

SOPHOS

Sophos NAC DHCP Guide de configuration

Version du produit : 3.3

Date du document : septembre 2009



Table des matières

1 A propos de ce guide.....	3
2 Aperçu de l'application du protocole DHCP.....	4
3 Liste de contrôle de l'application de DHCP.....	5
4 Installation du logiciel DHCP Enforcer.....	6
5 Tâches du NAC Manager	7
6 Annexe A : utilisation de l'outil de configuration DHCP.....	19
7 Annexe B : mise à niveau de l'application de DHCP.....	22
8 Support technique.....	24
9 Copyright.....	25

1 A propos de ce guide

Ce guide vous aide à configurer l'application du protocole DHCP dans le cadre de Sophos Endpoint Security and Control afin que vous puissiez identifier les systèmes d'extrémité inconnus se connectant à votre réseau, évaluer leurs niveaux de sécurité et contrôler leur accès au réseau. Il décrit comment configurer NAC DHCP Enforcer et le serveur NAC. Ce document contient aussi des informations sur la reconfiguration de votre application du protocole DHCP pour utiliser la configuration DHCP de Endpoint Security and Control 8.

Tout particulièrement, il vous fournit des informations sur :

- L'installation et la configuration du logiciel DHCP Enforcer pour la première fois.
- La configuration de DHCP à l'aide du NAC Manager.
- La reconfiguration de l'application du protocole DHCP pour qu'il fonctionne avec la mise en place précédente si vous avez utilisé l'application du protocole DHCP dans Sophos Endpoint Security and Control 8.

Ce guide s'adresse à vous si :

- Vous utilisez l'Enterprise Console.
- Vous utilisez Sophos NAC pour Endpoint Security and Control.
- Vous voulez configurer l'application du protocole DHCP.

Consultez le *Guide de démarrage rapide de Sophos Endpoint Security and Control* avant de lire ce guide.

Tous les documents Sophos Endpoint Security and Control sont disponibles sur : http://www.sophos.fr/support/docs/Endpoint_Security_Control-all.html.

1.1 Configuration requise pour le logiciel DHCP Enforcer

Pour utiliser l'application de DHCP avec Sophos NAC, vous devez installer le logiciel Sophos DHCP Enforcer sur chaque serveur DHCP.

Configuration requise pour le logiciel DHCP Enforcer	
Système d'exploitation	Serveur Windows 2000 ou 2003
Logiciel DHCP	Logiciel Microsoft [®] Dynamic Host Configuration Protocol (DHCP)

2 Aperçu de l'application du protocole DHCP

Sophos NAC contient les paramètres par défaut de l'application du protocole DHCP. Ces paramètres par défaut concernent la mise en place la plus usuelle de DHCP afin qu'une configuration minimale soit requise dès que Sophos NAC est installé. Toutefois, les mises en place de DHCP sont très variables, aussi, il se peut qu'une configuration supplémentaire soit nécessaire.

Remarque : la liste de contrôle d'application du protocole DHCP fournit une liste des tâches requises pour mettre en place l'application du protocole DHCP. Pour plus d'informations, reportez-vous à la section [Liste de contrôle de l'application de DHCP](#) à la page 5.

Paramètres d'application du protocole DHCP prédéfinis par défaut

Si nécessaire, utilisez le NAC Manager pour modifier les paramètres par défaut.

- Les systèmes d'extrémité inconnus sont autorisés à accéder au réseau. Les systèmes d'extrémité inconnus ne disposent pas de l'agent et ne sont pas exemptés.

Remarque : pour mettre en quarantaine les systèmes d'extrémité inconnus à l'aide de l'application du protocole DHCP, modifiez le paramètre Unknown Endpoint sur Enforce. Pour plus d'informations, reportez-vous à la section [Activation de l'application de DHCP pour les systèmes d'extrémité inconnus](#) à la page 14.

- Les systèmes d'extrémité connus, qui sont ceux exécutant l'agent, sont autorisés à accéder au réseau. Les stratégies NAC sont paramétrées sur Report Only. Pour activer l'application du protocole DHCP pour les systèmes d'extrémité connus, vous devez modifier le mode de la stratégie sur Enforce pour chaque stratégie que vous souhaitez utiliser.

Remarque : lorsque l'application du protocole DHCP est activée, les systèmes d'extrémité conformes et partiellement conformes exécutant l'agent sont autorisés à accéder au réseau. Les systèmes d'extrémité non conformes exécutant l'agent sont interdits d'accès au réseau. Pour plus d'informations, reportez-vous à la section [Activation de l'application du protocole DHCP pour les systèmes d'extrémité connus](#) à la page 14.

Sophos vous recommande d'utiliser l'application du protocole DHCP pour les systèmes d'extrémité inconnus et l'application de l'agent pour les systèmes d'extrémité connus. Toutefois, Sophos NAC ne vous permet pas d'utiliser l'application du protocole DHCP pour les systèmes d'extrémité connus. Pour plus d'informations sur l'application de l'agent, reportez-vous au *Guide de configuration de Sophos Compliance Agent*.

3 Liste de contrôle de l'application de DHCP

La liste de contrôle d'application de DHCP fournit une liste des tâches requises pour mettre en place l'application de DHCP. Sauf mention contraire, toutes les tâches sont effectuées conformément aux instructions du présent document.

Tâche	Description	Terminée
Installation de Sophos NAC et de Sophos Compliance Agent		
1.	Installez et configurez Sophos NAC. Pour plus d'informations, reportez-vous au <i>Guide de démarrage de Sophos Endpoint Security and Control</i> .	
2.	Déployez Compliance Agent sur les systèmes d'extrémité à l'aide de la Sophos Enterprise Console. Pour plus d'informations, reportez-vous au <i>Guide de démarrage rapide de Sophos Endpoint Security and Control</i> .	
Tâches du serveur DHCP		
3.	Installez le logiciel DHCP Enforcer sur chaque serveur DHCP. Remarque : vous devez désinstaller la version précédente du logiciel avant d'installer le logiciel mis à jour.	
Tâches du Sophos NAC Manager		
4.	Exécutez l'assistant de configuration de DHCP pour configurer les serveurs proxy, de correction, de l'agent temporaire et DHCP à utiliser avec la mise en place de DHCP NAC.	
5.	Exécutez le rapport DHCP Enforcer pour : <ul style="list-style-type: none"> ■ Déterminer si les systèmes d'extrémité connus vont recevoir l'accès réseau approprié lorsque l'application de DHCP sera activée. ■ Rechercher les systèmes d'extrémité nécessitant une exemption. 	
6.	Créez des exemptions pour les systèmes d'extrémité qui ne sont pas en mesure d'exécuter Compliance Agent, tels que les systèmes d'extrémité avec systèmes d'exploitation non Windows. Les exemptions s'appliquent également aux systèmes d'extrémité ne nécessitant pas la vérification de leur conformité, tels que les serveurs, les routeurs et les imprimantes. Remarque : pour les systèmes d'extrémité nécessitant la protection NAC, utilisez Sophos Enterprise Console pour installer Compliance Agent.	
7.	Activez l'application de DHCP	

4 Installation du logiciel DHCP Enforcer

Installez le logiciel DHCP Enforcer sur chaque serveur Microsoft DHCP. Le logiciel DHCP Enforcer inclut DHCP Enforcer et l'outil de configuration DHCP Enforcer Configuration Utility. Le serveur DHCP est configuré lors de l'installation. Si vous devez modifier les paramètres du serveur DHCP qui ont été définis lors de l'installation de DHCP Enforcer, utilisez l'outil de configuration DHCP Enforcer Configuration Utility. Pour plus d'informations, reportez-vous à la section [Annexe A : utilisation de l'outil de configuration DHCP](#) à la page 19.

Remarque: vous devez désinstaller la version précédente du logiciel avant d'installer le logiciel mis à jour.

1. Allez sur le site Web de Sophos, téléchargez le programme d'installation Sophos NAC DHCP Enforcer et exécutez-le.
Autrement, insérez le CD-ROM Sophos DHCP Enforcer Install CD. Le CD-ROM doit démarrer automatiquement.
2. Un assistant d'installation se lance. Dans la boîte de dialogue **Welcome**, cliquez sur **Next**.
3. Dans la boîte de dialogue **Sophos DHCP Enforcer**, saisissez l'adresse IP du serveur NAC, la clé partagée du serveur NAC et confirmez cette clé partagée. Cliquez sur **Next**.
Conservez une trace de la clé partagée que vous avez saisie. La même clé partagée doit être saisie lorsque vous lancez l'assistant DHCP Configuration Wizard à l'aide du NAC Manager.
4. Dans la boîte de dialogue **Ready to Install the Program**, cliquez sur **Install** pour installer DHCP Enforcer.
5. Cliquez sur **Finish**.
Dès que vous avez installé DHCP Enforcer sur chaque serveur DHCP, utilisez le NAC Manager pour configurer vos serveurs DHCP afin qu'ils fonctionnent avec Sophos NAC. Pour plus d'informations, reportez-vous à la section [Tâches du NAC Manager](#) à la page 7.

4.1 Désinstallation du logiciel DHCP Enforcer

1. Depuis le menu Démarrer, sélectionnez **Panneau de configuration > Ajouter ou supprimer des programmes**.
2. Sélectionnez **Sophos DHCP Enforcer Software** et cliquez sur **Supprimer**.
3. Cliquez sur **Oui** pour confirmer la suppression du logiciel DHCP Enforcer.

5 Tâches du NAC Manager

L'application du protocole DHCP nécessite une configuration minimale à l'aide du NAC Manager. L'application du protocole DHCP est paramétrée par défaut sur Report Only. Vous devez activer l'application.

- Les **systèmes d'extrémité inconnus** ne sont pas administrés par la Sophos Enterprise Console, ne disposent pas du Compliance Agent, ne sont pas exemptés et n'ont pas exécuté l'agent temporaire.
- Les **systèmes d'extrémité connus** sont administrés par la Sophos Enterprise Console, disposent et exécutent le Compliance Agent.

Remarque : créez des exemptions pour les systèmes d'extrémité qui ne sont pas en mesure d'exécuter Compliance Agent, tels que les systèmes d'extrémité avec systèmes d'exploitation non Windows. Les exemptions s'appliquent également aux systèmes d'extrémité ne nécessitant pas la vérification de leur conformité, tels que les serveurs, les routeurs et les imprimantes. Les systèmes d'extrémité recevant une adresse IP affectée de manière dynamique par le biais de DHCP sont les seuls systèmes d'extrémité devant être exemptés.

Effectuez les tâches suivantes dans le NAC Manager :

1. Exécutez l'assistant de configuration de DHCP pour configurer les serveurs proxy, de correction, de l'agent temporaire et DHCP à utiliser avec la mise en place de DHCP NAC.
2. Exécutez le rapport NAC Manager DHCP Enforcer pour déterminer si les systèmes d'extrémité connus vont recevoir l'accès réseau approprié lorsque l'application du protocole DHCP sera activée. Recherchez également les systèmes d'extrémité nécessitant une exemption.
3. Créez des exemptions pour les systèmes d'extrémité qui ne sont pas en mesure d'exécuter Compliance Agent ou qui ne nécessitent pas la vérification de conformité.
4. Activez l'application du protocole DHCP.

5.1 Exécution de l'assistant de configuration de DHCP

L'assistant de configuration de DHCP vous aide à identifier les serveurs proxy, de correction, de l'agent temporaire et DHCP à utiliser avec les mises en place de Sophos NAC DHCP et configure automatiquement les modèles d'accès DHCP Enforcer par défaut avec vos définitions de serveurs.

Procédure

1. Ouvrez une session sur le NAC Manager.
2. Cliquez sur **Configure System > DHCP Configuration Wizard**. Cliquez sur **Next** pour continuer.
3. Procédez de l'une des manières suivantes :
 - Si vous utilisez des serveurs proxy, cliquez sur **Yes** et cliquez sur **Next**. Passez à l'étape suivante.
 - Si vous n'utilisez **pas** de serveurs proxy, cliquez sur **No** et cliquez sur **Next**. Passez à l'étape 5.

4. Définissez les serveurs proxy requis pour autoriser l'accès Internet et cliquez sur **Next**.
Procédez de l'une des manières suivantes :
 - Dessélectionnez les cases des serveurs que vous ne souhaitez **pas** inclure en tant que serveur proxy.
 - Cliquez sur **Add** pour ajouter de nouveaux serveurs, puis saisissez les informations du serveur proxy et cliquez sur **OK**. Répétez cette étape autant de fois que nécessaire pour ajouter d'autres serveurs. Dès qu'ils sont créés, ces serveurs peuvent être administrés sur la page **Enforce > Network Resources**.

Remarque : les serveurs proxy sélectionnés remplaceront les serveurs actuellement utilisés dans le modèle d'accès DHCP - Internet Access DHCP Enforcer par défaut.
5. Définissez les serveurs de correction requis pour autoriser l'accès aux opérations de correction, tels que les contrôleurs de domaine, et cliquez sur **Next**.
Procédez de l'une des manières suivantes :
 - Dessélectionnez les cases des serveurs que vous ne souhaitez **pas** inclure en tant que serveur de correction.
 - Cliquez sur **Add** pour ajouter de nouveaux serveurs, puis saisissez les informations du serveur de correction et cliquez sur **OK**. Répétez cette étape autant de fois que nécessaire pour ajouter d'autres serveurs. Dès qu'ils sont créés, ces serveurs peuvent être administrés sur la page **Enforce > Network Resources**.

Remarque : les serveurs de correction sélectionnés remplaceront les serveurs en cours d'utilisation dans le modèle d'accès DHCP - Remediation Access DHCP Enforcer par défaut.
6. Procédez de l'une des manières suivantes :
 - Si vous avez installé l'agent temporaire, cliquez sur **Yes** puis, cliquez sur **Next**. Passez à l'étape suivante.
 - Si vous n'avez **pas** installé l'agent temporaire, cliquez sur **No** puis, cliquez sur **Next**. Passez à l'étape 8.

Remarque : si vous avez installé l'agent temporaire sur le même serveur que Sophos NAC, il n'est pas nécessaire de créer un serveur de l'agent temporaire supplémentaire.
7. Définissez les serveurs hébergeant l'agent temporaire afin que DHCP Enforcer puisse y accéder. Cet accès est requis afin que les systèmes d'extrémité inconnus, tels que les invités, puissent être connus du réseau. Cliquez sur **Add** pour ajouter de nouveaux serveurs, puis, saisissez les informations du serveur de l'agent temporaire et cliquez sur **OK**. Puis, cliquez sur **Next**. Dès qu'ils sont créés, ces serveurs peuvent être administrés sur la page **Configure System > Server Settings**.
8. Définissez les serveurs qui seront utilisés pour l'application de DHCP. Cliquez sur **Add** pour ajouter de nouveaux serveurs, puis, saisissez les informations du serveur DHCP Enforcer et cliquez sur **OK**. Répétez cette étape autant de fois que nécessaire pour ajouter d'autres serveurs. Puis, cliquez sur **Next**. Dès qu'ils sont créés, ces serveurs peuvent être administrés sur la page **Configure System > Server Settings**.
9. Cliquez sur **Finish**.

5.2 Exécution du rapport DHCP Enforcer

Exécutez le rapport Sophos NAC DHCP Enforcer pour déterminer l'état de conformité des systèmes d'extrémité avant d'activer l'application du protocole DHCP. Les stratégies NAC prédéfinies sont paramétrées sur Report Only. Le rapport DHCP Enforcer peut être utilisé pour déterminer si le bon modèle d'accès sera appliquée lorsque la mise en application sera activée. Vous pouvez exempter des périphériques et accéder aux détails de l'évaluation depuis le rapport DHCP Enforcer.

Procédure

1. Ouvrez une session sur le NAC Manager.
2. Cliquez sur **Report > Troubleshooting**.
3. Cliquez sur la liste **Report Type** et sélectionnez **DHCP Enforcer**.
4. Le cas échéant, cliquez sur le **signe plus** se trouvant à côté de **Report Criteria** et saisissez ou sélectionnez les options de recherche appropriées. Vous pouvez aussi cliquer sur le lien **Custom Sort** pour étendre vos options de triage. Les options de tri personnalisées du rapport sont modifiées temporairement lors de son exécution.

Remarque : vous pouvez utiliser le symbole * ou % pour effectuer une recherche avec un caractère joker sur la plupart des champs. Par exemple, si vous tapez M% dans le champ Returned User Class, toutes les classes utilisateur qui commencent par un M s'affichent. De même, si vous tapez M sans le symbole % dans le champ Returned User Class, seules les classes utilisateur qui s'appellent M s'affichent.

5. Cliquez sur **Run**.

Champs et descriptions

Champ	Description
Entrée du rapport Summary	
Date/Time	Date et heure de la tentative d'accès réseau. Remarque : la date et l'heure proviennent du fuseau horaire du navigateur Web accédant au NAC Manager.
MAC Address	Adresse MAC du périphérique tentant de se connecter au réseau. L'adresse MAC qui apparaît est affectée au NIC associé à la requête DHCP du client.
Computer Name	Nom du périphérique tentant de se connecter au réseau. Le nom de l'ordinateur est dérivé de la requête du client.
Compliance Status	Etat de conformité du système d'extrémité, affecté lors de l'évaluation de la conformité. Les états de conformité disponibles sont Compliant (conforme), Partially Compliant (partiellement conforme) et Non-Compliant (non conforme). Trois tirets (---) signifient que l'agent n'a pas signalé d'état de conformité. Les modèles d'accès DHCP Enforcer associés à l'état de conformité de stratégie déterminent l'accès réseau.

Champ	Description
Template Name (Version)	<p>Nom et version du modèle d'accès qui détermine l'action prise par le DHCP Enforcer. Le modèle d'accès utilisé est basé sur la raison. Les modèles d'accès disponibles incluent les modèles par défaut suivants ainsi que tous les modèles d'accès que vous avez créés :</p> <ul style="list-style-type: none"> ■ DHCP - Full Access : autorise l'accès intégral au réseau. ■ DHCP - Internet Access : autorise tous les accès au réseau sauf au réseau local (LAN). ■ DHCP - Remediation Access : refuse tout accès au réseau sauf au serveur NAC Sophos et au serveur de l'agent temporaire.
Reason	<p>Raison pour laquelle un modèle d'accès particulier a été affecté par le DHCP Enforcer. Les conditions disponibles sont :</p> <ul style="list-style-type: none"> ■ Assessment : l'évaluation effectuée par l'agent a déterminé l'état de conformité. Les modèles d'accès DHCP Enforcer associés à l'état de conformité de stratégie déterminent l'accès réseau. Un lien apparaît vers les informations d'évaluation de conformité associée à cette entrée DHCP Enforcer. ■ Default Template : le système d'extrémité peut avoir une stratégie associée ou être une exemption désignée, mais aucun modèle d'accès associé n'a été trouvé. Les modèles d'accès par défaut désignés dans la zone Configure System > Enforcer Settings déterminent l'accès réseau. ■ Enforcer Override : l'application n'a pas été vérifiée. Si la case à cocher Override DHCP Enforcer est sélectionnée dans la zone Configure System > Enforcer Settings, ce sont les modèles d'accès Maintenance Mode/Enforcer Override aussi désignés dans cette zone qui déterminent l'accès réseau. ■ Exempted : le système d'extrémité est exempté selon les critères d'exemption définis dans la zone Enforce > Exemptions. Les modèles d'accès associés aux critères d'exemption déterminent l'accès réseau. Les sous-raisons Exempted apparaissent entre parenthèses : <ul style="list-style-type: none"> ■ User Class : la classe d'utilisateur a été spécifiée comme une exemption. ■ Vendor Class : la classe du fournisseur a été spécifiée comme une exemption. ■ MAC : l'adresse MAC a été spécifiée comme une exemption. ■ IP Scope : l'étendue IP a été spécifiée comme une exemption. ■ Maintenance Mode : le logiciel est en mode de maintenance. Les modèles d'accès Maintenance Mode/Enforcer Override désignés dans la zone Configure System > Enforcer Settings déterminent l'accès réseau. ■ Policy Retrieval Error : l'état de conformité du système d'extrémité est obsolète d'après le champ DHCP Policy Update Threshold configuré dans la zone Configure System > Enforcer Settings. Les modèles d'accès DHCP Enforcer de la stratégie associés à l'état Policy Retrieval Error déterminent l'accès réseau.

Champ	Description
	<ul style="list-style-type: none"> ■ Remediate : la stratégie est en mode Remediate. Les modèles d'accès DHCP Enforcer associés au mode de stratégie Remediate déterminent l'accès réseau. ■ Report Only : la stratégie est en mode Report Only. Les modèles d'accès DHCP Enforcer associés au mode de stratégie Report Only déterminent l'accès réseau. ■ Reserved : l'adresse MAC du périphérique demandant l'accès réseau est réservé pour un périphérique particulier sur le serveur DHCP. ■ System Error : Enforcer a rencontré une erreur qui a empêché le succès de l'opération. Le paramètre du registre SystemErrors sur le serveur NAC de Sophos est défini par défaut pour refuser l'accès réseau. ■ Template Error : un modèle d'accès associé était introuvable et les modèles d'accès Default désignés dans la zone Configure System > Enforcer Settings n'ont pas pu être utilisés. Si cette erreur survient, l'accès réseau est déterminé par le serveur DHCP, lequel ne renverra pas de classe d'utilisateur et refusera l'accès à l'utilisateur. ■ Unknown Endpoint : aucun enregistrement de conformité n'existe. Les modèles d'accès Unknown Endpoint désignés dans la zone Configure System > Enforcer Settings déterminent l'accès réseau.
Returned User Class	Classe d'utilisateur DHCP renvoyée au serveur DHCP par le DHCP Enforcer pour application.
DHCP Server	Adresse IP du serveur DHCP demandant l'accès réseau depuis le DHCP Enforcer. Il s'agit du serveur DHCP sur lequel le logiciel DHCP Enforcer est installé.
Entrée du rapport Detailed	
Agent Enforcement Action	<p>Action prise par le système d'extrémité concernant l'affectation des adresses IP. Le système d'extrémité initialise la publication et le renouvellement des adresses IP d'après l'action d'application d'agents spécifiée dans la stratégie. L'agent obtient de nouvelles adresses IP lorsqu'il démarre et lance une évaluation de conformité, lorsque l'état de conformité du système d'extrémité change, lorsque le mode de stratégie change et lorsque les modèles d'accès DHCP Enforcer définis dans la stratégie du système d'extrémité changent. Les valeurs disponibles incluent :</p> <ul style="list-style-type: none"> ■ None : les adresses IP du système d'extrémité ne sont ni publiées ni renouvelées. ■ Release Renew : les adresses IP du système d'extrémité sont publiées, puis renouvelées à l'aide du serveur DHCP. Les adresses IP courantes sont laissées de côté avant l'obtention de nouvelles. ■ Triple Dash (---) : l'agent n'a pas signalé d'action.
Vendor Class	Classe du fournisseur du client DHCP.

Champ	Description
DHCP Relay	Adresse IP du relais DHCP (s'il est présent dans la requête DHCP originale) utilisé par le DHCP Enforcer pour sélectionner un modèle d'accès DHCP Enforcer. 0.0.0.0 apparaît si un relais DHCP n'est pas utilisé.
Transaction ID	Identifiant de transaction renvoyé depuis le serveur DHCP. L'identifiant de transaction associe les messages du client DHCP avec les réponses du serveur.

5.3 Création d'exemptions DHCP

Les systèmes d'extrémité exemptés ne sont pas en mesure d'exécuter le Compliance Agent, tels que les systèmes d'extrémité avec systèmes d'exploitation non Windows. Les exemptions s'appliquent également aux systèmes d'extrémité ne nécessitant pas la vérification de leur conformité, tels que les serveurs, les routeurs et les imprimantes. Les systèmes d'extrémité recevant une adresse IP affectée de manière dynamique par le biais de DHCP sont les seuls systèmes d'extrémité devant être exemptés. Vous devez créer les exemptions DHCP pour ces systèmes d'extrémité ou alors ces systèmes d'extrémité seront interdits d'accès au réseau lorsque vous activerez l'application de DHCP.

A l'aide du NAC Manager, vous pouvez créer deux types d'exemptions DHCP :

- **Exemptions par critères DHCP :** exemptions créées par l'adresse MAC, la classe d'utilisateur et la classe du fournisseur.
- **Exemptions par étendues IP :** exemptions créées pour les segments réseau.

5.3.1 Création d'exemptions par critères DHCP

Utilisez la page NAC Manager Exemptions pour créer des exemptions par critères DHCP. Les critères d'exemption et les modèles d'accès DHCP Enforcer sont utilisés conjointement les uns avec les autres pour identifier les exemptions et indiquer des actions. Une fois que le critère d'exemption défini est trouvé, les modèles d'accès DHCP Enforcer déterminent l'action d'accès réseau appropriée à prendre.

Procédure

1. Ouvrez une session sur le NAC Manager.
2. Cliquez sur **Enforce > Exemptions**. Puis cliquez sur **Create Exemption** dans la section inférieure gauche de la page.
3. Saisissez un nom et une description d'exemption.
4. Cliquez sur la zone de liste **Exemption Type** et sélectionnez **DHCP Criteria**.

5. Sous Exemption Criteria, sélectionnez l'option **MAC Address**, **User Class** ou **Vendor Class** pour spécifier les critères d'exemption que vous voulez définir, saisissez l'adresse MAC (ou le préfixe) appropriée, la classe d'utilisateur ou la classe de fournisseur dans le champ prévu, puis cliquez sur **Add**.

Répétez cette opération autant que nécessaire pour ajouter des critères d'exemption supplémentaires.

Remarque : vous pouvez utiliser le * pour spécifier des exemptions avec des caractères joker à partir du moment où le symbole * est en dernier. Par exemple, si vous spécifiez AA* comme adresse MAC, toutes les adresses PAC commençant par AA seront exemptées. Si vous spécifiez une adresse MAC sans le symbole *, vous devez spécifier l'adresse MAC exacte que vous voulez exempter.

6. Cliquez sur **Select** pour ajouter des modèles d'accès DHCP Enforcer à l'exemption, sélectionnez le modèle d'accès **DHCP - Full Access** et cliquez sur **OK**.

Le modèle d'accès **DHCP - Full Access** est prédéfini dans Sophos NAC pour permettre l'accès au réseau. Vous avez configuré cette exemption pour accéder au réseau sans évaluation de la conformité par Sophos NAC.

7. Cliquez sur **Save**.

5.3.2 Création d'exemptions par étendues IP

Les systèmes d'extrémité recevant une adresse IP affectée de manière dynamique par le biais de DHCP sont les seuls systèmes d'extrémité devant être exemptés. Utilisez la page Exemptions du NAC Manager pour créer des exemptions par étendues IP. Les exemptions par étendues IP sont des exemptions créées pour les segments de réseau. Les exemptions par étendues IP sont utiles lors d'un déploiement par phases de l'application dans toute l'entreprise, vous pouvez exempter des segments de réseau que vous ne souhaitez pas encore appliquer.

Procédure

1. Ouvrez une session sur le NAC Manager.
2. Cliquez sur **Enforce > Exemptions**. Puis cliquez sur **Create Exemption** dans la section inférieure gauche de la page.
3. Saisissez un nom et une description d'exemption.
4. Cliquez sur la liste **Exemption Type** et sélectionnez **IP Scope**.
5. Sous Exempted IP Scopes, cliquez sur **Select** pour ajouter des étendues IP existantes à l'exemption, sélectionnez les étendues appropriées et cliquez sur **OK**.

Si vous ne voyez pas l'étendue IP dont vous avez besoin, vous pouvez en créer une. Pour cela, créez un nouveau modèle d'accès DHCP Enforcer ou mettez à jour un des modèles d'accès DHCP Enforcer prédéfinis.

6. Si nécessaire, utilisez les flèches pour classer les étendues par ordre de priorité.

Si plusieurs étendues IP s'appliquent à une exemption particulière, la première étendue IP rencontrée sera utilisée. Sophos vous recommande de classer par ordre de priorité les étendues les plus spécifiques/strictes, puis les moins spécifiques/strictes.

7. Cliquez sur **Save**.

Important : une fois que vous avez créé des exemptions, vous pouvez les classer par ordre de priorité sur la page de liste **Exemptions**. Si plusieurs exemptions s'appliquent à un système d'extrémité particulier, la première exemption associée à ce système sera utilisée. Sophos vous recommande de classer par ordre de priorité les exemptions les plus spécifiques/strictes, puis les moins spécifiques/strictes.

5.4 Activation de l'application de DHCP

Vous pouvez activer l'application de DHCP pour les systèmes d'extrémité inconnus et connus. Cette souplesse d'utilisation vous permet d'utiliser l'application de DHCP pour les systèmes d'extrémité inconnus et l'application de l'agent pour les systèmes d'extrémité connus.

5.4.1 Activation de l'application de DHCP pour les systèmes d'extrémité inconnus

Vous pouvez activer l'application de DHCP pour les systèmes d'extrémité inconnus sur chaque serveur DHCP. Ainsi, vous pouvez spécifier quels serveurs DHCP mettra en quarantaine les systèmes d'extrémité inconnus. Utilisez cette fonction pour effectuer un déploiement par étapes de l'application de DHCP.

Avant d'activer l'application de DHCP pour les systèmes d'extrémité inconnus, vous devez créer des exemptions. Les systèmes d'extrémité recevant une adresse IP affectée de manière dynamique par le biais de DHCP sont les seuls systèmes d'extrémité devant être exemptés. Pour plus d'informations, reportez-vous à la section [Création d'exemptions DHCP](#) à la page 12.

Procédure

1. Cliquez sur **Configure System > Server Settings**.
2. Cliquez sur le nom du serveur DHCP pour lequel vous souhaitez activer l'application de DHCP.
3. Cliquez sur la liste **Unknown Endpoint Mode** et sélectionnez **Enforce**.

Remarque : par défaut, le modèle d'accès **DHCP - Remediation Access** détermine l'accès au réseau. Ce modèle met en quarantaine le système d'extrémité et autorise l'accès aux serveurs de correction que vous avez défini lors de l'exécution de l'assistant de configuration de DHCP. Vous pouvez changer le modèle d'accès dans la zone **Configure System > Enforcer Settings**.

4. Cliquez sur **Save**.

5.4.2 Activation de l'application du protocole DHCP pour les systèmes d'extrémité connus

Si vous envisagez d'utiliser l'application du protocole DHCP soit à la place, soit en supplément de l'application de l'agent pour les systèmes d'extrémité connus, vous devez changer le mode de vos stratégies dans Policy Mode de Report Only sur Enforce.

Important : toutes les stratégies et changements de stratégies s'appliquent immédiatement, en revanche, une stratégie ne s'applique pas au système d'extrémité tant que l'agent ne la récupère pas.

Procédure

1. Ouvrez une session sur le NAC Manager.
2. Cliquez sur **Manage > Politiques**. Puis cliquez sur le nom de la stratégie que vous voulez mettre à jour. Pour plus d'informations sur les stratégies prédéfinies, reportez-vous à la section [Utilisation des stratégies prédéfinies](#) à la page 16.
3. Cliquez sur la liste **Policy Mode** et sélectionnez **Enforce**.
 - **Enforce :** le mode de stratégie Enforce spécifie que les systèmes d'extrémité sont évalués par rapport à la stratégie affectée et les informations de rapport sont générées dans le NAC Manager. Les messages apparaissent, les actions correctives sont exécutées et des actions d'application sont prises à travers l'utilisation de modèles d'accès pour l'état d'accès approprié. Le mode Enforce utilise les modèles d'accès affectés à l'étape 5.
4. Cliquez sur la liste **Agent Enforcement Action** et sélectionnez **Release Renew**. Vous devez sélectionner Release Renew lors de l'utilisation de l'application DHCP pour les systèmes d'extrémité connus.
5. Dans la zone de navigation gauche Network Access, cliquez sur **DHCP**. Cliquez sur l'onglet **Enforce** et vérifiez les affectations des modèles d'accès.

Remarque : par défaut, chaque stratégie est automatiquement chargée avec les modèles d'accès. Assurez-vous que les modèles d'accès corrects sont appliqués. Conservez les affectations des modèles d'accès Report Only et Remediate.

Affectations du modèle d'accès DHCP Enforcer prédéfini

- **Policy Retrieval Error :** l'état de conformité du système d'extrémité est obsolète d'après le champ DHCP Policy Update Threshold configuré dans la zone **Configure System > Enforcer Settings**. Le modèle d'accès DHCP - Remediation Access refuse l'accès au réseau sauf aux serveurs de correction que vous avez défini lors de l'exécution de l'assistant de configuration de DHCP.
 - **Compliant :** le système d'extrémité est conforme. Le modèle d'accès DHCP - Full Access autorise l'accès au réseau lorsque le système d'extrémité est conforme.
 - **Partially Compliant :** le système d'extrémité est partiellement conforme. Le modèle d'accès DHCP - Full Access autorise l'accès au réseau lorsque le système d'extrémité est conforme.
 - **Non-Compliant :** le système d'extrémité est non conforme. Le modèle d'accès DHCP - Remediation Access refuse l'accès au réseau sauf aux serveurs de correction que vous avez défini lors de l'exécution de l'assistant de configuration de DHCP.
6. Si nécessaire, utilisez les flèches pour classer par ordre de priorité les modèles d'accès DHCP Enforcer.

Si plusieurs modèles s'appliquent à un état particulier, le premier modèle correspondant à l'état est utilisé. Sophos vous recommande d'attribuer d'abord les modèles d'accès les plus spécifiques/stricts et ensuite les modèles d'accès les moins spécifiques/stricts.
 7. Cliquez sur **Save**.

5.4.2.1 Utilisation des stratégies prédéfinies

Vous pouvez utiliser les stratégies prédéfinies pour appliquer la conformité de la sécurité pour les systèmes d'extrémité administrés et non administrés.

- **Valeur par défaut :** cette stratégie est utilisée si Compliance Agent est installé sur un système d'extrémité et qu'aucune autre stratégie n'a été affectée. Par défaut, le mode de stratégie est paramétré sur Report Only. Cette stratégie effectue des actions correctives sur le système d'extrémité si le mode de stratégie est paramétré sur Remediate ou Enforce.
- **Administrés :** cette stratégie peut être utilisée pour les systèmes d'extrémité qui sont administrés avec la Sophos Enterprise Console et sur lesquels Compliance Agent est installé. Par défaut, le mode de stratégie est paramétré sur Report Only. Cette stratégie effectue des actions correctives sur le système d'extrémité si le mode de stratégie est paramétré sur Remediate ou Enforce.
- **Non administrés :** cette stratégie peut être utilisée pour les systèmes d'extrémité situés hors de l'entreprise. Cette stratégie n'effectue pas d'actions correctives sur le système d'extrémité. L'agent temporaire utilise la stratégie Non administrés.

Remarque : si Compliance Agent n'est pas installé sur un système d'extrémité et si ce dernier n'utilise pas l'agent temporaire, les paramètres Enforcer déterminent l'accès réseau.

5.4.3 Expérience utilisateur de l'application du protocole DHCP

Dès que vous avez activé l'application du protocole DHCP, l'expérience utilisateur de l'application du protocole DHCP dépend de l'état inconnu ou connu du système d'extrémité. En outre, les invités peuvent exécuter le Compliance Dissolvable Agent pour obtenir l'accès au réseau.

- Les **systèmes d'extrémité inconnus** ne sont pas administrés par la Sophos Enterprise Console, ne disposent pas du Compliance Agent, ne sont pas exemptés et n'ont pas exécuté l'agent temporaire.
- Les **systèmes d'extrémité invités** peuvent utiliser le Compliance Dissolvable Agent pour le contrôle d'accès réseau.
- Les **systèmes d'extrémité connus** sont administrés par la Sophos Enterprise Console, disposent du Compliance Agent et l'exécutent.

Expérience utilisateur de l'application du protocole DHCP pour systèmes d'extrémité inconnus

Lorsque l'application du protocole DHCP est activée, les utilisateurs des systèmes d'extrémité inconnus sont soumis à l'expérience suivante :

1. Le système d'extrémité démarre.
2. Lorsque l'application du protocole DHCP pour les systèmes d'extrémité inconnus est activée, les systèmes d'extrémité disposent d'un accès au réseau limité. Ces systèmes d'extrémité ont accès à Internet et à tous les serveurs de correction que vous avez défini lors de l'exécution de l'assistant de configuration de DHCP.

Expérience utilisateur de l'application du protocole DHCP pour systèmes d'extrémité invités

Lorsque l'application du protocole DHCP est activée et que les systèmes d'extrémité invités doivent utiliser le Compliance Dissolvable Agent, les utilisateurs invités sont soumis à l'expérience suivante :

1. Le système d'extrémité démarre.
2. L'utilisateur ouvre Internet Explorer, navigue jusqu'à l'URL du Compliance Dissolvable Agent et exécute le Compliance Dissolvable Agent.
3. Le Compliance Dissolvable Agent effectue une évaluation et détermine si le système d'extrémité est conforme, partiellement conforme ou non conforme à la stratégie NAC.
4. Lorsque l'application du protocole DHCP est configurée et activée, il se passe ce qui suit :
 - Les systèmes d'extrémité conformes sont autorisés à accéder au réseau.
 - Les systèmes d'extrémité partiellement conformes sont autorisés à accéder au réseau. Le Compliance Dissolvable Agent affiche des messages à l'utilisateur afin que celui-ci puisse corriger son système d'extrémité afin qu'il soit conforme. Si la stratégie NAC est configurée pour corriger automatiquement le système d'extrémité, la correction du système d'extrémité a lieu. Par défaut, la correction est désactivée. Dans la plupart des cas, nous vous recommandons de ne pas corriger le système d'extrémité d'un utilisateur invité.
 - Les systèmes d'extrémité non conformes sont interdits d'accès au réseau. Ces systèmes d'extrémité ont accès à Internet et à tous les serveurs de correction que vous avez défini lors de l'exécution de l'assistant de configuration de DHCP. Le Compliance Dissolvable Agent affiche des messages à l'utilisateur afin que celui-ci puisse corriger son système d'extrémité afin qu'il soit conforme. Si la stratégie NAC est configurée pour corriger automatiquement le système d'extrémité, la correction du système d'extrémité a lieu. Par défaut, la correction est désactivée. Dans la plupart des cas, nous vous recommandons de ne pas corriger le système d'extrémité d'un utilisateur invité.

Expérience utilisateur de l'application du protocole DHCP pour les systèmes d'extrémité connus

Lorsque l'application du protocole DHCP est activée, les systèmes d'extrémité connus sont soumis à l'expérience DHCP suivante :

1. Le système d'extrémité démarre et le Compliance Agent s'exécute.
2. Le Compliance Agent effectue une évaluation et détermine si le système d'extrémité est conforme, partiellement conforme ou non conforme à la stratégie NAC.
3. Lorsque l'application du protocole DHCP est configurée et activée, il se passe ce qui suit :
 - Les systèmes d'extrémité conformes sont autorisés à accéder au réseau.
 - Les systèmes d'extrémité partiellement conformes sont autorisés à accéder au réseau. Le Compliance Agent affiche des messages à l'utilisateur afin que celui-ci puisse corriger son système d'extrémité afin qu'il soit conforme. Si la stratégie NAC est configurée pour corriger automatiquement le système d'extrémité, la correction a lieu.
 - Les systèmes d'extrémité non conformes sont interdits d'accès au réseau. Ces systèmes d'extrémité ont accès à Internet et à tous les serveurs de correction que vous avez défini

lors de l'exécution de l'assistant de configuration de DHCP. Le Compliance Agent affiche des messages à l'utilisateur afin que celui-ci puisse corriger son système d'extrémité afin qu'il soit conforme. Si la stratégie NAC est configurée pour corriger automatiquement le système d'extrémité, la correction du système d'extrémité a lieu.

6 Annexe A : utilisation de l'outil de configuration DHCP

Si vous devez modifier les paramètres de DHCP Enforcer qui ont été définis lors de l'installation de DHCP Enforcer, utilisez l'outil de configuration DHCP Enforcer Configuration Utility. Cet outil est installé sur le serveur DHCP lors de l'installation de DHCP Enforcer. Si vous avez plusieurs serveurs DHCP, vous devez modifier les paramètres de DHCP Enforcer sur chaque serveur DHCP.

6.1 Mise à jour de la clé partagée

Procédure

1. Depuis le menu Démarrer du serveur DHCP, sélectionnez **Sophos > NAC > Support Tools > DHCP Enforcer Configuration Utility**.

La boîte de dialogue **DHCP Enforcer Configuration Utility** apparaît avec l'onglet **Enforcer** sélectionné.

2. Dans la boîte de dialogue **DHCP Enforcer Configuration Utility**, cliquez sur le bouton **Edit**.
3. Dans la boîte de dialogue **DHCP Enforcer RADIUS Enforcer Server Settings**, saisissez et confirmez la nouvelle clé partagée et cliquez sur **OK**.

6.2 Mise à jour des paramètres avancés

Cette section vous décrit comment mettre à jour les paramètres avancés de DHCP Enforcer à l'aide de l'outil DHCP Enforcer Configuration Utility. Dans la majorité des cas, ces paramètres ne devraient pas nécessiter de mise à jour.

Procédure

1. Depuis le menu **Démarrer** du serveur DHCP, sélectionnez **Sophos > NAC > Support Tools > DHCP Enforcer Configuration Utility**.

La boîte de dialogue **DHCP Enforcer Configuration Utility** apparaît avec l'onglet **Enforcer** sélectionné.

2. Dans la boîte de dialogue **DHCP Enforcer Configuration Utility**, cliquez sur l'icône **Advanced**.
3. Si nécessaire, modifiez les paramètres DHCP Enforcer.
4. Cliquez sur **OK**.

Répétez ces instructions sur tous les serveurs DHCP auxquelles elles s'appliquent.

6.2.1 Champs et descriptions de l'outil DHCP Configuration Utility

Champs	Descriptions
Onglet Enforcer	
Access for Multiple Servers	Cette option ne s'applique pas à Sophos Endpoint Security and Control.
<p>Boîte de dialogue DHCP Enforcer RADIUS Enforcer Server Settings</p> <p>Cliquez sur l'icône Edit pour accéder à cette boîte de dialogue.</p> <p>Remarque : les champs de cette boîte de dialogue concernent le serveur NAC.</p>	
Enable	Indique si le serveur NAC est activé. Lorsqu'il est activé, le serveur NAC est utilisé dans le cadre de la conformité à la stratégie et de l'activité d'édition de rapports.
IP Address	Indique l'adresse IP du serveur NAC.
Authentication Port	Indique le port d'authentification du serveur NAC.
Accounting Port	Indique le port de gestion de compte du serveur NAC.
Shared Key	Identifie la clé partagée du serveur DHCP. La clé partagée est la même que celle utilisée lors de l'installation de DHCP Enforcer.
Confirm Shared Key	Confirme la clé partagée du serveur DHCP.
Boîte de dialogue DHCP Enforcer Resolve IP	
Hostname	Identifie le nom d'hôte, en cas d'adresse IP inconnue, du serveur NAC. Lorsque vous saisissez le nom d'hôte, vous pouvez résoudre le nom d'hôte en adresse IP.
Onglet Advanced	
Enable Policy Compliance	Lorsque ce champ est sélectionné, les activités de conformité à la stratégie et d'édition de rapports sont activées pour tous les paquets de requêtes DHCP, sauf pour ceux qui sont identifiés par le code d'option réservée.
Attempts	Indique la fréquence d'exécution de la conformité à la stratégie pour un paquet de requêtes DHCP.
Timeout	Indique, en secondes, combien de temps le serveur DHCP attend avant de lancer une nouvelle vérification de conformité à la stratégie.
Default User Class	Identifie la classe d'utilisateur à utiliser s'il est impossible d'obtenir la classe d'utilisateur définie dans la stratégie en raison d'une erreur au cours d'une évaluation de la conformité à la stratégie.

Champs	Descriptions
Error	Lorsque cette option est sélectionnée, elle enregistre les messages d'erreur Microsoft dans le journal des événements de l'application (Application Event Log).
Warning	Lorsque cette option est sélectionnée, elle enregistre les messages d'avertissement Microsoft dans le journal des événements de l'application (Application Event Log).
Information	Lorsque cette option est sélectionnée, elle enregistre les messages d'information Microsoft dans le journal des événements de l'application (Application Event Log).
Trace	Lorsque cette option est sélectionnée, la journalisation du suivi Microsoft est activée et enregistrée dans le journal des événements de l'application (Application Event Log).
Subnet Mask Override	Spécifie le masque de sous-réseau disponible aux utilisateurs qui ne sont pas conformes à la stratégie et annule le sous-réseau du serveur DHCP pour restreindre l'accès au réseau.
Black Hole IP Address	Adresse IP factice utilisée par DHCP Enforcer pour éliminer/exclure le trafic des ressources bloquées.
Boîte de dialogue DHCP Enforcer Informs IP Address	
IP Address	Indique l'adresse IP associée au client, comme un concentrateur d'accès à distance (RAC : remote access concentrator) pour lequel vous souhaitez contourner les activités de vérification de la conformité et d'édition de rapports pour les paquets d'informations DHCP. Par défaut, les activités de vérification de la conformité et d'édition de rapports sont effectuées pour les paquets d'informations DHCP. Lorsqu'une adresse IP est spécifiée, la vérification de la conformité et l'édition de rapports ne sont pas effectuées pour les paquets d'informations DHCP depuis ce client.
Boîte de dialogue DHCP Enforcer Resolve IP	
Hostname	Identifie le nom d'hôte, lorsque l'adresse IP n'est pas connue, du client pour lequel vous souhaitez contourner la vérification de la conformité et l'édition de rapports. Lorsque vous saisissez le nom d'hôte, vous pouvez résoudre le nom d'hôte en adresse IP.

7 Annexe B : mise à niveau de l'application de DHCP

Si vous procédez à la mise à niveau de Endpoint Security and Control 9, votre configuration DHCP ne fonctionnera plus après cette mise à niveau. Vous devez impérativement reconfigurer l'application de DHCP.

La mise à niveau affecte la configuration DHCP de Endpoint Security and Control 8 comme suit :

- Supprime les anciens modèles d'accès DHCP Enforcer de toutes les stratégies et de la page NAC Manager Enforcer Settings.
- Met à jour tous les modèles d'accès DHCP Enforcer que vous avez créés avec l'option DHCP Subnet Override activée pour restreindre l'accès réseau. L'accès à Internet est autorisé.
- Met à jour tous les modèles d'accès DHCP Enforcer que vous avez créés avec l'option DHCP Subnet Override désactivée pour autoriser l'accès réseau.

7.1 Reconfiguration de l'application de DHCP

Lorsque vous procédez à la mise à niveau à Endpoint Security and Control 9, la mise en place de DHCP doit être reconfigurée. Utilisez les instructions suivantes pour continuer à utiliser votre configuration de l'application de DHCP depuis Endpoint Security and Control 8.

1. Ouvrez une session sur le NAC Manager.
2. Cliquez sur **Configure System > Enforcer Settings**.
3. Dans la zone **DHCP Enforce Access Templates**, cliquez sur l'icône **corbeille** située à côté de chaque modèle d'accès DHCP.

Cette étape supprime les modèles d'accès DHCP des paramètres Enforcer (Enforcer Settings) afin que vous puissiez ajouter les modèles d'accès DHCP existant aux paramètres Enforcer au cours des étapes suivantes.

4. Cliquez sur **Select** sous **DHCP Enforcer Access Templates** ; sélectionnez les cases à cocher **Unknown Endpoint (Report Only)**, **Maintenance Mode/Enforcer Override**, et **Default - DHCP Permit (NULL User Class)** et cliquez sur **OK**.

Cette sélection autorise l'accès à tous les systèmes d'extrémité inconnus et autorise l'accès à tous les systèmes d'extrémité lorsque le serveur NAC est en mode de maintenance ou lorsque vous avez sélectionné la case **Override DHCP Enforcer**.

5. Cliquez sur **Select** sous **DHCP Enforcer Access Templates** ; sélectionnez les cases à cocher **Unknown Endpoint (Enforce)**, **Default**, et **Default - DHCP Deny (NACDeny User Class)** et cliquez sur **OK**.

Cette sélection refuse l'accès aux systèmes d'extrémité inconnus lorsque vous activez l'application de DHCP pour les systèmes d'extrémité inconnus. Pour plus d'informations, reportez-vous à la section [Activation de l'application de DHCP pour les systèmes d'extrémité inconnus](#) à la page 14. Cette sélection refuse également l'accès aux systèmes d'extrémité lorsque Sophos NAC n'est pas en mesure de déterminer un modèle d'accès associé.

6. Cliquez sur **Manage > Politiques**. Puis, cliquez sur le nom de la stratégie que vous utilisez pour l'application de DHCP.

7. Dans la zone de navigation gauche **Network Access**, cliquez sur **DHCP**, cliquez sur l'onglet du mode de stratégie **Report Only**, cliquez sur l'icône **corbeille**.

Répétez cette étape pour les onglets du mode de stratégie **Remediate** et **Enforce**.

Cette étape supprime les modèles d'accès DHCP de la stratégie afin que vous puissiez ajouter les modèles d'accès DHCP existants à la stratégie au cours de l'étape suivante.

8. Cliquez sur l'onglet du mode de stratégie **Report Only**, cliquez sur **Select**, sélectionnez la case **Default - DHCP Permit (NULL User Class)** et cliquez sur **OK**.

Répétez cette étape pour les onglets du mode de stratégie **Remediate** et **Enforce**. Pour corriger, sélectionnez le modèle d'accès **Default - DHCP Permit (NULL User Class)**. Pour appliquer, sélectionnez le modèle d'accès **Default - DHCP Deny (NACDeny User Class)**.

Lorsque la stratégie est en mode Report Only ou Remediate, les systèmes d'extrémité sur lesquels Compliance Agent est installé sont autorisés d'accès. Lorsque la stratégie est en mode Enforce, les systèmes d'extrémité sur lesquels Compliance Agent est installé et qui sont non conformes sont interdits d'accès.

9. Cliquez sur **Save**.

L'application de DHCP a été configurée pour que vous puissiez continuer à utiliser la configuration de l'application de DHCP depuis Endpoint Security and Control 8.

8 Support technique

Pour obtenir du support technique, visitez <http://www.sophos.fr/support>.

Si vous contactez le support technique, fournissez autant d'informations que possible, y compris :

- Le(s) numéro(s) de version du logiciel Sophos
- Le(s) système(s) d'exploitation et le(s) niveau(x) de correctif
- Le texte exact de tous les messages d'erreur

9 Copyright

Copyright © 2009 Sophos Group. Tous droits réservés. Aucune partie de cette publication ne peut être reproduite, stockée dans un système de recherche documentaire ou transmise, sous quelque forme ou par quelque moyen que ce soit, électronique, mécanique, photocopie, enregistrement ou autre sauf si vous possédez une licence valide, auquel cas vous pouvez reproduire la licence conformément à ses termes ou si vous avez le consentement préalable écrit du propriétaire du copyright.

Tous les autres noms de produits et de sociétés mentionnés sont des marques ou des marques déposées appartenant à leurs propriétaires respectifs.