungen auswählen.
- **DNS Servers:** Über diese Option wählen Sie primäre und sekundäre DNS-Server aus. Die Option ist nur für Eigenportale erforderlich. Unbekannte Benutzer oder Besucher können basierend auf dem Konformitätszustand ihres Endpoints an DNS-Server weitergeleitet werden.
- **DHCP Server IP Scopes:** Hier können Sie die IP-Bereiche angeben, für die die Access Template gelten soll. Markieren Sie das Kontrollkästchen **ANY** oder geben Sie die Start- und End-IP-Adresse des IP-Bereichs in die entsprechenden Felder ein und klicken Sie auf **Add**. Wiederholen Sie diesen Schritt für weitere DHCP-Bereiche.

7. Klicken Sie auf **Save**.

Hinweis: Wenn die DHCP Enforcer Access Template erstellt ist, können Sie über ein Rechtsklickmenü auf der **DHCP Enforcer Access Templates**-Listenseite oder beim Bearbeiten der Vorlage durch Klicken auf den Link **View Usage Details** die Richtlinien, Ausnahmen und Enforcer-Einstellungen anzeigen, die auf dieser Vorlage basieren.

3.4 Der 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. Wenn mit dem Assistenten Einstellungen ändern, wird die derzeitige DHCP-Konfiguration überschrieben. Die in den voreingestellten DHCP Enforcer Access Templates angegebenen Server werden durch die im Assistenten angegebenen Server ersetzt.

Weitere Informationen zur Konfiguration von DHCP Enforcement finden Sie in der *Sophos NAC DHCP Konfigurationsanleitung*.

Vorgehensweise

1. Klicken Sie auf **Configure System > DHCP Configuration Wizard** . Klicken Sie auf **Weiter**.
2. 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 4 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.

3. 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.

4. 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.

5. 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 **No** und anschließend auf **Next**. Fahren Sie mit Schritt 7 fort.

Hinweis: Wenn der Dissolvable Agent auf dem gleichen Server wie Sophos NAC installiert ist, müssen Sie keinen weiteren Dissolvable Agent-Server erstellen.

6. 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 Dissolvable Agent-Serverdaten ein und klicken auf **OK**. Klicken Sie auf **Next**. Nach der Einrichtung können diese Server im Bereich **Configure System > Server Settings** verwaltet werden.
7. 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.
8. Klicken Sie auf **Finish**.

Hinweis: Standardmäßig sind neue DHCP Enforcer-Server so eingestellt, dass sie Zugriffe durch unbekannte Endpoints lediglich melden. Um den Netzwerkzugriff für unbekannte Endpoints zu durchzusetzen, muss der unbekannte Endpoint-Modus für jeden DHCP-Enforcer-Server im Bereich **Configure System > Server Settings** auf **Enforce** gestellt werden. Weitere Informationen finden Sie unter [Erstellen von DHCP-Enforcer-Servern](#) (Seite 83).

Hinweis: Die Richtlinien sind standardmäßig nur auf das Melden von Endpoint-Zugriffen eingestellt. Um den Netzwerkzugriff für verwaltete oder nicht verwaltete Endpoints durchzusetzen, muss der Richtlinienmodus für jede Richtlinie im Bereich **Manage > Policies** auf **Enforce** gestellt werden. Weitere Informationen finden Sie unter [Aktualisieren von Richtlinien](#) (Seite 16).

3.5 Erstellen von Netzwerkressourcen

Bei Netzwerkressourcen handelt es sich um Anwendungen oder Geräte, die zur Korrektur von Endpoints erforderlich sind oder auf die Endpoints in Quarantäne keinen Zugriff erhalten sollen. Zum Beispiel können Sie Zugriff für Virenschutzanwendungen oder auf Dateiserver gewähren, die diese Anwendungen beherbergen. Oder Sie können Unternehmens-E-Mail-Anwendungen bzw. -Geräte im Netzwerk, die öffentliche IP-Adressen verwenden, sperren. Netzwerkressourcen können zu Agent Enforcer oder DHCP Enforcer Access Templates hinzugefügt werden. Die Access Templates können dann den Richtlinien zugewiesen werden, um je nach dem Access State des Endpoints Zugriff freizugeben oder zu verweigern.

Vorgehensweise

1. Klicken Sie auf **Enforce > Network Resources** . Klicken Sie links unten auf der Seite auf **Create Network Resource**.
2. Geben Sie einen Namen und eine Beschreibung für die Netzwerkressource ein.

3. Klicken Sie auf das Listenfeld **Network Resource Type** und wählen Sie entweder **Port/Protocol** oder **Executable**.

Bei ausführbaren Netzwerkressourcen in Agent Enforcer Access Templates analysiert der Agent vom Endpoint ausgehenden Datenverkehr, um zu ermitteln, welche Prozesse zugelassen oder abgewiesen werden sollen. Bei Port-/Protokoll-Netzwerkressourcen in Agent Enforcer Access oder DHCP Enforcer Access Templates analysiert der Agent Enforcer bzw. der DHCP Enforcer die Ziele, auf die der Endpoint Zugriff erhalten soll.

Hinweis: Für jede ausführbare Anwendungsdatei müssen Sie eine separate Netzwerkressource erstellen.

Hinweis: Für DHCP Enforcement stehen nur Port-/Protokoll-Netzwerkressourcen zur Auswahl.

4. Führen Sie einen der folgenden Schritte aus:

- Wenn Sie in Schritt 3 **Port/Protocol** gewählt haben, wählen Sie die Server-Kategorie aus der Liste **Server Category**. Klicken Sie auf die Option **ANY**, um eine Netzwerkressource zu erstellen, die für beliebige Ports gilt, oder klicken Sie auf die Option neben dem entsprechenden Feld und geben Sie einen spezifischen Port in das Feld ein. Wählen Sie das Protokoll aus und klicken Sie auf **Add**. Wiederholen Sie diesen Schritt ggf. für weitere Ports und Protokolle.
- Wenn Sie in Schritt 3 **Executable** ausgewählt haben, geben Sie in das Feld **Name** den Namen des ausführbaren Prozesses der Anwendung ein.

Wichtig:

- Der Name des ausführbaren Prozesses **muss** dem im Windows Task Manager unter **Prozesse** angezeigten Namen entsprechen.
 - Solange ein Prozessname keine Erweiterung enthält, **müssen** Namen von ausführbaren Dateien eine **.exe**-Erweiterung erhalten. Ihre Länge **darf nicht** 64 Zeichen überschreiten, und folgende Zeichen dürfen **nicht** verwendet werden: \ / : * ? " < > und |. Ferner darf der Name **nicht** den Dateipfad enthalten. Die Eingabe von Platzhaltern ist **nicht** zulässig. Die Namen werden **nur** von TCP- und UDP-Protokollen unterstützt.
 - Die Software erkennt nur ausführbare Dateien auf der Winsock-Ebene.
5. Sie können auch einen Zielserver angeben. Wählen sie dazu **IP Address** oder **Host Name** und geben Sie die IP-Adresse, das Subnetz (optional), eine Beschreibung oder den Hostnamen plus Beschreibung in die entsprechenden Felder ein. Klicken Sie anschließend auf **Add**.

Wiederholen Sie diesen Schritt ggf. für weitere IP-Adressen und -Subnetze oder Hostnamen.

Wichtig: Netzwerkressourcen, deren Subnetzmaske **nicht** 255.255.255.255 entspricht und die in DHCP Enforcer Access Templates vorkommen, verweigern Endpoints unter Windows 2000 den Zugriff.

6. Klicken Sie auf **Save**.

Hinweis: Wenn die Netzwerkressource erstellt ist, können Sie über ein Rechtsklickmenü auf der **Network Resources**-Listenseite oder beim Bearbeiten der Netzwerkressource durch Klicken auf den Link **View Usage Details** die Access Templates anzeigen, die sich dieser Netzwerkressource bedienen.

3.6 Erstellen von Ausnahmen

Auf der Seite **Exemptions** (Ausnahmen) können Sie Endpoints, die bei Verbindung mit dem Netzwerk nicht auf Konformität überprüft werden müssen, anhand diverser Kriterien identifizieren. Hierzu zählen Endpoints, auf denen entweder der Agent nicht ausgeführt werden kann (z.B. Endpoints, die nicht unter Windows laufen), oder für die keine Konformitätsprüfung erforderlich ist – z.B. Server, Router und Drucker. Wenn Sie Richtlinien im Unternehmen schrittweise durchsetzen möchten, können Sie Endpoints oder Netzwerke ausnehmen, die noch nicht einbezogen werden sollen.

Hinweis: Exemptions betreffen ausschließlich DHCP Enforcement.

3.7 Erstellen von DHCP-Ausnahmekriterien

Auf der Seite **Exemptions** können Sie Endpoints identifizieren, die bei Verbindung mit dem Netzwerk nicht auf Konformität überprüft werden. 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. Nachdem Sie Exemptions erstellt haben, können Sie ihnen auf der Listenseite **Exemptions** eine Prioritätsstufe zuordnen.

Vorgehensweise

1. Klicken Sie auf **Enforce > Exemptions** . Klicken Sie links unten auf der Seite auf **Create Exemption**.
2. Geben Sie einen Namen und eine Beschreibung für die Exemption ein.
3. Zum Deaktivieren dieser Exemption markieren Sie das Kontrollkästchen **Disable Exemption**.

Durch das Deaktivieren einer Exemption wird der Endpoint auf Konformität überprüft. Wenn eine Exemption deaktiviert ist und auf dem Endpoint nicht Sophos Compliance Agent installiert ist, wird der Endpoint als unbekannt eingestuft.

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 unter **Access Templates** auf **Select**, um der Exemption DHCP Enforcer Access Templates zuzuordnen. Wählen Sie die gewünschten Vorlagen und klicken Sie auf **OK**.
Wenn die gewünschte DHCP Enforcer Access Template nicht aufgeführt wird, erstellen Sie eine neue. Weitere Informationen finden Sie unter [Erstellen von DHCP Enforcer Access Templates](#) (Seite 49).
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.

3.8 Erstellen von Exemptions nach IP-Bereichen

Auf der Seite Exemptions können Sie Endpoints anhand von IP-Bereichen identifizieren, die bei Verbindung mit dem Netzwerk nicht auf Konformität überprüft werden. Bei Exemptions nach IP-Bereichen (IP Scope Exemptions) handelt es sich um Exemptions, die für Netzwerksegmente erstellt werden. In den zugehörigen DHCP Enforcer Access Templates sind sowohl die IP-Bereiche als auch die jeweiligen Netzwerkzugriffsrechte festgelegt. Ausnahmen nach IP-Bereichen sind hilfreich, wenn Sie Richtlinien im Unternehmen schrittweise durchsetzen möchten. Sie können Endpoints oder Netzwerke ausnehmen, die noch nicht einbezogen werden sollen. Nachdem Sie Exemptions erstellt haben, können Sie ihnen auf der Listenseite **Exemptions** eine Prioritätsstufe zuordnen.

Vorgehensweise

1. Klicken Sie auf **Enforce > Exemptions**. Klicken Sie links unten auf der Seite auf **Create Exemption**.
2. Geben Sie einen Namen und eine Beschreibung für die Exemption ein.
3. Zum Deaktivieren dieser Exemption markieren Sie das Kontrollkästchen **Disable Exemption**.

Durch das Deaktivieren einer Exemption wird der Endpoint auf Konformität überprüft. Wenn eine Exemption deaktiviert ist und auf dem Endpoint nicht Sophos Compliance Agent installiert ist, wird der Endpoint als unbekannt eingestuft.

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. Weitere Informationen finden Sie unter [Erstellen von DHCP Enforcer Access Templates](#) (Seite 49).
6. Ändern Sie bei Bedarf die Prioritätsstufe der Bereiche anhand der Pfeile.
Wenn mehr als ein Bereich auf eine Ausnahme zutrifft, wird der erste Bereich verwendet. Es empfiehlt sich, speziellen bzw. einschränkenden Bereichen eine höhere Priorität zuzuordnen als allgemeineren Bereichen.

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.

3.9 Deaktivieren/Aktivieren von Exemptions

Bei der Erstellung einer Exemption wird sie automatisch aktiviert. Sie kann jedoch auf Ihren Wunsch hin deaktiviert werden. Durch das Deaktivieren einer Exemption wird der Endpoint auf Konformität überprüft. Wenn eine Exemption deaktiviert ist und auf dem Endpoint nicht Sophos Compliance Agent installiert ist, wird der Endpoint als unbekannt eingestuft.

Vorgehensweise

1. Klicken Sie auf **Enforce > Exemptions**.
2. Klicken Sie neben der zu aktivierenden/deaktivierenden Exemption auf die **Status**-Liste und klicken Sie auf **Enabled** oder **Disabled**.

Hinweis: Wenn Sie eine vorhandene Exemption verwenden möchten, z.B. einen Drucker, setzen Sie den Status auf **Enabled**.

3. Klicken Sie auf **Save**.

4 Report-Bereich im Überblick

Der Report-Bereich enthält alle Komponenten zur Verwaltung von Compliance Reports und Troubleshooting Reports. Die im Folgenden aufgeführten Bereiche erreichen Sie über das Report-Menü:

Bereich und Aktion	Beschreibung
Compliance Reports	
Anhand von Compliance Reports können Sie die Richtlinien-übereinstimmung des Endpoints nachverfolgen.	<p>Compliance Reports bestehen aus Compliance Detail Reports und Compliance Summary Reports.</p> <ul style="list-style-type: none"> Die Compliance Reports umfassen Details zur allgemeinen Richtlinienkonformität von Endpoints und High-Level-Gesamtwerte der in einem bestimmten Zeitraum mit Richtlinien übereinstimmenden Endpoints. Die Prüfungsdetails des Compliance Detail Reports enthalten nähere Informationen zur Konformitätsprüfung auf einem Endpoint.
Troubleshooting Reports	
Anhand von Troubleshooting Reports können Sie Zugriffs-, Richtlinien-übereinstimmungs-, Quarantäne- und Ausnahmen-Probleme einkreisen.	<p>Troubleshooting Reports bestehen aus Agent Session, Non-Compliance Detail, Agent Enforcer, DHCP Enforcer und DHCP Exemption Reports.</p> <ul style="list-style-type: none"> Agent Session Report zeigt alle Agenten-Sitzungen und Überprüfungen an, die in einem bestimmten Zeitraum auf dem Endpoint durchgeführt wurden. Non-Compliance Detail Report enthält Angaben darüber, welche Endpoints nicht richtlinienkonform sind. Der Agent Enforcer Report zeigt Netzwerkzugriff durch Agent Quarantine Enforcement an, der in einem bestimmten Zeitraum erfolgt ist. Der DHCP Enforcer Report zeigt Netzwerkzugriff durch DHCP Enforcement an, der in einem bestimmten Zeitraum erfolgt ist. Der DHCP Exemption Report zeigt DHCP-Exemptions an, die in einem bestimmten Zeitraum aufgetreten sind. Prüfungsdetails werden in folgenden Reports festgehalten: Agent Session, Non-Compliance Detail, Agent Enforcer und DHCP Enforcer Troubleshooting. Die Prüfungsdetails in den Reports enthalten nähere Informationen zur Konformitätsprüfung auf einem Endpoint.
Gespeicherte Reports	
Anhand von gespeicherten Reports können Sie ganz einfach Reports neu erstellen.	Anhand von Saved Reports können Sie allgemeine Report-Einstellungen speichern und wiederverwenden, damit Sie nicht dieselben Kriterien neu eingeben müssen. Jede Report-Konfiguration kann gespeichert und später als Saved Report wiederverwendet werden.
Audits	

Bereich und Aktion	Beschreibung
Audits enthalten Update-Informationen zu Systemereignissen.	Audits ermöglichen eine Audit-Nachverfolgung oder den Verlauf von Ereignissen, die im System stattgefunden haben. Zu Ereignissen können Updates, neue Elemente oder Systemaktivitäten zählen, z.B. Updates auf aktuelle Richtlinien, Erstellung neuer Access Templates oder Konten, die sich am NAC Manager an- bzw. abmelden.

4.1 Drucken von Reports

Sie können einen erstellten Report oder einen bestimmten Report-Eintrag ausdrucken.

Vorgehensweise

1. Klicken Sie auf **Report > Compliance or Troubleshooting**.
2. Klicken Sie auf das Listenfeld **Report Type** und wählen Sie den Namen des auszudruckenden Reports.
3. 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. Im Verlauf 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 **Computer Name** *M** oder *M%* eingeben, werden alle mit „M“ beginnenden Computernamen angezeigt. Wenn Sie dagegen in das Feld **Computer Name** nur *M* ohne * oder % eingeben, wird nur der Computer namens „M“ angezeigt.

4. Klicken Sie auf **Run**.
5. Klicken Sie auf **Drucken**.

4.2 Erstellen von Compliance Reports

Anhand von Compliance Reports können Sie die Endpoints identifizieren, bei denen in einem bestimmten Zeitraum Richtlinienkonformität gegeben ist. Mit Compliance Reports können Sie Trends in der Konformität erkennen. Es wird zwischen zwei Arten von Compliance Reports unterschieden:

- **Compliance Detail:** Dieser Report gibt Aufschluss darüber, welche Endpoints in einem bestimmten Zeitraum, basierend auf der letzten Agentensitzung des Endpoints, Richtlinienkonformität aufweisen. Die Analyse-Details können Sie im Compliance Detail Report abrufen.
- **Compliance Summary:** Dieser Report enthält die Gesamtwerte der richtlinienkonformen Endpoints in einem bestimmten Zeitraum.

Vorgehensweise

1. Klicken Sie auf **Report > Compliance**.

2. Klicken Sie auf das Listenfeld **Report Type** und wählen Sie **Compliance Detail** oder **Compliance Summary**.
3. 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. Im Verlauf 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 **Computer Name** *M** oder *M%* eingeben, werden alle mit „M“ beginnenden Computernamen angezeigt. Wenn Sie dagegen in das Feld **Computer Name** nur *M* ohne * oder % eingeben, wird nur der Computer namens „M“ angezeigt.

4. Klicken Sie auf **Run**.

Weitere Informationen zu den Ergebnisfeldern entnehmen Sie bitte der folgenden Tabelle.

Beschreibung der Felder

Hinweis: Der Compliance Summary Report enthält nicht alle im Folgenden aufgeführten Felder. Die Nummern in den Feldern des Compliance Summary Reports geben die Anzahl der Instanzen eines bestimmten Objekts an.

Feld	Beschreibung
Compliance State	Der dem Endpoint bei der Konformitätsprüfung zugewiesene Konformitätszustand. Weitere Informationen finden Sie unter Ermitteln des Konformitätszustands (Seite 43). 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.
Policy Name	Name der Richtlinie, die vom Agenten analysiert wurde.
Policy Version	Version der Richtlinie, die vom Agenten analysiert wurde. Die neueste Version wird als Latest entsprechend gekennzeichnet. Hinweis: Mit jeder Änderung der Richtlinie wird die Versionsnummer jeweils um 1 erhöht.
Computer Name	Name des Endpoints, auf dem der Agent installiert ist.
Agent ID	Kennung der Agenten-Installation oder des Endpoints, auf dem die Sitzung gestartet wurde. Hinweis: Die Agent ID ist ein von der Software generierter GUID, der jede Agenten-Installation eindeutig kennzeichnet.
Last Assessment Date/Time	Datum und Zeit der letzten Konformitätsüberprüfung innerhalb des im Report angegebenen Zeitintervalls. Zur Überprüfung gehören die Operationen, die Richtlinien auf dem Endpoint analysieren und durchsetzen. Die Häufigkeit einer Überprüfung richtet sich nach dem hinter „Assess and Enforce Interval“

Feld	Beschreibung
	<p>der Richtlinie angegebenen Wert. Drei Striche hintereinander (---) deuten darauf hin, dass die Agentensitzung das angegebene Zeitintervall überschritten hat.</p> <p>Hinweis: Datum und Uhrzeit werden von der Zeitzone des Webbrowsers abgeleitet, der auf NAC Manager zugreift.</p>
Associated Reports	<p>Durch Anklicken des hier dargestellten Symbols erfahren Sie Näheres über die Konformitätsprüfung, die mit diesem Compliance Detail-Eintrag in Zusammenhang steht. Weitere Informationen finden Sie unter Anzeigen von Assessment Details (Seite 73).</p>

4.3 Erstellen des Agent Session Reports

Der Agent Session Report zeigt alle Agenten-Sitzungen und Überprüfungen an, die in einem bestimmten Zeitraum auf dem Endpoint durchgeführt wurden. Dieser Report ist zur Behebung von Netzwerkzugriffs- und Konformitätsproblemen nützlich. Dieser Report enthält nähere Informationen über die Agenten-Sitzung auf dem Endpoint, die auf dem Endpoint durchgeführten Konformitätsprüfungen und Änderungen des Konformitätszustands. Sie können verwandte Agent Enforcer Einträge, DHCP Enforcer Einträge oder die Prüfungsdetails des Agent Session Reports anzeigen.

Hinweis: Da Echtzeitdaten aus mehreren Quellen stammen und zusammengeführt werden müssen, können Daten in einigen Fällen unvollständig sein.

Vorgehensweise

1. Klicken Sie auf **Report > Troubleshooting**.
2. Klicken Sie auf das Listenfeld **Report Type** und wählen Sie **Agent Session**.
3. 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. Im Verlauf 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 **Computer Name** *M** oder *M%* eingeben, werden alle mit „M“ beginnenden Computernamen angezeigt. Wenn Sie dagegen in das Feld **Computer Name** nur *M* ohne * oder % eingeben, wird nur der Computer namens „M“ angezeigt.

4. Klicken Sie auf **Run**.

Weitere Informationen zu den Ergebnisfeldern entnehmen Sie bitte der folgenden Tabelle.

Beschreibung der Felder

Feld	Beschreibung
Summary Report	
Computer Name	Name des Endpoints, auf dem der Agent installiert ist.
Agent ID	Kennung der Agenten-Installation oder des Endpoints, auf dem die Sitzung gestartet wurde. Hinweis: Die Agent ID ist ein von der Software generierter GUID, der jede Agenten-Installation eindeutig kennzeichnet.
MAC Address	MAC-Adressen des Endpoints, auf dem der Agent installiert ist. Im Report wird jede MAC-Adresse derselben Netzwerkkarte wie der IP-Adresse daneben zugewiesen.
IP-Adresse	IP-Adressen des Endpoints, auf dem der Agent installiert ist. Im Report wird jede IP-Adresse derselben NIC wie der MAC-Adresse daneben zugewiesen. Drei Striche (---) deuten darauf hin, dass die Netzwerkkarte (NIC) keine IP-Adresse aufweist.
Betriebssystem	Das auf dem Endpoint installierte Betriebssystem.
Session Start	Datum und Uhrzeit, an denen der Agent auf einem Endpoint eine Sophos Sophos NAC-Sitzung startet. Hinweis: Datum und Uhrzeit werden von der Zeitzone des Webbrowsers abgeleitet, der auf NAC Manager zugreift.
Session End	Datum und Uhrzeit, an denen der Agent auf einem Endpoint eine Sophos Sophos NAC-Sitzung endet. Drei Striche (---) deuten darauf hin, dass die Agentensitzung noch nicht beendet ist. Hinweis: Datum und Uhrzeit werden von der Zeitzone des Webbrowsers abgeleitet, der auf NAC Manager zugreift.
Detailed Report	
Assessment Start	Datum und Uhrzeit der ersten Instanz des Konformitätsüberprüfungsergebnisses innerhalb des im Report angegebenen Zeitintervalls. Zur Überprüfung gehören die Operationen, die Richtlinien auf dem Endpoint analysieren und durchsetzen. Die Häufigkeit einer Überprüfung richtet sich nach dem hinter „Assess and Enforce Interval“ der Richtlinie angegebenen Wert. Hinweis: Datum und Uhrzeit werden von der Zeitzone des Webbrowsers abgeleitet, der auf NAC Manager zugreift.
Assessment End	Datum und Uhrzeit der letzten Instanz des Konformitätsüberprüfungsergebnisses innerhalb des im Report angegebenen Zeitintervalls. Zur Überprüfung gehören die Operationen, die Richtlinien auf

Feld	Beschreibung
	dem Endpoint analysieren und durchsetzen. Drei Striche (---) deuten darauf hin, dass die Konformitätsprüfung noch nicht beendet ist. Hinweis: Datum und Uhrzeit werden von der Zeitzone des Webbrowsers abgeleitet, der auf NAC Manager zugreift.
Count	Anzahl der Konformitätsüberprüfungen mit unveränderten Prüfungsergebnissen. Dieser Wert gibt an, wie oft der Agent innerhalb des hinter „Assess and Enforce Interval“ angegebenen Intervalls eine Konformitätsüberprüfung durchgeführt hat.
Compliance State	Der dem Endpoint bei der Konformitätsprüfung zugewiesene Konformitätszustand. Weitere Informationen finden Sie unter Ermitteln des Konformitätszustands (Seite 43). 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.
Policy Name	Name der Richtlinie, die vom Agenten analysiert wurde.
Policy Version	Version der Richtlinie, die vom Agenten analysiert wurde. Die neueste Version wird als Latest entsprechend gekennzeichnet. Hinweis: Mit jeder Änderung der Richtlinie wird die Versionsnummer jeweils um 1 erhöht.
Associated Reports	Durch Anklicken des hier dargestellten Symbols öffnen Sie die Agent Enforcer-Einträge, DHCP Enforcer-Einträge oder erfahren Näheres über die Konformitätsprüfung, die mit diesem Agent Session-Eintrag in Zusammenhang steht. Es wird nur dann ein Symbol angezeigt, wenn es einen zugehörigen Eintrag gibt. Mehr dazu erfahren Sie unter Erstellen des Agent Enforcer Reports (Seite 65), Erstellen des DHCP Enforcer Reports (Seite 67) und Anzeigen von Assessment Details (Seite 73).

4.4 Erstellen des Non-Compliance Detail Reports

Anhand von Non-Compliance Detail Reports können Sie die Endpoints identifizieren, bei denen in einem bestimmten Zeitraum seit der letzten Agentensitzung keine Richtlinienkonformität oder nur Teilkonformität gegeben ist. Der Non-Compliance Detail Report hilft beim schnellen Auffinden von Endpoints, die nicht oder nur teilweise richtlinienkonform sind, und gibt Aufschluss über die Gründe für diesen Zustand. Die Analyse-Details können Sie im Non-Compliance Detail Report abrufen.

Hinweis: Da Echtzeitdaten aus mehreren Quellen stammen und zusammengeführt werden müssen, können Daten in einigen Fällen unvollständig sein.

Vorgehensweise

1. Klicken Sie auf **Report > Troubleshooting**.

2. Klicken Sie auf das Listenfeld **Report Type** und wählen Sie **Non-Compliance Detail**.
3. 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. Im Verlauf 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 **Computer Name** *M** oder *M%* eingeben, werden alle mit „M“ beginnenden Computernamen angezeigt. Wenn Sie dagegen in das Feld **Computer Name** nur *M* ohne * oder % eingeben, wird nur der Computer namens „M“ angezeigt.

4. Klicken Sie auf **Run**.

Weitere Informationen zu den Ergebnisfeldern entnehmen Sie bitte der folgenden Tabelle.

Beschreibung der Felder

Feld	Beschreibung
Summary Report	
Computer Name	Name des Endpoints, auf dem der Agent installiert ist.
Compliance State	Der dem Endpoint bei der Konformitätsprüfung zugewiesene Konformitätszustand. Weitere Informationen finden Sie unter Ermitteln des Konformitätszustands (Seite 43). Es gibt zwei Zustände: „Partially Compliant“ (teilweise konform) und „Non-Compliant“ (nicht konform). Drei Striche (---) deuten darauf hin, dass der Agent einen Compliance State nicht gemeldet hat.
Associated Reports	Durch Anklicken des hier dargestellten Symbols erfahren Sie Näheres über die Konformitätsprüfung, die mit diesem Non-Compliance Detail-Eintrag in Zusammenhang steht. Weitere Informationen finden Sie unter Anzeigen von Assessment Details (Seite 73).
Detailed Report	
Profile Name	Name des Profils, das der Agent auf dem Endpoint gesucht hat. Der zugehörige Profiltyp wird in Klammern angezeigt.
Capability	Die Fähigkeit des Profils, mit dem der Endpoint entweder teilweise oder vollständig konform ist.
Compliance State	Konformitätszustand, der nur im Report festgehalten wird, wenn die Bedingung auf dem Endpoint zutrifft. Es gibt zwei Zustände: „Partially Compliant“ (teilweise konform) und „Non-Compliant“ (nicht konform). Drei Striche (---) deuten darauf hin, dass der Agent einen Compliance State nicht gemeldet hat.

4.5 Erstellen des Agent Enforcer Reports

Im Agent Enforcer Report sind alle Netzwerkzugriffe durch Agent Quarantine Enforcement festgehalten, die über einen bestimmten Zeitraum stattgefunden haben. Anhand des Agent Enforcer Reports können Sie Quarantäne-Probleme auf Endpoints ausmachen und beheben. Dieser Report gibt Aufschluss über den Konformitätszustand von Endpoints, die zugehörige Access Template und den Grund für die Zuweisung einer bestimmten Access Template. Die Analyse-Details können Sie im Agent Enforcer Report abrufen.

Hinweis: Da Echtzeitdaten aus mehreren Quellen stammen und zusammengeführt werden müssen, können Daten in einigen Fällen unvollständig sein.

Vorgehensweise

1. Klicken Sie auf **Report > Troubleshooting**.
2. Klicken Sie auf das Listenfeld **Report Type** und wählen Sie **Agent Enforcer**.
3. 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. Im Verlauf 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 **Computer Name** *M** oder *M%* eingeben, werden alle mit „M“ beginnenden Computernamen angezeigt. Wenn Sie dagegen in das Feld **Computer Name** nur *M* ohne * oder % eingeben, wird nur der Computer namens „M“ angezeigt.

4. Klicken Sie auf **Run**.

Weitere Informationen zu den Ergebnisfeldern entnehmen Sie bitte der folgenden Tabelle.

Beschreibung der Felder

Feld	Beschreibung
Date/Time	Datum und Uhrzeit der Änderung des Durchsetzungszustands des Agent Enforcers. Hinweis: Datum und Uhrzeit werden von der Zeitzone des Webbrowsers abgeleitet, der auf NAC Manager zugreift.
Agent ID	Kennung der Agenten-Installation oder des Endpoints, zu der bzw. auf dem eine Änderung des Durchsetzungszustands gemeldet wurde. Hinweis: Die Agent ID ist ein von der Software generierter GUID, der jede Agenten-Installation eindeutig kennzeichnet.
Computer Name	Name des Endpoints, auf dem der Agent installiert ist.
Compliance State	Der dem Endpoint bei der Konformitätsprüfung zugewiesene Konformitätszustand. Weitere Informationen finden Sie unter Ermitteln des

Feld	Beschreibung
	<p><i>Konformitätszustands</i> (Seite 43). 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 Agent Enforcer Access Template, die der Richtlinie zugeordnet ist, bestimmt den Netzwerkzugriff.</p>
<p>Template Name (Version)</p>	<p>Name und Version der Access Template, in der die Maßnahme des Agent Enforcers festgelegt ist. Welche Access Template verwendet wird, richtet sich nach dem Grund (Reason). Weitere Informationen finden Sie unter Erstellen von Agent Enforcer Access Templates (Seite 48). Neben Ihren individuell erstellten Access Templates sind die folgenden Access Templates standardmäßig verfügbar:</p> <ul style="list-style-type: none"> ■ Default - Agent and Internet Access Only: Diese Access Template gibt in internen Netzwerken, die private IP-Adressen verwenden, den Zugriff auf Sophos Produkte und auf das Internet frei. Alle übrigen Datenbewegungen nach außen werden blockiert. ■ Default - Agent Permit All: Diese Access Template lässt jeglichen Datenverkehr nach außen zu. ■ None: Wenn die obigen beiden Access Templates aus der Richtlinie entfernt werden und keine unternehmensspezifische Template ausgewählt wurde, wird standardmäßig der gesamte Datenverkehr nach außen zugelassen. Dadurch ist gewährleistet, dass der Agent auf den NAC-Server zugreifen kann.
<p>Reason</p>	<p>Hier wird der Grund für die Zuweisung einer bestimmten Access Template durch Agent 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 Agent 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. ■ No Agent Tray: Der Agent läuft nicht auf dem Endpoint. Dieser Zustand kann von Agent Enforcer gemeldet werden, wenn der Benutzer nicht an Windows angemeldet ist oder das Programm „Agent Tray“ nicht mehr läuft. Die zu diesem Zustand gehörige Agent Enforcer Access Template der Richtlinie bestimmt den Netzwerkzugriff. ■ Policy Retrieval Error: Eine bestimmte Richtlinie konnte nicht für den Endpoint abgerufen werden. Dieser Zustand kann vorliegen, wenn der Agent eine Richtlinie nicht vom NAC-Server herunterladen kann oder der Konformitätszustand des Endpoints gemäß dem Feld Agent Policy Update Threshold (unter Configure System > Enforcer Settings) abgelaufen ist. ■ Remediate: Die Richtlinie befindet sich im Modus „Remediate“ (Korrektur). Die zu diesem Richtlinienmodus gehörige Agent Enforcer Access Template bestimmt 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 Agent Enforcer Access Template bestimmt den Netzwerkzugriff. ■ User Override: Der Benutzer hat die Quarantäne des Agenten auf dem Endpoint außer Kraft gesetzt. Die zu diesem Zustand gehörige Agent Enforcer Access Template der Richtlinie bestimmt den Netzwerkzugriff.

4.6 Erstellen des DHCP Enforcer Reports

Im DHCP Enforcer Report sind alle Netzwerkzugriffe durch DHCP Enforcement festgehalten, die über einen bestimmten Zeitraum stattgefunden haben. Der Report ist zur Behebung von Netzwerkzugriffsproblemen nützlich. Dieser Report gibt Aufschluss über den Konformitätszustand von Endpoints, die zugehörige Access Template und den Grund für die Zuweisung einer bestimmten Access Template. Über den DHCP Enforcer Report lassen sich Geräte ausschließen und Prüfungsdetails abrufen.

Hinweis: Da Echtzeitdaten aus mehreren Quellen stammen und zusammengeführt werden müssen, können Daten in einigen Fällen unvollständig sein.

Vorgehensweise

1. Klicken Sie auf **Report > Troubleshooting**.
2. Klicken Sie auf das Listenfeld **Report Type** und wählen Sie **DHCP Enforcer**.
3. 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. Im Verlauf 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.

4. Klicken Sie auf **Run**.

Weitere Informationen zu den Ergebnisfeldern entnehmen Sie bitte der folgenden Tabelle. Weitere Information zum Ausschließen von Geräten über diesen Report finden Sie unter [Erstellen von Exemptions über Reports](#) (Seite 72).

Beschreibung der Felder

Feld	Beschreibung
Summary Report	

Feld	Beschreibung
Date/Time	<p>Datum und Uhrzeit des versuchten Netzwerkzugriffs.</p> <p>Hinweis: Datum und Uhrzeit werden von der Zeitzone des Webbrowsers abgeleitet, der auf NAC Manager zugreift.</p>
MAC Address	<p>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.</p>
Computer Name	<p>Name des Geräts, durch das der Netzwerkzugriff versucht wurde. Der Computername wird automatisch über den Client Request ermittelt.</p>
Compliance State	<p>Der dem Endpoint bei der Konformitätsprüfung zugewiesene Konformitätszustand. Weitere Informationen finden Sie unter Ermitteln des Konformitätszustands (Seite 43). 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.</p>
Template Name (Version)	<p>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). Weitere Informationen finden Sie unter Erstellen von DHCP Enforcer Access Templates (Seite 49). Neben Ihren individuell erstellten Access Templates sind die folgenden Access Templates standardmäßig verfügbar:</p> <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. Weitere Informationen finden Sie unter Der DHCP Configuration Wizard (Seite 51).</p> <ul style="list-style-type: none"> ■ DHCP - Remediation Access: Sperrt den Zugriff auf das Netzwerk mit Ausnahme der festgelegten Korrekturserver, des NAC-Server- und des Dissolvable Agent-Servers.
Reason	<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.

Feld	Beschreibung
	<ul style="list-style-type: none"> ■ 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 Enforcers 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 Ausnahmekriterien 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. ■ 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

Feld	Beschreibung
	<p>Netzwerkzugriff vom DHCP-Server bestimmt, der keine Benutzerklasse zurückgibt und dem Benutzer den Zugriff verweigert.</p> <ul style="list-style-type: none"> ■ 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 derzeitig verwendeten IP-Adressen gestrichen. ■ Drei Striche (---): Der Agent hat keine Maßnahme angegeben.
Vendor Class	Herstellerklasse des DHCP-Clients.
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.

4.7 Erstellen des DHCP Exemption Reports

Im DHCP Exemption Report sind DHCP-Exemptions verzeichnet, die in einem bestimmten Zeitraum aufgetreten sind. Dieser Report ist zur Behebung von Zugriffsproblemen auf Netzwerke nützlich, die von der Konformitätsprüfung ausgenommen sind.

Hinweis: Da Echtzeitdaten aus mehreren Quellen stammen und zusammengeführt werden müssen, können Daten in einigen Fällen unvollständig sein.

Vorgehensweise

1. Klicken Sie auf **Report > Troubleshooting**.
2. Klicken Sie auf das Listenfeld **Report Type** und wählen Sie **DHCP Exemption**.
3. 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. Im Verlauf 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.

4. Klicken Sie auf **Run**.

Weitere Informationen zu den Ergebnisfeldern entnehmen Sie bitte der folgenden Tabelle.

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.
Template Name (Version)	Name der Access Template, in der die vom DHCP Enforcer durchgeführte Maßnahme festgelegt ist. Weitere Informationen finden Sie unter Erstellen von DHCP Enforcer Access Templates (Seite 49).
Exemption Condition Name	Name der Ausnahme und Ausnahmekriteriendetails.
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.
Returned User Class	Hierbei handelt es sich um die DHCP-Benutzerklasse, die vom DHCP Enforcer zur Durchsetzung an den DHCP-Server übermittelt wird.

Feld	Beschreibung
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	
Source User Class	DHCP-Benutzerklasse, die vom DHCP-Client an den DHCP-Server gesendet wird.
Vendor Class	Herstellerklasse des DHCP-Clients.
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.

4.8 Erstellen von Exemptions über Reports

Über den DHCP Enforcer Report lassen sich für Geräte, die beim DHCP Enforcement gemeldet wurden, Exemptions erstellen.

Exemptions werden im DHCP Enforcer Report unter ihrem „Exempted“-Grund aufgeführt. Wenn Sie ein im Report aufgeführtes Gerät ausschließen, wird es so lange nicht im Report als „exempted“ angezeigt, bis das Gerät erneut auf das Netzwerk zugreift. Der DHCP Enforcer Report wird ausführlich unter [Erstellen des DHCP Enforcer Reports](#) (Seite 67) beschrieben.

Vorgehensweise

1. Klicken Sie auf **Report > Troubleshooting**.
2. Klicken Sie auf das Listenfeld **Report Type** und wählen Sie **DHCP Enforcer**.
3. 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. Im Verlauf 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.

4. Klicken Sie auf **Run**.
5. Markieren Sie die Kontrollkästchen neben den auszuschließenden Geräten und klicken Sie auf **Exempt**.
6. Überprüfen Sie Ihre Auswahl, wählen Sie eine Access Template für die Exemptions und klicken Sie auf **OK**.

Weitere Access Templates können Sie im Bereich **Enforce > Exemptions** einrichten bzw. zuweisen. Weitere Informationen finden Sie unter [Erstellen von DHCP-Ausnahmekriterien](#) (Seite 55).

4.9 Anzeigen von Assessment Details

In den Assessment Details erhalten Sie ausführliche Informationen zu den Konformitätsprüfungen auf einem Endpoint.

Die Assessment Details können Sie in folgenden Reports abrufen. Compliance Detail, Agent Session, Non-Compliance Detail, Agent Enforcer oder DHCP Enforcer. Die angezeigten Assessment Details stehen mit dem Report-Eintrag in Zusammenhang, von dem aus die Details abgerufen werden. Assessment Details zeigen die Profilbedingungen an, die auf dem Endpoint getestet wurden, die Ergebnisse der getesteten Bedingungen, den Konformitätszustand nach der Überprüfung sowie jegliche Maßnahmen, die auf dem Endpoint durchgeführt wurden.

Vorgehensweise

1. Klicken Sie auf **Report > Compliance or Troubleshooting**.
2. Klicken Sie auf das Listenfeld **Report Type** und wählen Sie **Compliance Detail, Agent Session, Non-Compliance Detail, Agent Enforcer** oder **DHCP Enforcer**.
3. 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. Im Verlauf 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 **Computer Name** *M** oder *M%* eingeben, werden alle mit „M“ beginnenden Computernamen angezeigt. Wenn Sie dagegen in das Feld **Computer Name** nur *M* ohne * oder % eingeben, wird nur der Computer namens „M“ angezeigt.

4. Klicken Sie auf **Run**.
5. Klicken Sie im Agent Session Report auf das **Pluszeichen** neben einem Eintrag im Summary Report, um den ausführlichen Report-Eintrag aufzurufen.
6. Je nachdem, um welchen Report es sich handelt, klicken Sie entweder auf das Symbol **Assessment Details** oder auf den Link **Assessment**.

Weitere Informationen zu den Ergebnisfeldern entnehmen Sie bitte der folgenden Tabelle.

Beschreibung der Felder

Feld	Beschreibung
Assessment Details für den Profiltyp	
Profile Type	Typ des Profils, den der Agent auf dem Endpoint gesucht hat.
Compliance State	Konformitätszustand des Profiltyps. Dieser Konformitätszustand setzt sich aus den auf dem Endpoint analysierten Profilen und dem Richtlinienverhalten (Required, Best oder All) zusammen. Weitere Informationen finden Sie in der Erläuterung zum Feld „Selection Reason“ (weiter unten). Es gibt drei Zustände: „Compliant“ (konform), „Partially Compliant“ (teilkonform) und

Feld	Beschreibung
	„Non-Compliant“ (nicht-konform). Drei Striche (---) deuten darauf hin, dass der Agent einen Compliance State nicht gemeldet hat.
Assessment Details zum Profil	
Profile Name	Name des Profils, das der Agent auf dem Endpoint gesucht hat.
Selected	Hier ist angegeben, ob das Profil zur Ermittlung des Konformitätszustands dieses Profiltyps verwendet wurde. Lautet der Wert „True“, wurde das Profil verwendet. Lautet der Wert „False“, wurde nicht dieses, sondern ein anderes Profil zur Ermittlung des Konformitätszustands verwendet. Weitere Informationen zur Analyse von Profilen auf dem Endpoint finden Sie in den Erläuterungen zum Feld „Selection Reason“.
Selection Reason	<p>Hier ist angegeben, warum das Profil zur Ermittlung des Konformitätszustands dieses Profiltyps verwendet wurde. Der Grund richtet sich nach dem Richtlinienverhalten, das bestimmt, wie Profile mit anderen Profilen desselben Typs auf dem Endpoint miteinander abgeglichen werden. Es sind folgende Werte möglich:</p> <ul style="list-style-type: none"> ■ Required (Best): Hier wird angezeigt, ob sich das erforderliche Betriebssystemprofil auf dem Endpoint befindet. Das Betriebssystemprofil ist erforderlich und wird als Musterprofil analysiert. ■ Best: Hier wird angezeigt, ob sich das Musterprofil auf dem Endpoint befindet. Jedes Profil eines bestimmten Typs in einer Richtlinie wird am Endpoint analysiert, die beste Übereinstimmung ermittelt und nur die berechtigten Maßnahmen in Verbindung mit dem Profil der besten Übereinstimmung werden verwendet. Das Musterverhalten verwendet das Profil, das auf dem Endpoint am chesten konform ist, um den Konformitätszustand des Profiltyps in der Richtlinie zu ermitteln. Falls nicht anders festgelegt, werden Anwendungsprofile auf diese Weise analysiert. ■ Best (No Match): Dieser Grund wird angezeigt, wenn in einer Musteranalyse keine Profile auf dem Endpoint gefunden wurden. Wenn keins der analysierten Profile auf dem Endpoint installiert ist, wird der Konformitätszustand der ELSE-Bedingung des Profils der höchsten Priorität für die Ermittlung des Konformitätszustands und der für diesen Profiltyp in der Richtlinie zu ergreifenden Maßnahmen übernommen. Falls eins der erforderlichen Betriebssysteme nicht auf dem Endpoint installiert ist, wird der Status der ELSE-Bedingungsübereinstimmung des Betriebssystemprofils mit höchster Priorität verwendet, um den Konformitätsstatus und die Maßnahmen für den Betriebssystemprofieltyp festzustellen. Keine weiteren Profile dieser Richtlinie werden analysiert. ■ All: Dieser Grund wird angezeigt, wenn alle Profile auf dem Endpoint analysiert werden. Alle Profile eines bestimmten Typs in einer Richtlinie werden auf dem Endpoint analysiert und berechtigte Maßnahmen in Verbindung mit allen Profilen ergriffen. Das Verhalten „All“ (Gesamtverhalten) verwendet das Profil, das auf dem Endpoint am wenigsten konform ist, um den Konformitätszustand des Profiltyps in

Feld	Beschreibung
	der Richtlinie zu ermitteln. Anwendungsprofile, die auf einem Endpoint nicht verwendet werden sollen, können auf diese Weise analysiert werden.
Detected	Hier wird angezeigt, ob das Profilelement (Betriebssystem oder Anwendung) auf dem Endpoint gefunden wurde. Lautet der Wert „True“, wurde das Profilelement gefunden. Lautet der Wert „False“, wurde das Profilelement nicht gefunden.
Compliance State	Konformitätszustand des Profils. Dieser Zustand wird über die auf dem Endpoint analysierten Profilbedingungen ermittelt. Alle Profilbedingungen werden analysiert, um den Konformitätszustand des Profils zu ermitteln. 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.
Assessment Details zur Profilmöglichkeit	
Profile Condition	Zeigt eine Bedingung an, die im Profil auf Grundlage des auf dem Endpoint vorliegenden Ergebnisses gefunden wurde. Bei dem Ergebnis kann es sich um eine Version, eine Nummer, ein Datum oder um ein sonstiges Element handeln, das die Bedingung am Endpoint abgrenzt. Drei Striche (---) deuten darauf hin, dass die Bedingung keine Abgrenzung aufweist.
Result	Hier wird das Ergebnis der Bedingungsanalyse angezeigt. Lautet das Ergebnis „True“, wurde die im Profil festgelegte Bedingung auf dem Endpoint erfüllt. Lautet das Ergebnis „False“, wurde die im Profil festgelegte Bedingung auf dem Endpoint nicht erfüllt.
Compliance State	Konformitätszustand, der nur im Report festgehalten wird, wenn die Bedingung auf dem Endpoint zutrifft. 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.
Action Type	<p>Art der Korrekturmaßnahme, die auf dem Endpoint durchgeführt wurde. Korrekturmaßnahmen werden nur auf einem Endpoint angezeigt oder durchgeführt, wenn die mit der Maßnahme verknüpfte Bedingung erfüllt ist. Es gibt folgende Maßnahmen:</p> <ul style="list-style-type: none"> ■ Message: Zeigt eine Meldung auf dem Endpoint an. Diese Maßnahme steht für alle Fähigkeiten bereit. ■ Enable: Aktiviert auf dem Endpoint Echtzeitschutz für Viren- oder Spywareschutzanwendungen, aktiviert die Firewall für Firewall-Anwendungen oder ermöglicht automatische Updates für Patch Manager-Anwendungen. Diese Maßnahme steht nur für die Anwendungsfähigkeit „Real-Time Protection“ oder „Enabled“ zur Auswahl. ■ Update: Aktualisiert die Signaturdatei auf dem Endpoint. Diese Maßnahme steht nur für die Anwendungsfähigkeit „Signature Date“ oder „Signature Grace Period“ zur Auswahl.

Feld	Beschreibung
	<ul style="list-style-type: none"> ■ Scan: Leitet eine Engine-Überprüfung auf dem Endpoint ein. Diese Maßnahme steht für die Anwendungsfähigkeit „Scan Date“ oder „Signature Grace Period“ bereit. ■ Apply: Die Sophos Enterprise Console-Richtlinie wird auf Sophos Anti-Virus auf dem Endpoint angewandt. Diese Maßnahme ist für die SEC Policy-Fähigkeit verfügbar.
Action Value	Meldung, die dem Benutzer auf dem Endpoint angezeigt wird. Eine Meldung wird auf dem Endpoint nur dann angezeigt, wenn die entsprechende Bedingung erfüllt ist. Keine anderen Maßnahmen zeigen einen Action Value an.

4.10 Speichern von Reports

Sie können einen Report speichern, wenn Sie die Such- und Sortierkriterien des Reports an Ihre Anforderungen anpassen. Die Kriterien werden gespeichert, sobald der Report gespeichert wird.

Vorgehensweise

1. Klicken Sie auf **Report > Compliance or Troubleshooting**.
2. Klicken Sie auf das Listenfeld **Report Type** und wählen Sie den Namen des zu speichernden Reports.
3. 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. Im Verlauf 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 **Computer Name** *M** oder *M%* eingeben, werden alle mit „M“ beginnenden Computernamen angezeigt. Wenn Sie dagegen in das Feld **Computer Name** nur *M* ohne * oder % eingeben, wird nur der Computer namens „M“ angezeigt.

4. Klicken Sie auf **Run**.
5. Klicken Sie auf **Save**.
6. Geben Sie im Dialogfeld in das Feld **Report Name** den Namen des Reports ein.
7. Klicken Sie auf **Save**.

4.11 Ausführen von gespeicherten Reports

Anhand von Saved Reports (gespeicherten Reports) können Sie allgemeine Report-Einstellungen speichern und wiederverwenden, damit Sie nicht dieselben Kriterien neu eingeben müssen. Sie können auch die Report-Einstellungen gespeicherter Reports ändern, ohne sie als neue Reports speichern zu müssen.

Vorgehensweise

1. Klicken Sie auf **Report > Saved** .
2. Klicken Sie auf das Listenfeld **Saved Report** und wählen Sie den Namen des auszuführenden gespeicherten Reports.
3. 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. Im Verlauf 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 **Computer Name** *M** oder *M%* eingeben, werden alle mit „M“ beginnenden Computernamen angezeigt. Wenn Sie dagegen in das Feld **Computer Name** nur *M* ohne * oder % eingeben, wird nur der Computer namens „M“ angezeigt.

4. Klicken Sie auf **Run**.

4.12 Löschen gespeicherter Reports

Durch das Löschen eines gespeicherten Reports wird dieser vollständig aus der Software entfernt.

Vorgehensweise

1. Klicken Sie auf **Report > Saved** .
2. Klicken Sie auf das Listenfeld **Saved Report** und wählen Sie den Namen des zu löschenden gespeicherten Reports.
3. Klicken Sie auf **Delete**.
4. Klicken Sie zur Bestätigung im Dialogfeld auf **OK**.

4.13 Anzeigen von Audits

Der Audit-Bereich bietet eine Audit-Nachverfolgung, d.h. den Verlauf von Ereignissen, die im System stattgefunden haben. Zu Ereignissen können Updates, neue Elemente oder Systemaktivitäten zählen, z.B. Updates auf aktuelle Richtlinien, Erstellung neuer Access Templates oder Konten, die sich am NAC Manager an- bzw. abmelden.

Vorgehensweise

1. Klicken Sie auf **Report > Audits** .
2. Geben Sie die entsprechenden Suchoptionen in die Felder ein bzw. wählen Sie sie aus und klicken Sie auf **Search**.

Hinweis: Mithilfe der Symbole * und % ist in den meisten Feldern eine Platzhaltersuche möglich. Wenn Sie beispielsweise in das Feld **Item Name** *M** oder *M%* eingeben, werden alle mit „M“ beginnenden Elemente angezeigt.

3. Führen Sie einen der folgenden Schritte aus:
 - Zum Sortieren der Liste klicken Sie auf die entsprechende Spaltenüberschrift.

- Wenn Sie Audit-Details zu einem Ereignis anzeigen möchten, klicken Sie auf den Link **Details**.

5 Konfigurationsbereich im Überblick

Im Konfigurationsbereich (Configure System) können Sie alle Systemkomponenten von NAC Manager konfigurieren. Die im Folgenden aufgeführten Bereiche erreichen Sie über das Menü **Configure System**:

Bereich und Aktion	Beschreibung
Accounts	
Erstellen von System Accounts.	Im Bereich Accounts lassen sich diverse Zugriffsberechtigungen für NAC Manager einrichten. Systemadministratoren können einen Namen erstellen und Benutzer (Security Roles) für System Accounts definieren. Die Zugangsdaten dienen der Anmeldung an NAC Manager. Die Sicherheitsfunktion bestimmt die Zugriffsrechte für jedes Konto.
Deaktivieren oder Aktivieren von Konten.	Konten können durch den Systemadministrator aktiviert und deaktiviert werden. Durch die Deaktivierung eines Kontos kann sich ein bestimmter Benutzer nicht mehr an NAC Manager anmelden, um Systeminformationen abzurufen oder Verwaltungsaufgaben durchzuführen. Durch das Aktivieren eines Kontos kann sich der entsprechende Benutzer an NAC Manager anmelden und alle Verwaltungsaufgaben durchführen, die dieser Berechtigungsklasse innewohnen.
Enforcer Settings	
Ändern der Enforcer-Einstellungen.	Die Enforcer Settings enthalten alle Details zur Richtliniendurchsetzung für den Agent Enforcer und DHCP Enforcer. Der Agent Enforcer wird für Client-basierte Quarantäne-Durchführung verwendet. Der DHCP Enforcer wird mit Sophos NAC DHCP-Implementierungen eingesetzt.
Server Settings	
Erstellen von DHCP-Enforcer-Servern.	In diesem Bereich legen Sie die DHCP-Enforcer-Server für den Einsatz mit Sophos NAC DHCP-Implementierungen fest. Hierbei handelt es sich um die DHCP-Server, auf denen die DHCP Enforcer-Software installiert wird.
Erstellen von Dissolvable Agent-Servern.	In diesem Bereich legen Sie die Host-Server für den Dissolvable Agent fest, damit der DHCP Enforcer den Zugriff darauf freigeben kann.
Ändern der NAC-Proxyserver-einstellungen.	Bei der Installation von NAC können Sie einen Proxyserver für den Internetzugang einrichten. Zum Herunterladen der neuesten Virenkennungen für Sicherheitsanwendungen ist Internetzugang erforderlich. In diesem Bereich können die Proxyeinstellungen geändert werden und optional die IP-Adressen des NAC-Servers angepasst werden.
Download-Kontodetails	
Ändern der Download-Kontodetails.	Über diese Kontodetails bezieht NAC die neuesten Virenkennungen für Sicherheitsanwendungen per Download.

5.1 Erstellen eines Kontos

Im Bereich **Accounts** können Systemadministratoren einen Namen erstellen und Benutzer (Security Roles) für Systemkonten (System Accounts) definieren. Die Zugangsdaten dienen der Anmeldung an NAC Manager. Die Sicherheitsfunktion bestimmt die Zugriffsrechte für jedes Konto.

Vorgehensweise

1. Klicken Sie auf **Configure System > Accounts** . Klicken Sie anschließend im linken unteren Seitenbereich auf **Create Account**.
2. Geben Sie den Kontonamen ein.
3. Sie können jedoch auch die Option **Disable Account** auswählen, um ein deaktiviertes Konto zu erstellen.
4. Geben Sie das Kennwort ein und bestätigen Sie es.

Hinweis: Wenn Sie das Kennwort eines vorhandenen Kontos aktualisieren, müssen Sie außerdem das Kennwort Ihres Kontos eingeben. Der Eintrag in diesem Feld sorgt dafür, dass nur Systemadministratoren mit gültigen Konten Kennwörter aktualisieren können.

5. Wählen Sie eine der folgenden Security Roles:
 - **System Administrator:** Vollzugriff auf alle Bereiche in NAC Manager. Systemadministratoren können Konten erstellen, ändern und löschen.
 - **Administrator:** Vollzugriff auf die Bereiche „Manage“, „Enforce“ und „Report“ in NAC Manager. Lesezugriff auf den Bereich „Configure System“ in NAC Manager. Administratoren haben keinen Zugriff auf den Kontenbereich (Accounts).
 - **Help Desk:** Vollzugriff auf den **Report**-Bereich in NAC Manager. Lesezugriff auf die Bereiche **Manage**, **Enforce** und **Configure System** in NAC Manager. Die Help-Desk-Funktion ermöglicht keinen Zugriff auf die Kontenverwaltung (Accounts).
 - **Guest:** Lesezugriff auf alle Bereiche in NAC Manager. Gäste haben keinen Zugriff auf den Kontenbereich (Accounts).

Hinweis: Alle Security Roles haben Zugriff auf die gesamten Navigationsfunktionen des Programms, darunter auch auf ihre eigenen Kennwörter, die Hilfe und Informationen zu NAC Manager.

6. Klicken Sie auf **Save**.

5.2 Deaktivieren/Aktivieren von Konten

Bei der Erstellung eines Kontos wird es automatisch aktiviert. Es kann jedoch auf Ihren Wunsch hin deaktiviert werden. Durch die Deaktivierung eines Kontos kann sich ein bestimmter Benutzer nicht mehr an NAC Manager anmelden, um Systeminformationen abzurufen oder Verwaltungsaufgaben durchzuführen.

Vorgehensweise

1. Klicken Sie auf **Configure System > Accounts** .

2. Klicken Sie neben einem Konto, das aktiviert bzw. deaktiviert werden soll, jeweils auf das Symbol **Enabled Account** oder **Disabled Account**. Neben jedem Konto wird nun das Symbol des aktuellen Zustands angezeigt.

5.3 Festlegen von Enforcer-Einstellungen

Auf der Seite **Enforcer Settings** können Sie den DHCP Enforcer und/oder Agent Enforcer konfigurieren. Der DHCP Enforcer wird mit Sophos NAC DHCP-Implementierungen eingesetzt. Der Agent Enforcer wird für Client-basierte Quarantäne-Durchführung verwendet.

Vorgehensweise

1. Klicken Sie auf **Configure System > Enforcer Settings**.
2. Wenn Sie den Agent Enforcer verwenden, geben Sie den folgenden Grenzwert ein. Wenn Sie auch den DHCP Enforcer verwenden, fahren Sie mit dem nächsten Schritt fort, ansonsten mit Schritt 7:

- **Agent Policy Update Threshold:** Hier legen Sie den Zeitraum (in Minuten, Stunden oder Tagen) zwischen dem Abruf der Richtlinie durch den Quarantine Agent und dem Durchsetzen der Quarantäne auf dem Endpoint fest. Bei Überschreitung eines Grenzwerts wird der Endpoint in Quarantäne gestellt und eine neue Richtlinie muss abgerufen werden. Der Netzwerkzugriff wird zwischenzeitlich von der Agent Enforcer Access Template ermittelt, die mit dem Policy Retrieval Error Access State der Richtlinie in Zusammenhang steht. Der Grenzwert wird beim Agent Enforcement verwendet. Die Vorgabe lautet acht Stunden. Der Mindestwert lautet 1.

Wichtig: Der Policy-Update-Grenzwert muss stets **über** dem Policy Refresh Interval liegen, der für jede Richtlinie festgelegt ist. Ansonsten wird der Netzwerkzugriff bei jeder Überschreitung des Grenzwerts durch den Policy Retrieval Error-Zugriffszustand der Richtlinie bestimmt, und der Endpoint wird in Quarantäne gesetzt.

3. Geben Sie für den DHCP Enforcer folgende Grenzwerte ein:

- **DHCP Policy Update Threshold:** Hier legen Sie den Zeitraum (in Minuten, Stunden oder Tagen) zwischen dem Abruf der Richtlinie durch den Agenten und dem Ablauf der Richtlinie fest. Wenn die Zeit abgelaufen ist, muss erneut eine Richtlinie abgerufen werden. Der Netzwerkzugriff wird zwischenzeitlich von der DHCP Enforcer Access Template ermittelt, die mit dem Policy Retrieval Error Access State der Richtlinie in Zusammenhang steht. Der Grenzwert wird beim DHCP Enforcement verwendet. Ein Wert von 0 deaktiviert den Grenzwert. Die Vorgabe lautet fünf Stunden.

Hinweis: Es empfiehlt sich, diesen Grenzwert so einzustellen, dass er mindestens 10 Minuten **über** dem Policy Refresh Interval liegt, das für jede Richtlinie festgelegt ist.

- **Dissolvable Agent Compliance Threshold:** Dieser Grenzwert legt die Zeitdauer (in Minuten, Stunden oder Tagen) fest, die ein nicht verwalteter Endpoint Compliance-Eintrag vom DHCP Enforcer als gültig betrachtet wird. Wenn der Grenzwert überschritten wird, wird der nicht verwaltete Endpoint so lange als unbekannt eingestuft, bis auf dem Endpoint eine Konformitätsprüfung durchgeführt wird. In der Zwischenzeit wird der Netzwerkzugriff durch die in Schritt 5 angegebenen Unknown Endpoint Access Templates ermittelt. Bei einem Wert von 0 ist der Grenzwert deaktiviert. Die Vorgabe lautet zwölf Stunden.

4. Wählen Sie die entsprechenden Server-Einstellungen für den DHCP Enforcer:
 - **Report Exemptions:** Über diese Option wird festgelegt, ob der DHCP Enforcer Ausschlüsse melden soll. Wenn die Option aktiviert ist, werden Endpoints, die als Exemptions definiert sind, ausgeschlossen, gemeldet und im DHCP Exemption Report aufgeführt. Wenn nicht ausgewählt, werden als Ausnahmen definierte Endpoints nur ausgeschlossen. Weitere Informationen finden Sie unter [Erstellen des DHCP Exemption Reports](#) (Seite 71).
 - **Exempt DHCP Reservations:** Diese Option bestimmt, ob auf dem DHCP-Server reservierte Endpoints ausgeschlossen werden. Ist diese Option ausgewählt, werden reservierte Endpoints vom Enforcement ausgeschlossen. Wenn jedoch auf einem Endpoint ein Agent installiert wurde, wird die dem Access State des Endpoints zugeordnete Access Template unabhängig von seiner Bestimmung als reservierter Endpoint zugewiesen.
 - **Override DHCP Enforcer:** Diese Einstellung bestimmt, ob der DHCP Enforcer die Durchsetzung anhand von festgelegten Sicherheitsrichtlinien durchführt. Ist dieses Kontrollkästchen aktiviert, wird die Durchsetzung deaktiviert, und der Netzwerkzugriff wird durch die in Schritt 5 angegebenen Maintenance Mode/Enforcer Override Access Templates bestimmt. Diese Access Templates kommen jedoch nur dann zum Einsatz, wenn für den Endpoint keine Ausnahmen festgelegt wurden.

5. Um Access Templates für einen bestimmten Zugriffszustand hinzuzufügen oder zu ändern, klicken Sie unter **DHCP Enforcer Access Templates** auf **Select**, aktivieren Sie die Kontrollkästchen neben den Access Templates und Zugriffszuständen, für die die Vorlagen zutreffen und klicken Sie auf **OK**. Sie können auch die vorhandene Access Template beibehalten oder löschen. Es stehen folgende Access States zur Auswahl:
 - **Unknown Endpoint:** Bestimmt den Netzwerkzugriff, wenn es keinen Eintrag zum Konformitätszustand gibt. Unbekannte Endpoints werden nicht von Sophos Enterprise Console verwaltet und nicht ausgeschlossen. Auf ihnen wird entweder nicht der Dissolvable Agent ausgeführt oder sie haben den in Schritt 2 festgelegten Dissolvable Agent Compliance Threshold überschritten. Sie können Access Templates für unbekannte Endpoints auswählen, wenn der DHCP-Server sich im Modus „Report Only“ oder „Enforce“ befindet. Weitere Informationen finden Sie unter [Erstellen von DHCP-Enforcer-Servern](#) (Seite 83).
 - **Maintenance Mode/Enforcer Override:** Bestimmt Netzwerkzugriff, wenn das System sich im „Maintenance“-Modus befindet oder die Durchsetzung am DHCP Enforcer über das Kontrollkästchen **Override DHCP Enforcer** deaktiviert wurde.
 - **Default:** Bestimmt den Netzwerkzugriff, wenn keine verbundene Access Template gefunden wurde.

6. Ändern Sie bei Bedarf die Prioritätsstufe der 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 **Save**.

5.4 Erstellen von DHCP-Enforcer-Servern

DHCP Enforcer-Server sind für das Enforcement in Sophos NAC DHCP-Implementierungen erforderlich. Hierbei handelt es sich um die DHCP-Server, auf denen die DHCP Enforcer-Software installiert wird. Weitere Informationen zur Konfiguration von DHCP Enforcement finden Sie in der *Sophos NAC DHCP Konfigurationsanleitung*.

Vorgehensweise

1. Klicken Sie auf **Configure System > Server Settings** . Klicken Sie links unten auf der Seite auf **Create Server**.
2. Geben Sie einen Namen und eine Beschreibung für den Server ein.
3. Klicken Sie auf das Listenfeld **Server Type** und wählen Sie **DHCP Enforcer Server**.
4. Geben Sie den Hostnamen oder die IP-Adresse des Servers ein und klicken Sie auf **Add**. Bei Eingabe eines Hostnamens versucht der NAC Manager, den Hostnamen den passenden IP-Adressen zuzuordnen. Wenn dies nicht gelingt, müssen Sie die IP-Adressen manuell eingeben.
5. Geben Sie den gemeinsamen Schlüssel des Servers ein.

Wichtig: Der Schlüssel muss mit Ihrer Eingabe bei der Installation des DHCP Enforcers auf dem Server übereinstimmen.

6. Der unbekannte Endpoint-Modus dient der Ermittlung, ob der DHCP Enforcer Server unbekannte Endpoint-Adressen aufzeichnen oder durchsetzen soll.

Die Option **Report Only** ermöglicht die Integration von DHCP-Enforcer-Servern ohne Auswirkung auf den Netzwerkzugriff. Sobald DHCP-Exemptions eingerichtet wurden und Gastbenutzer sich über den Dissolvable Agent anmelden, können Sie den unbekanntem Endpoint-Modus auf **Enforce** umstellen und so DHCP Enforcement aktivieren.

Unbekannte Endpoints werden nicht von Sophos Enterprise Console verwaltet. Entweder wird der Dissolvable Agent nicht darauf ausgeführt oder sie haben die Dissolvable Agent Compliance Threshold überschritten.

Hinweis: Die im Bereich **Configure System > Enforcer Settings** unter **Unknown Endpoint** aufgeführten Access Templates bestimmen, basierend auf dem unbekanntem Endpoint-Modus, den Netzwerkzugriff. Weitere Informationen finden Sie unter [Festlegen von Enforcer-Einstellungen](#) (Seite 81).

7. Klicken Sie auf **Save**.

5.5 Erstellen von Dissolvable Agent-Servern

Dissolvable Agent-Server hosten den Dissolvable Agent. Der DHCP Enforcer ermöglicht den Zugriff auf diese Server.

Hinweis: Wenn der Dissolvable Agent auf dem gleichen Server wie Sophos NAC installiert ist, müssen Sie keinen weiteren Dissolvable Agent-Server erstellen.

Vorgehensweise

1. Klicken Sie auf **Configure System > Server Settings** . Klicken Sie links unten auf der Seite auf **Create Server**.

2. Geben Sie einen Namen und eine Beschreibung für den Server ein.
3. Klicken Sie auf das Listenfeld **Server Type** und wählen Sie **Dissolvable Agent Server**.
4. Geben Sie den Hostnamen oder die IP-Adresse des Servers ein und klicken Sie auf **Add**. Bei Eingabe eines Hostnamens versucht der NAC Manager, den Hostnamen den passenden IP-Adressen zuzuordnen. Wenn dies nicht gelingt, müssen Sie die IP-Adressen manuell eingeben.
5. Klicken Sie auf **Save**.

5.6 Ändern der NAC-Proxyservereinstellungen

Bei der Installation von NAC können Sie einen Proxyserver für den Internetzugang einrichten. Zum Herunterladen der neuesten Virenkennungen für Sicherheitsanwendungen ist Internetzugang erforderlich. In diesem Bereich können die Proxyeinstellungen geändert werden und optional die IP-Adressen des NAC-Servers angepasst werden.

Vorgehensweise

1. Klicken Sie auf **Configure System > Server Settings**.
2. Klicken Sie auf den Namen des NAC-Server-Servers, um die Servereinstellungen zu ändern.
3. Sie können auch den Hostnamen oder die IP-Adresse des Servers eingeben und auf **Add** klicken. Bei Eingabe eines Hostnamens versucht der NAC Manager, den Hostnamen den passenden IP-Adressen zuzuordnen. Wenn dies nicht gelingt, müssen Sie die IP-Adressen manuell eingeben.

Wichtig: Stellen Sie sicher, dass die IP-Adressen korrekt sind, da sie für die Verbindung zwischen den Agenten und den NAC-Server wichtig sind. Wenn die IP-Adressen nicht korrekt sind, können die Agenten nicht mit dem NAC-Server kommunizieren.

4. Klicken Sie auf die Liste verfügbarer **Proxyeinstellungen** und wählen Sie die gewünschte Proxyserveroption aus:
 - **No Proxy:** Der NAC-Server-Server greift nicht über einen Proxyserver auf das Internet zu.
 - **Use Proxy:** Der NAC-Server-Server greift über einen Proxyserver auf das Internet zu. Die Proxyservereinstellungen werden im Zuge der Installation von NAC festgelegt, können jedoch bei Bedarf geändert werden.
 - **Use SEC Proxy Settings:** Der NAC-Server-Server richtet sich beim Zugriff auf das Internet nach den in Sophos Enterprise Console definierten Proxyeinstellungen. Die Option ist nur verfügbar, wenn Sophos Enterprise Console auf dem gleichen Server wie Sophos NAC installiert ist. Bei Auswahl der Option müssen die Proxyservereinstellungen in Sophos Enterprise Console aktualisiert werden.

5. Aktualisieren Sie die Proxyservereinstellungen.

Hinweis: 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.

6. Klicken Sie auf **Save**.

5.7 Ändern der Download-Kontodetails

Über diese Kontodetails bezieht NAC die neuesten Virenkennungen für Sicherheitsanwendungen per Download. Geben Sie bei der Installation von NAC die Zugangsdaten ein, die Sie von Sophos erhalten haben. Sollten Sie die falschen Daten eingegeben haben, können Sie sie nach der Installation von NAC auf der Seite **Download Account Details** korrigieren.

Vorgehensweise

1. Klicken Sie auf **Configure System > Download Account Details** .
2. Ändern Sie den Benutzernamen und/oder das Kennwort.
Wenn Sie das Kennwort ändern, müssen Sie es zur Bestätigung ein zweites Mal eingeben.
3. Klicken Sie auf **Save**.

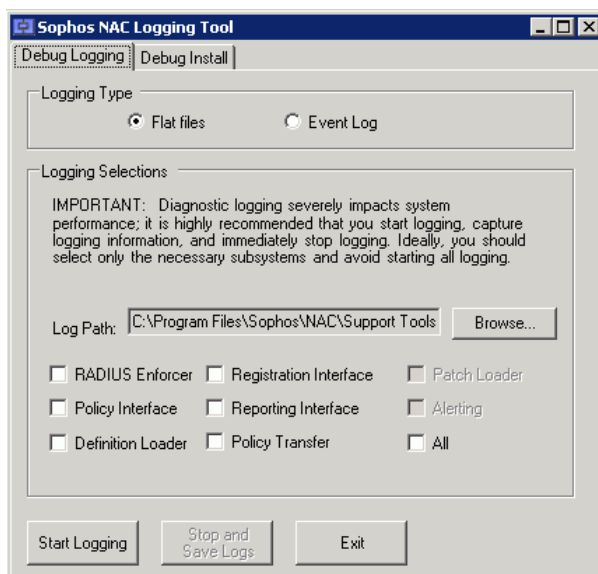
6 Logging Tool

Über das Logging Tool können Sie die Installations- und Subsystemprotokollierung aktivieren, die bei einer Fehlersuche hilfreich ist. Auf der Registerkarte „Debug Logging“ können Sie die Protokollierungsmethode und den Speicherort der Datei feststellen sowie die Protokollierung für individuelle Subsysteme manuell starten und stoppen. Auf der Registerkarte „Debug Install“ können Sie die zu analysierende Installationsdatei und den Speicherort der Protokolldatei feststellen. Die Protokollierung wurde auf die Höchchststufe eingestellt. Die erfassten Daten hängen vom Protokollierungstyp ab.

Wichtig: Es empfiehlt sich, dieses Tool nur unter Anleitung von Sophos zur Fehlersuche zu nutzen. Außerdem sollte nach Behebung des Problems die Protokollierung wieder deaktiviert werden, da sie das System abbremst.

6.1 Sophos NAC-Server-Subsystemprotokollierung

1. Sie finden das Logging Tool auf dem Sophos NAC-Server. Es befindet sich standardmäßig unter C:\Programme\Sophos\NAC\Support Tools.
2. Doppelklicken Sie auf **LoggingUtil.exe**.



3. Wählen Sie im Register **Debug Logging** die gewünschte Protokollierungsmethode, treffen Sie eine Auswahl unter „Logging Selections“ und klicken Sie anschließend auf **Start Logging**. Weitere Informationen zu jedem Feld finden Sie unter [Registerkarte „Debug Logging“](#) (Seite 87).

Hinweis: Nach Klicken auf die Schaltfläche **Start Logging** können Sie keine weiteren Subsysteme auswählen oder deaktivieren. Sie müssen die Protokollierung stoppen, Ihre Auswahl ändern und die Protokollierung erneut starten.

4. Führen Sie auf dem NAC-Server die Tasks aus, für die Sie Protokolleinträge erfassen möchten.
5. Klicken Sie nach Durchführung der Tasks auf **Stop and Save Logs**, um die gewünschten Protokollinformationen in den entsprechenden Protokolldateien zu speichern.

Die Dateien werden in dem Pfad gespeichert, den Sie im Feld **Log Path** angegeben haben. Der Standardprotokollpfad lautet: C:\Programme\Sophos\NAC\Support Tools\Logs. Weitere Informationen zum Typ der Protokolldateien und was sie enthalten, finden Sie unter [Protokolldateien](#) (Seite 89).

Hinweis: Wenn die Protokollierung deaktiviert ist, wird die Schaltfläche **Stop and Save Logs** grau dargestellt.

6.2 Registerkarte „Debug Logging“

Diagnostisches Protokollieren bremst die Systemgeschwindigkeit ab. Es empfiehlt sich daher, die Protokollierung zu starten, die Informationen zu erfassen und die Protokollierung danach sofort zu stoppen. Damit nichts unnötig protokolliert wird, wählen Sie am besten nur die notwendigen Subsysteme.

Hinweis: Die Protokollierung läuft auf der Höchsthöhe und umfasst Protokollfehler-, Warn-, Info-, vollständige Rückverfolgbarkeits- und Aufruflistenmeldungen.

Feld	Beschreibung
Logging Type	
Flat File	Protokollierung erzeugt Flachdateien. Für jedes gewählte Subsystem wird eine Flachdatei erstellt.
Ereignisprotokoll	Protokollierung fügt Subsysteminformationen zum Ereignisprotokoll auf dem NAC-Server hinzu.
Logging Selections	
Log Path	Bestimmt den Pfad, in dem die erzeugten Protokolldateien abgelegt werden.
RADIUS Enforcer	Sets logging for the NAC-Server. Diese Auswahl wird nur beim DHCP Enforcement verwendet. Der NAC-Server ist die Softwarekomponente, die für den DHCP Enforcer die Konformitätsergebnisse des Agenten prüft.
Policy Interface	Protokollierung des Policy Interface-Dienstes. Das Policy Interface ist die Serverkomponente, die Richtlinien für den Agenten abrufen und die Gültigkeit der Agentenanforderung prüft.
Definition Loader	Protokollierung für den Definition Loader. Der Definition Loader ist das Server-Tool, das für die Erkennung von Sicherheitsanwendungen, der Signaturversion, der Scan Engine-Version, des Datums der letzten Überprüfung, des Echtzeitschutzes und für die

Feld	Beschreibung
	aktivierte Erkennung sowie automatische Korrekturmaßnahmen verantwortlich ist.
Registration Interface	Protokollierung des Registration Interface-Dienstes. Das Registration Interface ist die Serverkomponente, die dem Agenten Registrierungsdienste zur Verfügung stellt. Das Registration Interface führt jedes Mal eine Benutzerauthentifizierung durch, wenn sich der Agent erstmals oder wieder registriert.
Reporting Interface	Protokollierung des Reporting Interface-Dienstes. Das Reporting Interface ist die Serverkomponente, die dem Agenten Reportingdienste zur Verfügung stellt. Das Reporting Interface prüft außerdem die Gültigkeit der Agentenanforderung.
Policy Transfer	Protokollierung des Policy Transfer-Dienstes. Policy Transfer ist die Server-Komponente, die Daten vom Richtliniendatenspeicher in den Reportdatenspeicher überträgt, damit aktualisierte Richtlinieninformationen in den Reports widerspiegelt werden.
All	Protokollierung aller Subsysteme von NAC.

6.3 Sophos NAC-Server-Installationsprotokollierung

Dieses Tool sollte nur zur Fehlersuche bei Installationsproblemen verwendet werden. Installieren Sie zunächst Sophos NAC. Wenn Sie während der Erstinstallation auf Fehler stoßen, können Sie mit diesem Tool Protokollinformationen über die Installation erfassen.

1. Sie finden das Logging Tool auf dem Sophos NAC-Server. Es befindet sich standardmäßig unter C:\Programme\Sophos\NAC\Support Tools.
2. Doppelklicken Sie auf **LoggingUtil.exe**.
3. Klicken Sie auf die Registerkarte **Debug Install**.
4. Wählen Sie den Pfad für die Installationsdatei, für die Sie eine Fehlersuche durchführen möchten, und den Pfad, unter dem die Protokolldateien abgelegt werden sollen. Klicken Sie dann auf **Start Install**.

Weitere Informationen zu jedem Feld finden Sie unter [Registerkarte „Debug Install“](#) (Seite 89).

Hinweis: Wenn die Installation abgeschlossen ist, werden die Dateien über den Pfad gespeichert, den Sie im Feld **Log Path** angegeben haben. Der Standardprotokollpfad lautet: C:\Programme\Sophos\NAC\Support Tools\Logs. Weitere Informationen zum Typ der Protokolldateien und was sie enthalten, finden Sie unter [Protokolldateien](#) (Seite 89).

6.4 Registerkarte „Debug Install“

Die Protokollierung läuft auf der vom Microsoft® Windows® Installer bestimmten Höchststufe.

Feld	Beschreibung
Install File Path	Dieses Feld enthält den Pfad zur Installationsdatei.
Log Path	Dieses Feld enthält den Pfad, unter dem die erzeugten Protokolldateien während der Installation abgelegt werden.

6.5 Protokolldateien

Der Standardprotokolldateipfad lautet: C:\Programme\Sophos\NAC\Support Tools\Logs auf dem Sophos NAC-Server. Dieser Pfad kann vor der Erstellung von Protokolldateien geändert werden. Bei jeder Protokollierung werden Dateien mit gleichem Namen, die sich unter dem angegebenen Pfad befinden, überschrieben.

Feld	Beschreibung
AppEvent.xml	Diese Datei enthält die vom Ereignisprotokoll des NAC-Servers exportierten Anwendungsereignisse. Wenn die Option „Event Log“ als Protokolltyp gewählt wird, sind die Subsystemprotokolldaten in dieser Datei enthalten.
SystemEvent.xml	Diese Datei enthält die vom Ereignisprotokoll des NAC-Servers exportierten Systemereignisse. Informationen zum Internet Authentication Service (IAS) sind in dieser Protokolldatei enthalten.
Systeminfo.nfo	Diese Datei enthält die Angaben zu Hardware und Betriebssystem des NAC-Servers.
UserInfo.txt	Diese Datei enthält Kontoinformationen, wie den Kontonamen und die Zugriffsrechte der Benutzer, die am NAC-Server angemeldet sind, und die Konteninformationen, unter denen die installierten Subsysteme ausgeführt werden.
<Subsystem>.xml	Diese Datei enthält die Aufzeichnungen des Subsystemprotokolls von Sophos NAC. Wenn die Option „Flat File“ als Protokolltyp gewählt wird, werden die Subsysteme des Sophos NACs jeweils in einer separaten Flachdatei gespeichert, wie im Folgenden aufgeführt: <ul style="list-style-type: none"> ■ Policy Interface: PolicyInterfaceLog.xml ■ Definition Loader: CurrentDefsLoaderLog.xml ■ Registration Interface: RegistrationInterfaceLog.xml

Feld	Beschreibung
	<ul style="list-style-type: none">■ Reporting Interface: ReportingInterfaceLog.xml■ Policy Transfer: PolicyTransferLog.xml
SophosNACLogs.zip	Diese Datei enthält die auf der Registerkarte „Debug Logging“ aufgeführten Protokolldateien.
InstallLogs.zip	Diese Datei enthält die auf der Registerkarte „Debug Install“ aufgeführten Protokolldateien.

7 Maintenance Mode Tool

Mit dem Maintenance Mode Tool können Sie die Datenbank verwalten und Netzwerk-/Datenbankprobleme ermitteln. Es handelt sich um ein Befehlszeilen-Tool zum Aktivieren oder Deaktivieren des Verwaltungsmodus. Es hält den jeweiligen Dienst von Sophos NAC an, falls daran Änderungen vorgenommen werden müssen. Wenn der Dienst wieder fortgesetzt werden kann, stoppen Sie das Maintenance Mode Tool. Das Tool startet die angehaltenen Dienste wieder automatisch.

Wenn sich Sophos NAC im Verwaltungsmodus („Maintenance Mode“) befindet, erkennt der Sophos Compliance 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. Außerdem führt der Agent Analysen auf der Basis der im Cache befindlichen Richtlinie durch. Wenn die Agent Quarantine benutzt wird, kann der Endpoint den Regeln dieser Richtlinie entsprechend isoliert werden. Beim DHCP Enforcement werden die DHCP Enforcer Access Templates und die Ausnahmen im Cache gespeichert und alle DHCP-Anforderungen damit beantwortet.

Hinweis: Dieses Tool ist bei Sophos NAC Upgrades nicht erforderlich. Der NAC-Server befindet sich bei der Installation im Modus „Maintenance“ und wird anschließend wieder in den ursprünglichen Modus versetzt.

7.1 Starten des Maintenance Mode Tools

1. Rufen Sie auf dem Sophos NAC-Server das Verzeichnis C:\Programme\Sophos\NAC\Support Tools auf.
2. Geben Sie **MaintMode.exe /start** ein. Dieser Befehl versetzt Sophos NAC in den Modus „Maintenance“.
3. Geben Sie **MaintMode.exe /stop** ein. Dieser Befehl versetzt Sophos NAC wieder in den Arbeitsmodus.

7.2 Befehle des Maintenance Mode Tools

Die Befehle sind nicht an die Groß- und Kleinschreibung gebunden. Befehlszeilenparameter werden mit einem Schrägstrich gefolgt vom eigentlichen Parameter dargestellt. Alle DOS-Parameter, die Leerzeichen enthalten, erfordern Anführungsstriche.

Befehl	Beschreibung
MaintMode.exe /start	Starten des Maintenance Mode Tools.
MaintMode.exe /stop	Anhalten des Maintenance Mode Tools.
MaintMode.exe /E:silent	Vorgabe, dass keine Meldungen in das Dialogfeld der Befehlszeile geschrieben werden. Fehlermeldungen werden immer im Ereignisprotokoll erfasst.

Befehl	Beschreibung
MaintMode.exe /E:error	Auf der Konsole werden nur Fehler angezeigt. Fehlermeldungen werden immer im Ereignisprotokoll erfasst.
MaintMode.exe /E:warn	Auf der Konsole werden nur Fehler und Warnungen angezeigt. Fehlermeldungen werden immer im Ereignisprotokoll erfasst.
MaintMode.exe /E:info	Auf der Konsole werden nur Fehler, Warnungen und Infomeldungen angezeigt. Fehlermeldungen werden immer im Ereignisprotokoll erfasst.
MaintMode.exe /?	Anzeige des Hilfefensters für das Maintenance Mode Tool.

8 Glossar

In diesem Glossar werden die in Zusammenhang mit Sophos NAC verwendeten Begriffe erläutert.

Access State	Bei einem Access State handelt es sich um einen Zustand, dem eine Access Template zur Regelung des Netzwerkzugriffs zugeordnet werden kann. Agent Enforcer Access Templates können auf Access States in Richtlinien übertragen werden. DHCP Enforcer Access Templates können auf Access States in Richtlinien, Ausnahmen und Enforcer-Einstellungen übertragen werden.
Access Template	Hierbei handelt es sich um Vorlagen, die bestimmten Access States in Richtlinien, Exemptions und Enforcer-Einstellungen (für jeden Enforcement-Typ unterschiedlich) zugeordnet sind und den Netzwerkzugriff regeln.
Account	Ein Account (bzw. Konto) besteht aus einem Anmeldenamen und einer Security Role (Sicherheitsfunktion) für den Benutzer. Die Zugangsdaten dienen der Anmeldung an NAC Manager. Die Sicherheitsfunktion bestimmt die Zugriffsrechte für jedes Konto.
Agent Configuration Template	In Agent Configuration Templates sind optionale Einstellungen zur Funktionsweise des Quarantine Agent auf Endpoints festgelegt.
Agent Enforcer	Der Agent Enforcer schützt das Netzwerk durch Client-basierte Überprüfung und Quarantäne-Durchsetzung auf Endpoints, auf denen der Quarantine Agent installiert ist.
Agenten-Einstellungen	Agenten-Einstellungen definieren die Funktionen für die Ausführung des Agenten auf dem Endpoint. Agenten-Einstellungen lassen sich bei der Erstellung von Agent Configuration Templates vornehmen.
Agentensitzung	Unter einer Agentensitzung ist die Dauer zu verstehen, in der ein Agent auf dem Endpoint aktiv ist und Zugriff auf Sophos NAC hat.
All Policy Behavior	Alle Profile eines bestimmten Typs in einer Richtlinie werden auf dem Endpoint analysiert und berechnete Maßnahmen in Verbindung mit allen Profilen ergriffen. Das Verhalten „All“ (Gesamtverhalten) verwendet das Profil, das auf dem Endpoint am wenigsten konform ist, um den Konformitätszustand des Profiltyps in der Richtlinie zu ermitteln. Anwendungsprofile, die auf einem Endpoint nicht verwendet werden sollen, können auf diese Weise analysiert werden.
Anwendung	Unter Applications (Anwendungen) sind Programme zu verstehen, die von Sophos NAC erkannt werden. Im Bereich Applications (Anwendungen) sind Fähigkeiten, Bedingungen, Konformitätszustände und mögliche Korrekturmaßnahmen zusammengefasst. Anwendungen sind an einen Anwendungstyp

	gebunden, der beim Hinzufügen des Anwendungsprofils zur Richtlinie eine Bewertungsmethode festlegt.
Anwendungstyp	Anwendungstypen dienen der Kategorisierung von Anwendungen und Festlegung von Standard-Richtlinien für alle unter einer Kategorie zusammengefassten Anwendungen.
Audits	Audits stellen eine Audit-Nachverfolgung oder den Verlauf von Ereignissen dar, die im System stattgefunden haben. Zu Ereignissen können Updates, neue Elemente oder Systemaktivitäten zählen, z.B. Updates auf aktuelle Richtlinien, Erstellung neuer Access Templates oder Konten, die sich am NAC Manager an- bzw. abmelden.
Best Policy Behavior	Jedes Profil eines bestimmten Typs in einer Richtlinie wird am Endpoint analysiert, die beste Übereinstimmung ermittelt und nur die berechtigten Maßnahmen in Verbindung mit dem Profil der besten Übereinstimmung werden verwendet. Das Verhalten „Best“ (Musterverhalten) verwendet das Profil, das auf dem Endpoint am ehesten konform ist, um den Konformitätszustand des Profiltyps in der Richtlinie zu ermitteln. Falls nicht anders festgelegt, werden Anwendungsprofile auf diese Weise analysiert. Wenn keins der analysierten Profile auf dem Endpoint installiert ist, wird der Konformitätszustand der ELSE-Bedingung des Profils der höchsten Priorität für die Ermittlung des Konformitätszustands und der für diesen Profiltyp in der Richtlinie zu ergreifenden Maßnahmen übernommen.
Capability	Unter Capabilities sind die Funktionen einer Anwendung zu verstehen, die im Rahmen einer Konformitätsbewertung getestet werden können. Dazu zählen Analyseregeln, die sich aus Bedingungen, Konformitätszuständen, Meldungen und Korrekturmaßnahmen zusammensetzen.
Compliance State	Der Konformitätszustand eines Endpoints wird durch den Abgleich der Endpoint-Erkennungsergebnisse mit den im Profil festgelegten Bedingungen ermittelt. Der Konformitätszustand wird dann zur Ermittlung der dem Endpoint tatsächlich zugewiesenen Netzwerkzugriffsrechte an die entsprechenden Access Templates der Richtlinie übermittelt. Es gibt die drei Konformitätszustände <i>compliant</i> (konform), <i>partially compliant</i> (teilweise konform) und <i>non-compliant</i> (nicht konform).
Condition	Conditions (Bedingungen) sind Anweisungen, die bei der Bewertung zur Ermittlung des zugehörigen Konformitätszustands und der am Endpoint durchzuführenden Maßnahmen verwendet werden.
Default	Ein im Bereich Configure System > Enforcer Settings definierter Access State, der den Netzwerkzugriff regelt, wenn keine entsprechende Access Template gefunden wurde.

DHCP Configuration Wizard	Dieser Assistent erkennt Web-Proxyserver, Korrekturserver, Dissolvable Agent- und DHCP-Enforcer-Server für Sophos NAC DHCP-Implementierungen.
DHCP Enforcer	Der DHCP Enforcer schützt in Sophos NAC DHCP-Umgebungen das Netzwerk.
Dissolvable Agent	Der Dissolvable Agent untersucht Endpoints vor dem Gewähren von Netzwerkzugriff auf ihre Konformität mit der NAC-Richtlinie. Der Dissolvable Agent muss über einen Browser gestartet werden. Der Dissolvable Agent wird für Benutzer verwendet, auf deren Endpoint kein Agent installiert ist, die jedoch Zugriff auf bestimmte Netzwerkressourcen benötigen. Bei solchen Benutzern kann es sich zum Beispiel um Auftragnehmer oder Besucher handeln. Der Dissolvable Agent ist für die DHCP Enforcement erforderlich.
Endpoint	Unter Endpoint ist ein Computer zu verstehen, der versucht, eine Netzwerkverbindung herzustellen. Ein Endpoint kann über einen Agenten verfügen, er kann von der Konformitätsprüfung ausgeschlossen sein oder er kann unbekannt sein.
Enforce Policy Mode	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.
Enforcer Settings	Die Enforcer Settings enthalten alle Details zur Richtliniendurchsetzung für den DHCP Enforcer und Agent Enforcer.
Erkennungsregel	Eine Erkennungsregel legt die Registrierungseinträge, Prozesse oder Dateien fest, die auf dem Endpoint analysiert werden. Somit lässt sich bestimmen, ob eine Anwendung installiert oder gestartet ist. Auch die Version oder der Wert lässt sich ermitteln.
Exemption	In Exemptions (Ausnahmen) sind Endpoints festgehalten, die bei Verbindung mit dem Netzwerk nicht auf Konformität überprüft werden müssen. Hierzu zählen Endpoints, auf denen entweder der Agent nicht ausgeführt werden kann (z.B. Endpoints, die nicht unter Windows laufen), oder für die keine Konformitätsprüfung erforderlich ist – z.B. Server, Router und Drucker. Wenn Sie Richtlinien im Unternehmen schrittweise durchsetzen möchten, können Sie Endpoints von der Konformitätsprüfung ausnehmen, die noch nicht einbezogen werden sollen.
Korrekturmaßnahme	Hierbei handelt es sich um eine Maßnahme zur Erzielung von Richtlinienkonformität auf nicht-konformen Endpoints. Sie wird bei der Konformitätsprüfung durchgeführt. Korrekturmaßnahmen stehen nicht für alle Anwendungen oder Anwendungsfähigkeiten zur Verfügung.

Maintenance Mode/Enforcer Override	Ein im Bereich Configure System > Enforcer Settings definierter Access State, der den Netzwerkzugriff regelt, wenn sich das System im Modus „Maintenance“ befindet oder der DHCP Enforcer deaktiviert wurde.
Managed-Richtlinie	Diese Richtlinie kommt auf Endpoints zum Einsatz, die von Sophos Enterprise Console verwaltet werden und auf denen ein 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.
Meldung	Hierbei handelt es sich um eine Informations- oder Fehlermeldung, die bei der Konformitätsprüfung auf dem Endpoint angezeigt wird. Meldungen werden nur auf einem Endpoint angezeigt, wenn die mit der Meldung verknüpfte Bedingung erfüllt ist. Es gibt Meldungen für jede Capability (Fähigkeit).
Netzwerkressource	Bei Netzwerkressourcen handelt es sich um Anwendungen oder Geräte, die zur Korrektur von Endpoints erforderlich sind oder auf die Endpoints keinen Zugriff erhalten sollen. Netzwerkressourcen können zu Agent Enforcer oder DHCP Enforcer Access Templates hinzugefügt werden.
Nicht verwalteter Endpoint	Nicht verwaltete Endpoints sind unternehmensexterne Systeme, die nicht von Sophos Enterprise Console verwaltet werden. Auf nicht verwalteten Endpoints werden Konformität und Netzwerkzugriff über den Dissolvable Agent ermittelt.
No Agent Tray	Access State, der in der Richtlinie festgelegt ist, die den Netzwerkzugriff regelt, wenn auf dem Endpoint der Agent nicht läuft. Dieser Zustand kann von Agent Enforcer gemeldet werden, wenn der Benutzer nicht an Windows angemeldet ist oder das Programm „Agent Tray“ nicht mehr läuft.
Policy	Anhand von Richtlinien wird, basierend auf den Profilbewertungen am Endpoint, der gesamte Zugriff auf das Unternehmensnetzwerk kontrolliert. Über Richtlinien wird die Konfiguration verwaltet, in der Konformitätszustand, angezeigte Meldungen sowie durchgeführte Korrektur- und Durchsetzungsmaßnahmen eines Endpoints festgehalten sind.
Policy Retrieval Error (Agent)	Access State, der in der Richtlinie festgelegt ist, die den Netzwerkzugriff regelt, wenn für den Endpoint keine Richtlinie abgerufen werden konnte. Dieser Zustand kann vorliegen, wenn der Agent eine Richtlinie nicht vom NAC-Server herunterladen kann oder der Konformitätszustand des Endpoints gemäß dem Feld Agent Policy Update Threshold (unter Configure System > Enforcer Settings) abgelaufen ist.
Policy Retrieval Error (DHCP)	Access State, der in der Richtlinie festgelegt ist, die den Netzwerkzugriff regelt, wenn der Konformitätszustand des

	Endpoints gemäß dem Wert im Feld DHCP Policy Update Threshold (unter Configure System > Enforcer Settings) nicht mehr aktuell ist.
Profil	In Profilen (Profiles) lassen sich Elemente festlegen, die auf dem Endpoint analysiert bzw. überprüft werden sollen, z.B. Betriebssysteme und Anwendungen. In Profilen werden Bedingungen, Konformitätszustände, Meldungen und Korrekturmaßnahmen definiert. Nach der Erstellung können Profile über Richtlinien verwaltet und priorisiert werden.
Profile Type	Profiltypen (Profile Types) dienen der Zuordnung von Profilen. Profile werden in Richtlinien abgelegt und basierend auf dem Typ und der zugehörigen Richtlinienfunktion miteinander auf Endpoints abgeglichen.
Quarantine Agent	Der Quarantine Agent untersucht Endpoints auf ihre Konformität mit der NAC-Richtlinie. Die Überprüfung erfolgt vor dem Gewähren von Netzwerkzugriff und wird danach in regelmäßigen Abständen wiederholt. Es ist kaum bzw. keine Interaktion mit dem Benutzer erforderlich. Der Quarantine Agent verfügt außerdem über eine Quarantäne-Funktion zur Durchsetzung, die den Endpoint auf Bereiche des Unternehmensnetzwerks beschränken, wenn auf dem Endpoint keine Konformität mit der NAC-Richtlinie mehr gegeben ist.
Remediate Policy Mode	Endpoints werden anhand der zugewiesenen Richtlinie auf Konformität überprüft. Die Ergebnisse werden von NAC Manager in einem Report festgehalten. Es werden Meldungen angezeigt und Korrekturmaßnahmen durchgeführt. Es werden jedoch keine Durchsetzungsmaßnahmen durchgeführt.
Report Only Policy Mode	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.
Required Policy Behavior	Ein Betriebssystemprofil ist erforderlich und wird als Musterprofil analysiert. Falls eins der erforderlichen Betriebssysteme nicht auf dem Endpoint installiert ist, wird der Status der ELSE-Bedingungsübereinstimmung des Betriebssystemprofils mit höchster Priorität verwendet, um den Konformitätsstatus und die Maßnahmen für den Betriebssystemprofiltyp festzustellen. Keine weiteren Profile dieser Richtlinie werden analysiert.
Richtlinienverhalten	Richtlinienverhalten bestimmt die Auswertungsmethode beim Vergleich von Profilen desselben Typs auf einem Endpoint. Es gibt drei Optionen: <i>Required</i> , <i>Best</i> und <i>All</i> . Weitere Informationen finden Sie in den Definitionen zu „Required Policy Behavior“, „Best Policy Behavior“ und „All Policy Behavior“.

Security Role	Security Roles bestimmen die Zugriffsrechte für jedes NAC Manager-Konto. Bei der Erstellung eines Kontos wird automatisch die passende Security Role zugewiesen.
Standardrichtlinie	Die vorhandene Standardrichtlinie wird für Endpoints verwendet, auf denen ein Agent installiert ist, und denen noch 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.
Unknown Endpoint	Im Bereich Configure System > Enforcer Settings definierter Access State, der den Netzwerkzugriff regelt, wenn es keinen Eintrag zum Konformitätszustand gibt. Verwaltungse Endpoints werden von Sophos Enterprise Console nicht ausgeschlossen. Entweder wird der Dissolvable Agent nicht darauf ausgeführt oder sie haben die Dissolvable Agent Compliance Threshold überschritten. Wenn sich der DHCP-Server im Modus „Report Only“ oder „Enforce unknown endpoint“ befindet, können Sie unbekanntes Endpoints Access Templates zuordnen.
Unmanaged-Richtlinie	Die vorhandene Richtlinie „Unmanaged“ ist für unternehmensexterne Endpoints konzipiert. Sie führt keine Korrekturmaßnahmen auf dem Endpoint durch. Der Dissolvable Agent verwendet die Richtlinie „Unmanaged“.
User Override	Access State, der in der Richtlinie festgelegt ist, die den Netzwerkzugriff regelt, wenn der Quarantänezustand eines Endpoints durch den Benutzer aufgehoben wurde. Der Quarantänezustand wird somit deaktiviert.
Verwalteter Endpoint	Verwaltete Endpoints werden von Sophos Enterprise Console verwaltet. Sophos Compliance Agent ist darauf installiert. Auf verwalteten Endpoints werden Konformität und Netzwerkzugriff über den Quarantine Agent ermittelt.

9 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.

10 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.

OPSWAT, Inc.

Diese Software enthält lizenzierte Technologie von © OPSWAT, Inc. OPSWAT ist eine Marke von OPSWAT, Inc.

Index

A

Access States 18, 82
 Access Templates 45
 Anzeigen oder Suchen 9
 Arbeitskopie 8
 Erstellen 48–49
 Löschen 9
 Praxistipps 46
 Sperren und Freigeben 10
 Überprüfen in Richtlinie 13
 Überprüfen, ob das Enforcement wie gewünscht erfolgt 46
 Agent Configuration Templates 12
 Anzeigen oder Suchen 9
 Anzeigen von Agenten-Einstellungen für 20
 Arbeitskopie 8
 Erstellen 20
 Löschen 9
 Sperren und Freigeben 10
 Agent Enforcer 18, 48, 81
 Agent Enforcer Report 65
 Agent Session Report 61
 Agenten-Einstellungen
 in Agent Configuration Templates 20
 in Richtlinien 16
 Aktivieren
 Exemptions 57
 Konten 80
 Anwendungen 9, 12
 Anwendungsprofile 31
 Anwendungstypen 12
 Anzeigen
 Agenten-Einstellungen 20
 Anwendungsfähigkeiten und Bedingungen 33
 Assessment Details 73
 Audits 77
 Listenelemente 9
 Richtlinienmodi und Access States 18
 Arbeitskopie 8
 Assessment Details 73
 Audits 58, 77
 Aufrufen der Startseite 4
 Ausführbare Netzwerkressourcen 53
 authentifizierter Proxyserver 84

B

Bedingungen 22, 30–33, 75
 Benutzerklasse 49, 55
 Betriebssystemprofile 29

C

Compliance Reports 59

D

Deaktivieren
 Exemptions 57
 Konten 80
 Definitionen 93
 Detail Reports 59
 DHCP Configuration Wizard 45, 51
 DHCP Enforcer 18, 49, 55–56, 81
 DHCP Enforcer Report 67, 72
 DHCP Exemption Report 71
 DHCP-Enforcer-Server 83
 DHCP-Lease-Einstellungen 49
 Dissolvable Agent-Webserver 83
 DNS-Server 49
 Download-Kontodetails 79, 85
 Drucken von Reports 59

E

Endpoint-Konformitätszustand 43
 Enforcer Settings 79, 81
 Enforcer-Typen 18, 48–49, 55, 81
 Ermitteln des Konformitätszustands 43
 Erstellen
 Access Templates 48–49
 Agent Configuration Templates 20
 DHCP-Enforcer-Server 83
 Dissolvable Agent-Webserver 83
 Exemptions 55–56
 Exemptions über Reports 72
 Konten 80
 Netzwerkressourcen 53
 Profile 28–29, 31
 Erstellen von Reports 59, 61, 63, 65, 67, 71, 73, 76
 Exemptions 45
 Anzeigen oder Suchen 9
 Arbeitskopie 8

Exemptions (*Fortsetzung*)

- Deaktivieren/Aktivieren 57
- Erstellen 55–56
- Erstellen über Reports 72
- Löschen 9
- Reporting 71, 82
- Sperren und Freigeben 10

F

- Fähigkeiten 22, 32–33, 75
 - Sophos Anti-Virus 33
- Festlegen von Enforcer-Einstellungen 81
- Freigeben von Elementen 10

G

- Gespeicherte Reports 58
 - Ausführen 76
 - Löschen 77
 - Speichern 76
- Glossar 93

H

- Herstellerklasse 55
- Hinzufügen
 - Objekte zu Profilen 29, 31
 - Profile zu Richtlinien 17

I

- Implementierung von Network Access Control 3
- IP-Bereich 49, 56

K

- Konfigurieren
 - des Agenten 17, 20
 - DHCP Enforcement 51
- Konformitätszustände 18, 22, 30–32, 43, 46, 48–49, 59, 61, 63, 65, 67, 73, 75
- Konten 79
 - Anzeigen oder Suchen 9
 - Deaktivieren/Aktivieren 80
 - Download-Kontodetails 85
 - Erstellen 80
 - Löschen 9
- Kontextmenüs 11
- Korrekturmaßnahmen 22, 32, 75

L

- Listenelemente 9
- Logging Tool 86
 - Installationsprotokoll von NAC 88
 - NAC Server-Protokollierung 86
 - Protokolldateien 89
- Löschen von Elementen 9, 77

M

- MAC-Adresse 55, 72
- Maintenance Mode Tool 91
 - Befehle 91
 - Starten des Tools 91
- Meldungen 22, 30, 32, 75
- Menübefehle 3, 12, 45, 58, 79

N

- NAC Manager 3
 - Anlegen von Arbeitskopien 8
 - Anzeigen oder Suchen von Listenelementen 9
 - Kontextmenüs 11
 - Löschen von Elementen 9
 - Sperren und Freigeben von Elementen 10
 - Symbole 5
- NAC-Proxyservereinstellungen 84
- Netzwerkressourcen 45, 48–49
 - Anzeigen oder Suchen 9
 - Arbeitskopie 8
 - Erstellen 53
 - Löschen (nur individuell) 9
 - Sperren und Freigeben (nur individuell) 10
- Nicht-verwaltete Endpoints 16, 29
- Non-Compliance Detail Report 63

P

- Patch-Analyse 28
- Port-/Protokoll-Netzwerkressourcen 53
- Praxistipps
 - Access Template 46
 - Profil 22
 - Richtlinie 13
- Profile 12, 74
 - Anzeigen oder Suchen 9
 - Anzeigen von Anwendungsfähigkeiten und Bedingungen für 33

Profile (Fortsetzung)

- Arbeitskopie 8
- Erstellen 28–29, 31
- Grundsätze 28
- Löschen 9
- Praxistipps 22
- Praxistipps:Fähigkeiten 22
- Profile, vorhandene Windows-Update-Profile 28
- Sperren und Freigeben 10
- vordefinierter Sophos Patch Agent 28

Profiltypen 17, 29, 31, 73**Proxyservereinstellungen 84****Q****Quarantine Override 13****R****Reports 58**

- Agent Enforcer Report 65
- Agent Session Report 61
- Assessment Details 73
- Compliance Reports 59
- DHCP Enforcer Report 67, 72
- DHCP Exemption Report 71
- Drucken 59
- Löschen gespeicherter 77
- Non-Compliance Detail Report 63
- Speichern 76–77

Richtlinien 12

- Abrufen von Richtlinienmodi und Access States für 18
- Anzeigen oder Suchen 9
- Praxistipps 13
- Sperren und Freigeben 10
- Updates 16
- Verwenden vorhandener 15

Richtlinienmodus 13, 16, 18

- Enforce 19
- Remediate 19
- Report Only 18

Richtlinienverhalten 17, 74**S****Security Roles 80****Server**

- DHCP Enforcer 83

Server (Fortsetzung)

- Dissolvable Agent 83
- NAC-Proxyeinstellungen 84
- Server-Einstellungen 79
- Sophos Enterprise Console 15, 33
- Sophos Patch 28
- Sophos Patch Agent-Profil 28
- Sperren von Elementen 10
- Startseite 4
- Suchen von Listenelementen 9
- Summary Reports 59

Symbole

- Allgemeine Funktionen 5
- Anwendungsprofile 7
- Exemptions 7
- Konformitätszustände der Vorlagen 6
- Konten 6
- Profile und Richtlinien 6
- Reports 7

Systemereignisse 77**T****Technischer Support 99****Tipps**

- Anwendungen 12
- Profile 12, 28
- Richtlinien 13

Tools

- Logging Tool 86
- Maintenance Mode Tool 91

U**Überblick, System 3, 12, 45, 58, 79****Updates**

- Download-Kontodetails 85
- NAC-Proxyservereinstellungen 84
- Richtlinien 16

V**verwaltete Endpoints 16, 28****Verwenden**

- vordefinierte Richtlinien 15
- vordefiniertes Sophos Patch Agent-Profil 28
- vorhandener Windows-Update-Profile 28

vordefinierte Richtlinien 15**Vorhandene Access Templates 46****Vorhandene Profile 22, 28**

W

Windows-Update-Profil 28

Z

Zuweisen von Access Templates 18, 55–56, 82