

SOPHOS

Sophos NAC Manager Guide de configuration

Version du produit : 3.3

Date du document : septembre 2009



Table des matières

1 A propos de ce guide.....	3
2 Bon usage du NAC Manager	4
3 Configuration du NAC Manager	21
4 Outils NAC	87
5 Glossaire.....	95
6 Support technique.....	101
7 Copyright.....	102

1 A propos de ce guide

Ce guide décrit la configuration de NAC pour le logiciel Sophos Endpoint Security and Control.

Plus particulièrement, il vous présente :

- Le bon usage en matière de configuration de NAC.
- Les instructions de configuration de NAC à l'aide du NAC Manager.
- Les instructions d'utilisation des outils NAC.

Ce guide s'adresse à vous si :

- Vous utilisez l'Enterprise Console.
- Vous utilisez Sophos NAC pour Endpoint Security and Control.
- Vous voulez obtenir des conseils sur les meilleures options pour la configuration de NAC.
- Vous voulez obtenir des instructions sur l'utilisation du NAC Manager.
- Vous voulez des instructions sur l'utilisation des outils NAC.

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.

2 Bon usage du NAC Manager

2.1 Bon usage général

Cette section contient le bon usage applicable au déploiement de Sophos NAC et à l'utilisation du NAC Manager. Ce bon usage s'applique à tout le NAC Manager.

2.1.1 Déploiement de Network Access Control

Processus	Etapes
Utiliser la Sophos Enterprise Console pour protéger les ordinateurs avec Sophos NAC.	<ol style="list-style-type: none"> 1. Depuis la Sophos Enterprise Console, exécutez l'assistant de protection des ordinateurs.
Passer en revue les rapports du NAC Manager pour déterminer l'état de conformité actuel de l'entreprise.	<ol style="list-style-type: none"> 1. Utilisez les rapports du NAC Manager pour déterminer l'état de conformité actuel des utilisateurs. Remarque : les rapports NAC Manager donnent une vue réaliste de la conformité des utilisateurs avec la stratégie Managed de NAC. 2. Utilisez les rapports du NAC Manager pour déterminer si les messages que les utilisateurs recevront sont appropriés. Remarque : les messages ne sont pas vus par les utilisateurs tant que vous ne changez pas le mode de stratégie à corriger ou à appliquer. Vous allez exécuter cette opération dans les étapes qui suivent.
Mettre à jour si besoin est les profils du NAC Manager.	<ol style="list-style-type: none"> 1. Mettez à jour les profils Sophos Anti-virus et/ou Sophos Client Firewall. Vérifiez que ces profils contiennent les systèmes d'exploitation et actions de messagerie et correctives corrects. 2. Utilisez les rapports du NAC Manager pour déterminer si les mises à jour de profils étaient appropriées.
Introduire une stratégie corrective.	<ol style="list-style-type: none"> 1. Mettez à jour la stratégie Managed. Changez le mode de stratégie de Report Only en Remediate. 2. Utilisez les rapports du NAC Manager pour déterminer l'état de conformité actuel. Remarque : avec le temps, les systèmes d'extrémité non conformes et partiellement conformes doivent être corrigés pour devenir conformes.

Processus	Etapes
Si besoin est, créer ou mettre à jour les modèles d'accès.	<ol style="list-style-type: none"> 1. Créez ou mettez à jour les modèles d'accès. Remarque : si vous prévoyez d'appliquer l'accès réseau à l'aide de l'application de l'agent, créez ou mettez à jour les modèles d'accès Agent Enforcer. Si vous prévoyez d'appliquer l'accès réseau à l'aide de l'application de DHCP, créez ou mettez à jour les modèles d'accès DHCP Enforcer. Pour plus d'informations, reportez-vous à la section Test des modèles d'accès pour des paramètres d'application exacts à la page 5. 2. Utilisez les rapports du NAC Manager pour déterminer si les modèles d'accès donneraient à chaque poste d'extrémité l'accès réseau correct.
Introduire une stratégie d'application.	<ol style="list-style-type: none"> 1. Mettez à jour la stratégie Managed. Changez le mode de stratégie de Remediate en Enforce. 2. Utilisez les rapports du NAC Manager pour déterminer l'état de conformité actuel. Remarque : avec le temps, les systèmes d'extrémité non conformes ou partiellement conformes doivent être corrigés ou l'accès au réseau sera refusé à leurs utilisateurs.

2.1.2 Test des modèles d'accès pour des paramètres d'application exacts

Bon usage	Description
<p>Ajouter des modèles d'accès à une stratégie pour voir si le modèle d'accès approprié est affecté au système d'extrémité.</p> <p>Pour plus d'informations sur le test des stratégies ou sur le déploiement de Sophos NAC, reportez-vous à la section Déploiement de Network Access Control à la page 4.</p>	<p>Assurez-vous que pour chaque modèle d'accès, les actions d'application correctes sont exécutées pour les états d'accès. Vérifiez que les exemptions sont exemptées. Consultez les rapports Agent Enforcer, DHCP Enforcer ou d'exemptions DHCP dans le NAC Manager pour voir quel modèle d'accès a été appliqué sur le système d'extrémité, la raison pour laquelle le modèle d'accès a été appliqué et des détails sur l'action d'application.</p>

2.1.3 Utilisation du bouton Save As New

Bon usage	Description
Utiliser le bouton Save As New pour enregistrer un profil ou un modèle d'accès existant sous un nouveau nom et effectuer des mises à jour.	L'enregistrement sous la forme d'un nouvel élément vous permet de dupliquer un profil ou un modèle d'accès si vous ne voulez pas ou ne pouvez pas modifier celui existant.
Utiliser le bouton Save as New pour mettre à jour un profil ou un modèle d'accès déjà appliqué aux stratégies à moins que vous ne vouliez que les changements soient effectifs immédiatement.	Si vous mettez à jour un profil ou un modèle d'accès existant déjà appliqué aux stratégies, les changements sont effectifs immédiatement et appliqués à la récupération suivante par l'agent de la stratégie. En résumé, utilisez le bouton Save As New à moins que vous vouliez que les changements soient effectifs immédiatement.

2.1.4 Utilisation de la fonction de verrouillage

Bon usage	Description
Verrouiller les stratégies, les profils, les modèles d'accès et les ressources réseau pour empêcher les changements involontaires.	<p>Le verrouillage de ces éléments NAC Manager empêche les changements involontaires. L'administrateur peut uniquement déverrouiller les éléments qu'il a verrouillés. L'administrateur système peut déverrouiller tous les éléments.</p> <p>Remarque : pour garantir qu'une stratégie demeure protégée, vous devez verrouiller tous les profils, modèles d'accès et ressources réseau associés à cette stratégie en plus de la stratégie elle-même.</p>

2.2 Bon usage des stratégies

Cette section présente le bon usage pour les stratégies. Les conventions utilisées pour les stratégies sont les suivantes :

- **Policy Mode :** le mode de stratégie détermine comment la stratégie évalue le système d'extrémité, génère des rapports d'information dans le NAC Manager et détermine si un message doit être envoyé à l'utilisateur, si des actions correctives doivent être effectuées et/ou si des actions d'application doivent être prises.
- **Profiles :** les profils vous permettent de définir les éléments que vous souhaitez voir évalués sur le système d'extrémité, comme les systèmes d'exploitation et les applications.

- **Access Templates** : les modèles d'accès déterminent comment l'accès réseau est accordé aux systèmes d'extrémité.

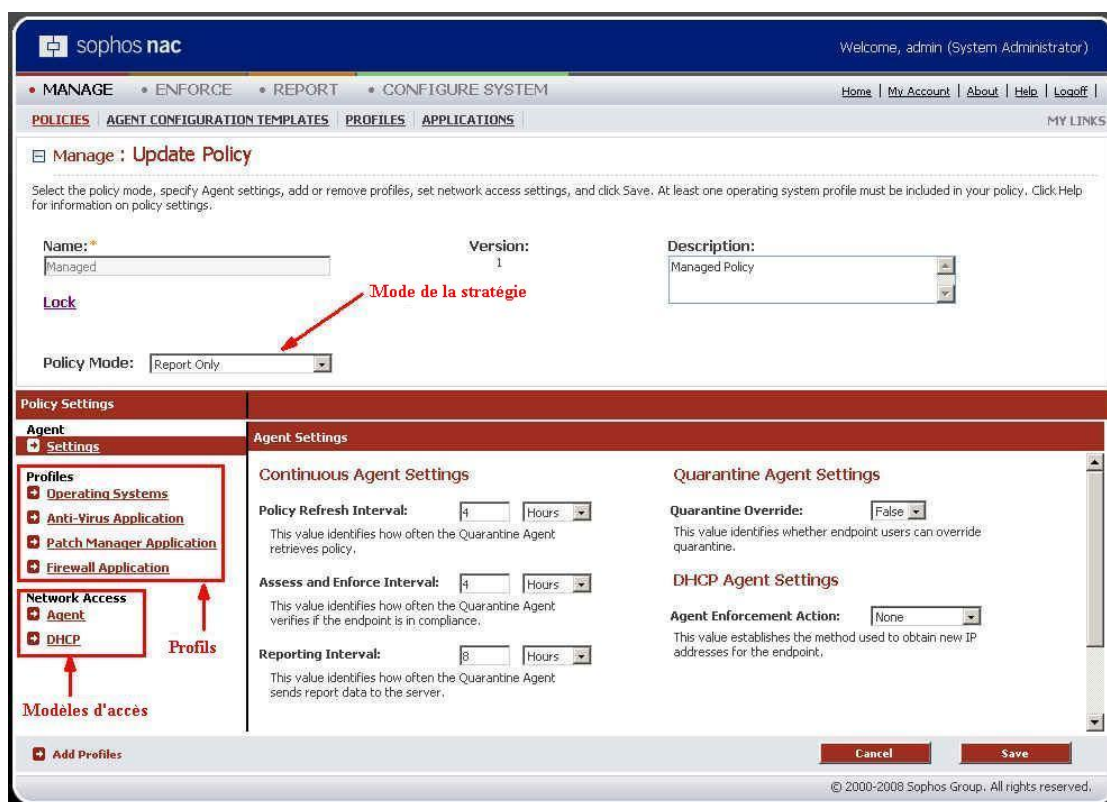


Schéma 1 : exemple de conventions des stratégies

2.2.1 Définition du mode de stratégie approprié

Important : vous devez vérifier que les modèles d'accès appropriés des modes de stratégie Report Only et Remediate sont associés à la stratégie. Si vous appliquez un modèle d'accès Enforcer qui empêche l'accès au réseau en modes Report Only ou Remediate, tous les systèmes d'extrémité seront interdits d'accès quel que soit l'état en cours de leur conformité. Pour appliquer un état de conformité, vous devez impérativement changer le mode de stratégie sur Enforce.

Bon usage	Description
Utiliser le mode Report Only pour vérifier l'état de conformité d'une entreprise.	Le mode Report Only est un moyen pour vous de rassembler des rapports d'information sur l'état de conformité de votre entreprise. Ce mode est le plus discret pour l'utilisateur.
Utiliser le mode Remediate pour signaler les utilisateurs non conformes et effectuer des actions correctives afin de les mettre en conformité avec les stratégies définies.	Le mode Remediate vous permet de signaler les utilisateurs non conformes et d'effectuer des actions correctives afin de les mettre en conformité avec les stratégies définies. Ce mode est aussi un moyen d'obtenir la conformité à la stratégie avant d'activer l'application.

Bon usage	Description
Utiliser le mode Enforce pour signaler, corriger et appliquer la conformité du réseau. Si les utilisateurs ne sont pas conformes à la stratégie, l'accès au réseau leur est refusé.	Le mode Enforce vous permet de signaler, corriger et appliquer la mise en conformité du réseau. Les modèles d'accès (Agent et/ou DHCP) sélectionnés dans la stratégie déterminent l'accès réseau. Si plusieurs modèles d'accès s'appliquent à un état particulier, le premier modèle qui correspond à l'état est utilisé.

2.2.2 Utilisation de la fonction d'annulation de la quarantaine uniquement lorsque l'accès au réseau est impératif

Bon usage	Description
Définir la fonction d'annulation de la quarantaine (Quarantine Override) sur true uniquement lorsque l'accès au réseau est absolument nécessaire à l'activité professionnelle et que les risques pour la sécurité sont minimes ou inexistants.	Le paramétrage de l'annulation de la quarantaine sur True permet à l'utilisateur de supprimer le système d'extrémité depuis la quarantaine même si ce dernier n'est pas conforme.

2.2.3 Gestion des stratégies contenant seulement les profils nécessaires

Bon usage	Description
Gérer les stratégies qui contiennent seulement les profils nécessaires. Supprimer les profils obsolètes de toutes les stratégies.	Gestion des stratégies contenant seulement les profils antivirus, de pare-feu personnel, antispyware et de système d'exploitation nécessaires afin qu'elles soient plus faciles à gérer et à supporter.

2.2.4 Ajout et classement par ordre de priorité des profils dans les stratégies

Bon usage	Description
Ajouter les profils de système d'exploitation à la stratégie, puis les classer par ordre de priorité.	<p>Les stratégies doivent contenir les profils de chaque système d'exploitation que vous voulez évaluer. Classez par ordre de priorité le plus important système d'exploitation en premier.</p> <p>Si l'un des systèmes d'exploitation n'est pas installé sur le système d'extrémité, le profil de système d'exploitation avec la priorité la plus élevée est utilisé pour déterminer l'état et les actions de conformité, et aucun profil supplémentaire de cette stratégie n'est évalué.</p> <p>Par exemple, si Windows XP et Windows 2000 sont les systèmes d'exploitation requis et Windows XP le système d'exploitation favori, ajoutez les deux profils de système d'exploitation dans la stratégie, classez par ordre de priorité Windows XP en premier, et assurez-vous que la condition Else dans le profil Windows XP est défini sur non conforme (Non-Compliant) et qu'elle contient un message pour les utilisateurs non conformes. Dans ce cas, si, sur un système d'extrémité, aucun des systèmes d'exploitation requis n'est installé, le système d'extrémité est non conforme, un message apparaît et aucun profil supplémentaire dans la stratégie n'est évalué.</p>
Ajouter les profils d'application appropriés à une stratégie, puis les classer par ordre de priorité.	Par exemple, si vous avez plusieurs profils antivirus dans la stratégie, classez par ordre de priorité l'application antivirus la plus importante.

2.2.5 Vérification des modèles d'accès affectés à la stratégie

Bon usage	Description
Supprimer les modèles d'accès obsolètes et non utilisés de toutes les stratégies.	Gérez les stratégies qui contiennent les modèles d'accès pour les types d'application implémentés. Ce bon usage facilite la résolution des problèmes d'accès réseau quel que soit le mode de la stratégie.
Vérifier que les modèles d'accès appropriés sont affectés à la stratégie.	<p>Par défaut, chaque stratégie est automatiquement chargée avec les modèles d'accès. Assurez-vous que les modèles d'accès corrects sont appliqués à chaque état d'accès.</p> <p>Vous pouvez classer par ordre de priorité ou supprimer les modèles d'accès selon vos besoins. Si plusieurs modèles s'appliquent à un état particulier, le premier modèle correspondant à l'état est utilisé.</p>

Bon usage	Description
	<p>Important :</p> <ul style="list-style-type: none"> ■ Si vous appliquez un modèle d'accès Enforcer qui empêche l'accès au réseau en modes Report Only ou Remediate, tous les systèmes d'extrémité seront interdits d'accès quel que soit l'état en cours de leur conformité. Pour appliquer un état de conformité, vous devez impérativement changer le mode de stratégie sur Enforce. ■ Si vous supprimez tous les modèles d'accès Agent Enforcer d'un état d'accès particulier, vous autorisez tout le trafic sortant pour cet état.

2.3 Bon usage des profils

Cette section présente le bon usage pour les profils. Les conventions utilisées pour les profils sont les suivantes :

- **Profiles :** les profils vous permettent de définir les éléments que vous souhaitez voir évalués sur le système d'extrémité, comme les systèmes d'exploitation et les applications. Les profils définissent des conditions, des états de conformité, des messages et des actions correctives. Grâce aux profils, les stratégies sont simples à configurer et à mettre à jour. En effet, lorsqu'un changement est effectué dans un profil, ce changement est répercuté dans toutes les stratégies dans lesquelles le profil se trouve.
- **Profile Types :** les types de profils permettent de catégoriser les profils. Les profils sont placés dans des stratégies en fonction du type de profil.
- **Operating Systems :** les systèmes d'exploitation pris en charge pour l'élément que vous avez ajouté au profil.
- **Installed :** une fonctionnalité évaluée tout d'abord pour déterminer si l'application est installée. Si l'application est installée, tout message configuré apparaît et les fonctionnalités d'application restantes sont évaluées. Si l'application n'est **pas** installée, tout message configuré apparaît et les fonctionnalités d'application restantes ne sont **pas** évaluées. Les systèmes d'exploitation utilisent la fonctionnalité Installed, puis vérifient les service packs.
- **Message :** une liste indiquant si oui ou non un message apparaît pour l'utilisateur.
- **Message Icon :** un icône affichant la fenêtre Message pour que vous puissiez créer des messages.
- **Condition :** les déclarations utilisées lors de l'évaluation pour déterminer l'état de conformité du système d'extrémité et les actions à prendre sur ce dernier.
- **Compliance State :** chaque condition peut être associée à un état conforme, partiellement conforme ou non conforme.

Important : l'état de conformité du système d'extrémité est déterminé par les profils présents dans la stratégie. L'état le moins conforme détermine l'état de conformité global.

Si Sophos NAC détermine qu'un système d'extrémité est conforme avec le profil antivirus, mais non conforme avec le profil de pare-feu, l'état de conformité global est non conforme.

- **Agent Types** : types d'agent pour lesquels la fonctionnalité est prise en charge.
- **Operating Systems** : systèmes d'exploitation sur lesquels la fonctionnalité est prise en charge.
- **Condition Parameter** : le paramètre qui teste la version.

Remarque : la définition d'une version dans le profil permet de gérer aisément les versions d'une application.

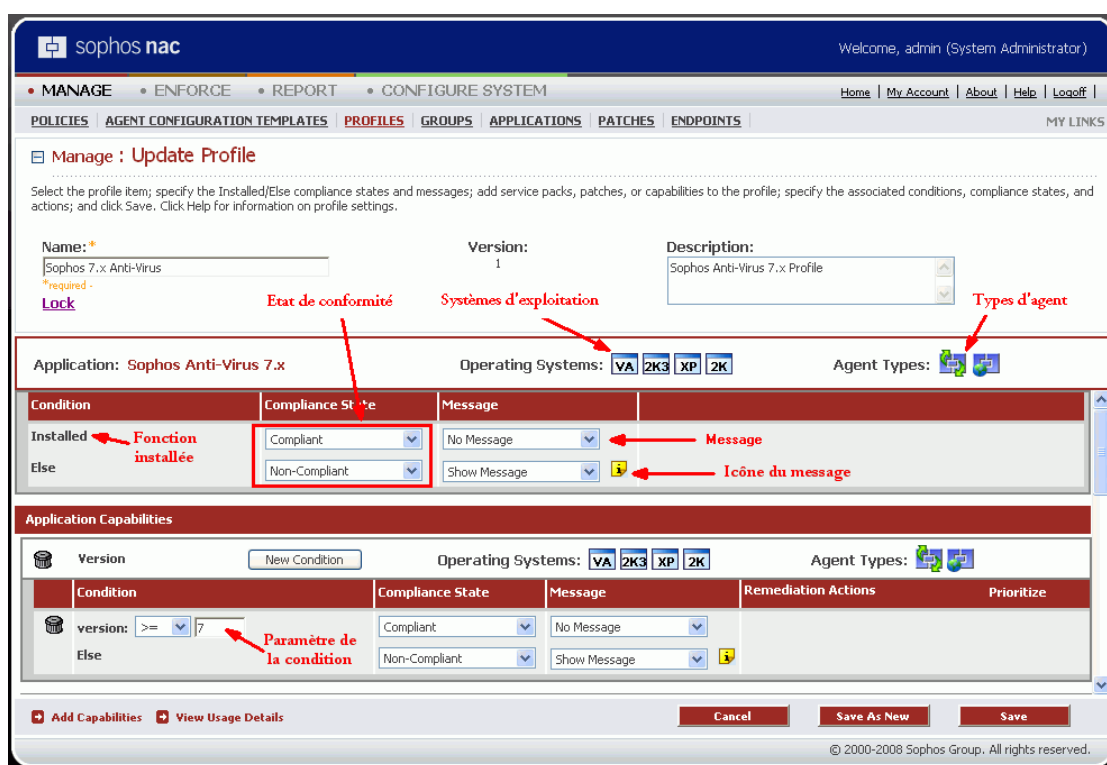


Schéma 2 : exemple de conventions des stratégies

2.3.1 Utilisation de profils prédéfinis pour créer des profils prêts pour la production

Bon usage	Description
Utiliser des profils prédéfinis comme guides.	Utilisez des profils prédéfinis : <ul style="list-style-type: none"> ■ Pour les démos, les pilotes ou les tests de démonstration, vous pouvez utiliser les profils prédéfinis tels qu'ils sont. ■ Pour le déploiement en production, vous pouvez copier (enregistrer comme nouveaux) les profils prédéfinis et personnaliser les messages, ajouter davantage de conditions,

Bon usage	Description
	<p>changer les actions, etc. ou simplement utiliser les profils comme un guide pour en créer des nouveaux.</p> <p>Dans le cas du profil Windows Update prédéfini, Sophos vous conseille d'utiliser ce profil pour les systèmes d'extrémité administrés afin de vous assurer que l'outil Windows Update est installé sur ceux-ci et que les mises à jour automatiques sont activées. Ce profil est automatiquement ajouté aux stratégies Default et Managed prédéfinies.</p>

2.3.2 Ajout de fonctionnalités aux profils

Les fonctionnalités sont les fonctions d'une application qui peuvent être testées pour leur conformité. Sophos NAC s'assure tout d'abord qu'un système d'exploitation ou qu'une application est installé à l'aide de la fonctionnalité Installed. Une fois que le logiciel vérifie qu'une application est installée, il évalue toutes les fonctionnalités supplémentaires sur le système d'extrémité.

Remarque : la disponibilité des fonctionnalités d'une application dépend de la conception du logiciel de cette application. Il se peut que certaines fonctionnalités ne soient pas disponibles pour certains systèmes d'exploitation prenant en charge l'application ou pour toutes les versions d'une application. Si une fonctionnalité n'est pas prise en charge, elle n'apparaît pas. Si une fonctionnalité est prise en charge sur certains systèmes d'exploitation mais pas sur d'autres, seuls les systèmes d'exploitation pris en charge apparaissent.

Bon usage	Description
Ajouter des fonctionnalités qui testent l'application pour s'assurer qu'elle protège le système d'extrémité de façon appropriée.	Ce n'est pas parce qu'une application est installée qu'elle protège activement le système d'extrémité. C'est pourquoi Sophos vous conseille d'ajouter des fonctionnalités comme Last Scan Grace Period ou Signature Grace Period qui testent l'application pour s'assurer qu'elle protège le système d'extrémité de façon appropriée.
Utiliser des fonctionnalités qui prennent en charge vos stratégies de sécurité de l'entreprise.	Par exemple, vous pouvez avoir une stratégie qui exige l'exécution d'un contrôle intégral du système par une application antivirus une fois par mois. Vous pouvez aussi avoir une stratégie de sécurité qui considère le contrôle en temps réel comme une protection adaptée. Dans le premier cas, vous pouvez inclure une fonctionnalité Scan dans le profil tandis que, dans le second, il est préférable de ne pas inclure de fonctionnalité Scan.
Utiliser des fonctionnalités Grace Period (Last Scan Grace Period et Signature Grace Period) plutôt que des fonctionnalités Date (Last Scan Date et Signature Date).	Grace period vous permet de paramétrer le profil et de l'oublier, ce qui signifie une maintenance minimale. Les fonctionnalités Grace Period et Date ne doivent pas être utilisées à moins que les conditions soient testées minutieusement. Le résultat peut être imprévisible.

Bon usage	Description
Utiliser toutes les fonctionnalités disponibles pour la plus sûre des évaluations de systèmes d'extrémité.	Utilisation si possible de toutes les fonctionnalités disponibles (à l'exclusion des fonctionnalités Grace Period et Date) pour la plus sûre des évaluations de systèmes d'extrémité. Elimination seule des fonctionnalités du profil si elles causent un problème dans votre déploiement NAC ou vos procédés d'entreprise.

2.3.3 Spécification des conditions et des états de conformité

Bon usage	Description
Affecter des états de conformité à des conditions en rapport avec l'accès réseau voulu.	<ul style="list-style-type: none"> ■ Utilisez Compliant pour autoriser l'accès réseau. ■ Utilisez Partially Compliant pour limiter l'accès réseau ou la quarantaine ; ou pour permettre l'accès réseau intégral mais en affichant des messages et en exécutant des actions correctives. ■ Utilisez Non-Compliant pour refuser ou limiter l'accès réseau, afficher des messages et exécuter des actions correctives. <p>L'état de conformité du système d'extrémité est déterminé par les profils présents dans la stratégie. L'état le moins conforme détermine l'état de conformité global. Si Sophos NAC détermine qu'un système d'extrémité est conforme avec le profil antivirus, mais non conforme avec le profil de pare-feu, l'état de conformité global est non conforme.</p>
Ajouter une nouvelle condition pour tester plus d'une valeur, pour définir un état de conformité différent ou pour spécifier un message ou une action corrective différent(e) basé(e) sur l'état de conformité.	Par exemple, pour Grace Period, vous pouvez déterminer quand le fichier signature d'un système d'extrémité est obsolète depuis 5 jours, mais seulement refuser l'accès réseau lorsque le fichier signature est obsolète depuis 10 jours. Pour ce cas, ajoutez une nouvelle condition selon laquelle, après 5 jours, le système d'extrémité est conforme, un avertissement apparaît pour l'utilisateur et l'accès réseau est autorisé. Ajoutez une autre condition selon laquelle, après 10 jours, le système d'extrémité est partiellement conforme, un avertissement apparaît pour l'utilisateur et l'accès réseau est autorisé. Si le fichier signature du système d'extrémité est obsolète depuis plus de 10 jours, un avertissement apparaît pour l'utilisateur et l'accès réseau est autorisé.

Bon usage	Description
<p>Classer les diverses conditions dans l'ordre dans lequel vous voulez qu'elles soient évaluées.</p>	<p>Une fois qu'une condition est remplie, l'état de conformité, le message et l'action corrective sont utilisés et aucune condition supplémentaire n'est évaluée pour cette fonctionnalité.</p> <p>Par exemple, en classant une condition partiellement conforme avant une condition non conforme, vous vous assurez qu'elle est évaluée en premier et que l'accès réseau est refusé seulement aux systèmes d'extrémité non conformes.</p>
<p>Veiller à ce que les états de conformité, messages et actions correctives correspondent à la condition sélectionnée.</p>	<p>Toutes les fonctionnalités affichent des conditions et des états de conformité dans un ordre par défaut. Si vous modifiez une condition, assurez-vous que les états de conformité correspondent à ce que vous aviez l'intention d'évaluer. En outre, si vous changez des conditions et des états de conformité, vous pouvez, si vous le voulez, afficher des messages différents à l'utilisateur ou exécuter sur le système d'extrémité des actions correctives différentes.</p> <p>Par exemple, l'ordre par défaut peut indiquer que si un pare-feu est activé (Enabled), le système d'extrémité est conforme (Compliant) ; Else (dans ce cas, signifiant que le pare-feu est non activé (Not Enabled)), le système d'extrémité est non conforme (Non-Compliant). Par conséquent, si vous changez la condition en non activé (Not Enabled), vous devez aussi changer les états de conformité associés pour déterminer que si un pare-feu est non activé (Not Enabled), le système d'extrémité est non conforme (Non-Compliant) ; Else (signifiant que le pare-feu est activé (Enabled)), le système d'extrémité est conforme (Compliant).</p>
<p>Utiliser des conditions et des états de conformité qui prennent en charge vos stratégies de sécurité.</p>	<p>Par exemple, vous pouvez avoir un stratégie de sécurité qui considère un système d'extrémité comme non conforme ou comme partiellement conforme si la protection en temps réel n'est pas activée. Dans le premier cas, assurez-vous que le système est considéré comme non conforme et que l'accès réseau lui est refusé. Dans le deuxième cas, exécutez une action corrective sur le poste partiellement conforme sans conséquences sur l'accès réseau.</p>
<p>Pour les fonctionnalités de version, s'assurer que le numéro de version contient le nombre correct de valeurs significatives.</p>	<p>Par exemple, si vous créez une condition qui spécifie == 8 et que la version du système d'extrémité est 8.1, le logiciel compare 8.1 à 8 dans la condition (une valeur significative), et la condition est remplie. En revanche, si vous créez une condition qui spécifie == 8.0 et que la version du système d'extrémité est 8.1, le logiciel compare 8.1 à 8 dans la condition (deux valeurs significatives), et la condition n'est pas remplie.</p>
<p>Pour les applications antivirus et antispywares, testez l'utilisation de</p>	<p>Si vous définissez un profil pour une application antivirus ou antispyware et si vous spécifiez une fonctionnalité de date (Last Scan Date et Signature Date) à l'aide de l'opérateur == (Egal</p>

Bon usage	Description
l'opérateur == dans les fonctionnalités de date.	à), veillez à ce que la date renvoyée du poste d'extrémité soit au format MM/JJ/AAAA. Si l'application renvoie une date au format MM/JJ/AAAA HH:MM:SS, la détection peut échouer même si la date sur le système d'extrémité est identique à la valeur spécifiée dans la condition. Pour éviter ce problème, vous pouvez utiliser l'opérateur >= (supérieur ou égal à) ou <= (inférieur ou égal à) au lieu de == lors de la définition des dates. Pour vous assurer que l'opérateur == ne fasse échouer la détection, testez une stratégie avant de la déployer.

2.3.4 Création de messages

Les messages apparaissent seulement lorsque des conditions sont remplies. En fonction de la stratégie, plusieurs messages peuvent s'afficher pour les utilisateurs. Testez les messages pour vérifier qu'ils sont exacts, contiennent des informations détaillées et qu'ils sont appropriés.

Important : considérez que peuvent se connecter au réseau des systèmes d'extrémité dont votre entreprise n'est pas propriétaire. Dans ce cas, les avertissements doivent être rédigés de manière adéquate car ces systèmes d'extrémité peuvent utiliser des applications non administrées différentes ou non prises en charge. La stratégie Unmanaged prédéfinie est utilisée spécifiquement pour les systèmes d'extrémité non administrés. Mettez à jour cette stratégie et ses profils et messages associés pour vous occuper de manière appropriée des systèmes d'extrémité non administrés.

Bon usage	Description
Créer des messages et les supprimer à l'aide du mode de stratégie Report Only.	Créez un profil pour lequel la messagerie est aussi proche que possible du prêt pour la production. Vous pouvez supprimer des messages en sélectionnant le mode de stratégie Report Only. Lorsque vous voulez afficher les messages et exécuter des actions correctives, mais pas appliquer la conformité, vous pouvez passer en mode Remediate. Lorsque vous voulez également appliquer la conformité, vous pouvez passer en mode Enforce. Pour plus d'informations, reportez-vous à la section Déploiement de Network Access Control à la page 4.
Utiliser des messages pour indiquer qu'une condition s'est produite.	Par exemple, créez un message qui indique que la signature antivirus n'est pas à jour et que Sophos NAC va mettre la signature à jour immédiatement.
Créer tous les messages en anglais, puis créer les messages correspondants dans toutes les autres langues.	L'agent sélectionne la langue la plus adaptée pour afficher les messages. Le message anglais s'affiche s'il ne peut s'afficher dans une autre langue. Si un message en anglais n'existe pas et si le message n'existe dans aucune autre langue, une boîte de dialogue de message vide apparaît à l'utilisateur. En outre, le NAC Manager affiche les message en anglais. Si aucun

Bon usage	Description
	message anglais n'existe, le champ du message n'affiche aucun message.

2.3.5 Utilisation des actions correctives

La disponibilité des actions correctives dépend de la conception du logiciel de cette application. Il se peut que certaines actions correctives ne soient pas disponibles pour certains systèmes d'exploitation prenant en charge l'application ou pour toutes les versions d'une application. Si une action corrective est prise en charge sur certains systèmes d'exploitation mais pas sur d'autres, les systèmes d'exploitation non pris en charge apparaissent avec un x.

Bon usage	Description
Sélectionner des actions correctives et les supprimer à l'aide du mode de stratégie Report Only.	Créez un profil pour lequel les actions correctives sont aussi proches que possible du prêt pour la production. Vous pouvez supprimer des actions correctives en sélectionnant le mode de stratégie Report Only. Lorsque vous voulez afficher les messages et exécuter des actions correctives, mais pas appliquer la conformité, vous pouvez passer en mode Remediate. Lorsque vous voulez également appliquer la conformité, vous pouvez passer en mode Enforce. Pour plus d'informations, reportez-vous à la section Déploiement de Network Access Control à la page 4.
Lors de l'exécution des actions correctives, créer une condition avec un état d'accès partiellement conforme.	Si vous créez seulement des conditions avec des états de conformité Compliant et Non-Compliant, le système d'extrémité doit être hors conformité pour que les actions correctives soient exécutées. Si vous créez une condition avec un état de conformité partiellement conforme, vous pouvez fournir des actions correctives pour vous assurer que les systèmes d'extrémité sont à jour et considérés comme non conformes seulement lorsqu'ils sont sérieusement obsolètes.
Utiliser toutes les actions correctives fournies lorsque cela est possible pour une évaluation des plus sûres des systèmes d'extrémité.	Éliminez seulement des actions correctives du profil si elles vont causer un problème dans votre déploiement.
Éviter les actions correctives si elles dérangent des tâches essentielles sur un système d'extrémité.	Pour éviter les actions correctives, vous pouvez créer des profils distincts sans certaines pour des utilisateurs spécifiques, temporairement désélectionner certaines dans des profils existants ou changer la stratégie de l'utilisateur en mode de stratégie Report Only. En fin de compte, vous devez évaluer à quelle point une action corrective dérange les utilisateurs et évaluer les risques de non-exécution de l'action corrective par rapport aux risques

Bon usage	Description
	qu'entraîne le fait d'empêcher une personne d'exécuter des tâches essentielles.

2.4 Bon usage des modèles d'accès

Cette section présente le bon usage pour les modèles d'accès. Les modèles d'accès déterminent comment l'accès réseau est accordé aux systèmes d'extrémité. Sophos NAC prend en charge l'application de l'agent et du protocole DHCP. Lorsque des modèles d'accès sont appliqués aux états d'accès conformes, partiellement conformes ou non conformes dans le NAC Manager, l'accès réseau est appliqué conjointement à l'évaluation de la stratégie. Pour de plus amples informations sur les modèles d'accès, reportez-vous à l'aide du NAC Manager.

Les conventions utilisées pour les modèles d'accès sont les suivantes :

- **Ressources réseau** : les ressources réseau sont des applications ou des périphériques nécessaires pour la correction ou ceux qui ne doivent pas être accessibles par des systèmes d'extrémité non conformes. Les ressources réseau peuvent être ajoutées soit aux modèles d'accès de l'Agent Enforcer soit à ceux du DHCP Enforcer.
- **Modèles d'accès Agent Enforcer** : les modèles d'accès Agent Enforcer identifient les ressources réseau auxquelles les systèmes d'extrémité peuvent ou ne peuvent pas accéder lors de l'utilisation de l'agent de quarantaine. Les ressources réseau déterminent les applications ou les périphériques auxquels le système d'extrémité peut accéder. les modèles d'accès Agent Enforcer s'appliquent seulement aux systèmes d'extrémité exécutant l'agent de quarantaine.
- **Modèles d'accès DHCP Enforcer** : les modèles d'accès DHCP Enforcer vous permettent de spécifier des paramètres d'accès nécessaires à la prise en charge de l'application du protocole DHCP.
- **Exemptions** : les exemptions identifient selon divers critères les systèmes d'extrémité dont la conformité n'a pas à être évaluée lors de la connexion au réseau. Les postes d'extrémités exemptés incluent soit ceux qui sont incapables d'exécuter l'agent, tels que les postes utilisant des systèmes d'exploitation autres que Windows soit ceux qui ne nécessitent pas d'évaluation de la conformité comme les serveurs, routeurs ou imprimantes. Les exemptions sont seulement utilisées avec l'application du protocole DHCP.

2.4.1 Création d'un modèle d'accès prêt pour la production

Bon usage	Description
Créer un modèle d'accès proche du prêt pour la production.	Utilisez la paramètre Policy Mode dans la stratégie pour augmenter peu à peu l'impact sur l'utilisateur. Vous pouvez activer l'application à travers une simple option, tout en apportant des changements minimales aux modèles d'accès. Pour plus d'informations,

Bon usage	Description
	reportez-vous à la section Définition du mode de stratégie approprié à la page 7.
Créer tous les modèles d'accès avant la mise à jour des stratégies.	Lorsque vous êtes prêt, vous pouvez mettre à jour les stratégies pour qu'elles contiennent les modèles d'accès que vous avez créés.

2.4.2 Utilisation de modèles d'accès prédéfinis comme guides

Bon usage	Description
Utiliser des modèles d'accès prédéfinis comme guides	<p>Utilisez les modèles d'accès prédéfinis :</p> <ul style="list-style-type: none"> ■ Pour les démos, les pilotes ou les tests de démonstration, vous pouvez utiliser les modèles d'accès prédéfinis tels qu'ils sont. ■ Pour le déploiement en production, vous pouvez copier (enregistrer en tant que nouveau) les modèles d'accès prédéfinis et personnaliser les paramètres.

2.4.3 Classement par ordre de priorité des ressources réseau, des modèles d'accès et des exemptions

Utilisez la priorité pour mettre en place un accès réseau approprié.

Bon usage	Description
Classer par ordre de priorité tout d'abord les ressources réseau, modèles d'accès et exemptions les plus	<ul style="list-style-type: none"> ■ Ressources réseau : si plusieurs ressources réseau s'appliquent à un système d'extrémité, la première qui correspond déterminera l'accès réseau. Les ressources réseau exécutables sont évaluées avant les ressources réseau de ports/protocoles.

Bon usage	Description
spécifiques/strictes, puis les moins spécifiques/strictes.	<ul style="list-style-type: none"> ■ Modèles d'accès : si plusieurs modèles d'accès s'appliquent à un état particulier, le premier modèle qui correspond à l'état est utilisé. Les modèles d'accès les plus spécifiques/stricts fournissent une adresse IP spécifique ou une plage d'adresses IP plus limitée tandis que les modèles d'accès moins spécifiques/stricts fournissent une plage d'adresses IP plus étendue. ■ Exemptions : si plusieurs exemptions s'appliquent à un système d'extrémité, la première correspondante détermine l'accès réseau. De plus, si plusieurs modèles d'accès s'appliquent à une exemption particulière, le premier modèle contenant l'adresse IP correspondante du serveur DHCP ou du relais DHCP est utilisé.

2.4.4 Spécification des états de conformité des modèles

Bon usage	Description
Ne pas sélectionner les états de conformité de modèles en conflit.	Par exemple, si vous sélectionnez Compliant, vous voulez créer un modèle qui autorise l'accès réseau. De même, si vous sélectionnez Non-Compliant, vous voulez créer un modèle qui limite l'accès réseau seulement aux serveurs de correction.

Enforce : Update Agent Enforcer Access Template

Select the template compliance states, select existing or create new network resources, specify access behavior for each network resource, and click Save. Click Help for information on access template settings.

Name: * Version: 1 Description:

Template Compliance States: (Used when creating policy)

- Compliant
- Partially Compliant
- Non-Compliant

Schéma 3 : exemple d'état de conformité modèle

2.4.5 Spécification de modèles d'accès pour l'état d'accès par défaut

Bon usage	Description
Spécifier des modèles d'accès pour l'état d'accès par défaut Ce bon usage s'applique seulement à l'application du protocole DHCP.	Si vous utilisez l'application du protocole DHCP, spécifiez les modèles d'accès appropriés pour l'état d'accès par défaut dans la page Configure System > Enforcer Settings du NAC Manager. L'état d'accès par défaut est essentiellement un dernier recours pour l'affectation des modèles d'accès. Sophos vous conseille donc de veiller à ce que toutes les adresses IP possibles soient incluses dans les modèles d'accès affectés à l'état d'accès par défaut. Classez par

Bon usage	Description
	ordre de priorité les modèles d'accès les plus spécifiques/stricts et identifiez le modèle d'accès à la plus basse priorité avec TOUS les paramètres - Deny All.

2.4.6 Création de ressources réseau

Bon usage	Description
Créer des ressources réseau exécutables exactes.	<p>Vous pouvez identifier les ressources réseau par exécutable ou port/protocole et aussi par adresse IP de destination et sous-réseau. Concernant les ressources réseau exécutables, l'agent de quarantaine évalue le trafic provenant du système d'extrémité pour déterminer quels processus autoriser ou refuser. Quant aux ports/protocoles et adresses IP, l'agent de quarantaine évalue vers quelles destinations autoriser ou refuser l'accès des systèmes d'extrémité.</p> <p>Les instructions de création d'exécutables d'accès réseau incluent :</p> <ul style="list-style-type: none"> ■ Le nom du processus exécutable doit être le nom qui apparaît dans l'onglet Processus du Gestionnaire des tâches Windows. ■ Les noms d'exécutables doivent posséder l'extension .exe à moins qu'un nom de processus ne contienne pas d'extension ; ne peuvent pas dépasser 64 caractères en longueur ; ne peuvent pas utiliser les caractères suivants : \ / : * ? " < > et ; ne peuvent pas contenir d'informations sur le chemin du fichier ; ne reconnaissent pas les caractères joker et seront seulement pris en charge pour les protocoles TCP et UDP. ■ Le logiciel détecte seulement les exécutables qui s'exécutent au niveau Winsock.

3 Configuration du NAC Manager

3.1 Aperçu du NAC Manager

Cette section contient des instructions et des informations sur l'utilisation du NAC Manager.

Restriction : l'utilisation des boutons du navigateur web pour naviguer dans le NAC Manager n'est **pas** prise en charge. La navigation et les fonctions doivent être exécutées à l'aide des options de menu, des liens et des boutons disponibles sur chaque page.

3.1.1 Nom et mot de passe du compte NAC Manager

Pour accéder au NAC Manager, utilisez un nom et un mot de passe de compte.

Utilisez le nom et le mot de passe de compte suivants pour accéder au NAC Manager pour la première fois :

- **Nom du compte** = admin.
- **Mot de passe** = un mot de passe de votre choix.

Lorsque vous accédez au NAC Manager pour la première fois, vous êtes invité à changer de mot de passe. Conservez une trace de ce mot de passe car c'est le seul moyen dont vous disposez pour accéder au NAC Manager tant que vous n'avez pas créé d'autres comptes utilisateurs. Pour plus d'informations, reportez-vous à la section [Création de comptes](#) à la page 81.















3.1.2 Visualisation de la page d'accueil

















Les commandes suivantes sont disponibles sur la page d'accueil.





- **Current Compliance** : graphique des états de conformité en cours de tous les agents de systèmes d'extrémité signalés ces sept derniers jours. Pour plus d'informations, reportez-vous à la section [Exécution de rapports de conformité](#) à la page 62.
- **Compliance Trend** : graphique des tendances de conformité ces sept derniers jours. Pour plus d'informations, reportez-vous à la section [Exécution de rapports de conformité](#) à la page 62.
- **Server Task Status** : état de chaque tâche de chargement par serveur. Si une tâche de chargement a échoué, cliquez sur le lien **Error** pour visualiser des informations détaillées sur l'erreur. Les tâches de chargement incluent :
 - **Current Definition Loader** : récupère les plus récentes dates de la signature à destination des applications antivirus et antispywares de Sophos.
 - **Report Warehouse Loader** : contrôle quand les données de rapports sont purgées.

3.1.3 Icônes du NAC Manager

Des icônes sont utilisées dans le NAC Manager pour représenter des actions possibles ou signifier quelque chose. Pour plus d'informations sur l'utilisation ou la signification de chaque icône, reportez-vous au tableau des icônes et des descriptions.

Icône	Description
Fonctions communes	
	Accroît la priorité d'un élément dans une liste.
	Décroît la priorité d'un élément dans une liste.
	Supprime un élément. Vous devez confirmer les suppressions des éléments dans une liste, tels que les profils. Il n'est pas nécessaire de confirmer les suppressions des paramètres d'un élément, comme les fonctionnalités.
	Indique un élément ou une tâche comme obligatoire, ce qui signifie qu'elle doit être terminée avant de passer à une autre tâche ou d'enregistrer les informations sur la page.
	Indique qu'un élément est déverrouillé. Le fait de cliquer sur l'icône verrouille l'élément. L'administrateur système et l'administrateur simple peuvent verrouiller les éléments.
	Indique qu'un élément est verrouillé. Le fait de cliquer sur l'icône déverrouille l'élément. L'administrateur système peut déverrouiller tous les éléments. L'administrateur peut uniquement déverrouiller les éléments qu'il a verrouillés.
	Indique qu'un élément est verrouillé et ne peut pas être déverrouillé par l'utilisateur du compte en cours, comme les ressources réseau personnalisées verrouillées par un autre utilisateur de compte.
	Indique une erreur devant être corrigée sur la page avant de passer à une autre tâche ou d'enregistrer des informations sur la page.
	Indique un message d'information pour confirmer qu'une action a été exécutée ou enregistrée avec succès.
	Indique un lien externe au NAC Manager.
	Représente un élément prédéfini qui ne peut pas être modifié comme une application standard ou une ressource réseau standard. Toutefois, vous pouvez enregistrer quelques éléments standard en tant que nouveaux éléments pour les modifier.
Etats de conformité des modèles	
	Indique qu'un modèle d'accès est censé être utilisé pour les systèmes d'extrémité à l'état conforme.
	Indique qu'un modèle d'accès est censé être utilisé pour les systèmes d'extrémité à l'état partiellement conforme.
	Indique qu'un modèle d'accès est censé être utilisé pour les systèmes d'extrémité à l'état non conforme.
Accounts	

Icône	Description
	Indique qu'un compte est activé. Le fait de cliquer sur l'icône désactive le compte.
	Indique qu'un compte est désactivé. Le fait de cliquer sur l'icône active le compte.
Profils et stratégies	
	Indique qu'un élément comme un profil, une application ou une fonctionnalité est pris en charge sur l'agent de quarantaine.
	Indique qu'un élément comme un profil, une application ou une fonctionnalité est pris en charge sur l'agent temporaire.
	Indique qu'un élément comme un profil, une application ou une fonctionnalité est pris en charge sur Windows Vista.
	Indique qu'un élément comme un profil, une application ou une fonctionnalité est pris en charge sur Windows XP.
	Indique qu'un élément comme un profil, une application ou une fonctionnalité est pris en charge sur Windows 2003.
	Indique qu'un élément comme un profil, une application ou une fonctionnalité est pris en charge sur Windows 2000.
	Indique que, malgré la prise en charge de la fonctionnalité sous Windows Vista, l'action corrective associée n'est pas prise en charge.
	Indique que, malgré la prise en charge de la fonctionnalité sous Windows XP, l'action corrective associée n'est pas prise en charge.
	Indique que, malgré la prise en charge de la fonctionnalité sous Windows 2003, l'action corrective associée n'est pas prise en charge.
	Indique que, malgré la prise en charge de la fonctionnalité sous Windows 2000, l'action corrective associée n'est pas prise en charge.
Profils d'applications	
	Indique qu'un message a été défini pour la condition. Le message apparaît sur le système d'extrémité seulement si la condition est remplie.
Exemptions	
	Représente une adresse MAC dans une exemption DHCP.
	Représente une classe d'édition dans une exemption DHCP.
	Représente une classe d'utilisateur dans une exemption DHCP.

Icône	Description
	Représente une étendue IP dans une exemption DHCP.
Rapports	
	Accède à l'enregistrement du rapport Agent Enforcer associé à une entrée sélectionnée du rapport Agent Session.
	Accède à l'enregistrement du rapport DHCP Enforcer associé à une entrée sélectionnée du rapport Agent Session.
	Accède aux informations concernant l'évaluation de la conformité associée à une entrée du rapport sélectionnée Compliance Detail, Agent Session ou Non-Compliance Detail.

3.1.4 Enregistrement d'un élément sous la forme d'un nouvel élément dans le NAC Manager

Vous pouvez enregistrer un élément sous la forme d'un nouvel élément afin de réutiliser les paramètres existants.

Nous vous conseillons d'enregistrer l'élément comme nouveau avant de mettre à jour ses paramètres. Les éléments pouvant être enregistrés sous la forme de nouveaux éléments incluent les modèles de configuration d'agents, les profils, les modèles d'accès, les ressources réseau et les exemptions.

Procédure

1. Cliquez sur le nom de zone approprié : **Manage**, **Enforce** ou **Configure System**.
2. Cliquez sur le nom de zone de l'élément que vous voulez réutiliser.
3. Cliquez sur le nom de l'élément dans la liste.
4. Cliquez sur **Save As New**. Dans la boîte de dialogue, saisissez un nouveau nom d'élément, puis cliquez sur **OK**.

Pour plus d'informations sur la création ou la mise à jour de paramètres d'élément, reportez-vous à la rubrique de création appropriée.

3.1.5 Visualisation ou recherche des éléments de liste dans le NAC Manager

Vous pouvez visualiser les éléments de liste ou rechercher des éléments spécifiques dans le NAC Manager.

Depuis chaque zone du NAC Manager, vous pouvez visualiser une liste des éléments créés ou ajoutés, accéder à des informations sur un élément, mettre à jour ou supprimer un élément. En outre, vous pouvez restreindre des listes d'éléments potentiellement extensibles à l'aide des options de recherche disponibles dans des zones spécifiques.

Procédure

1. Cliquez sur le nom de zone approprié : **Manage**, **Enforce** ou **Configure System**.

2. Cliquez sur le nom de zone des éléments que vous voulez réutiliser.

Remarque : pour que tous les noms d'applications de la page de liste **Applications** s'affichent correctement, vous devez installer les fichiers de prise en charge des langues d'Asie Orientale (via le **Panneau de configuration > Options régionales et linguistiques**) sur la machine depuis laquelle vous visualisez le NAC Manager.

3. Si vous êtes dans **Manage > Profiles or Applications** , cherchez de manière facultative des éléments spécifiques dans la liste à l'aide des critères de recherche. Saisissez ou sélectionnez les options de recherche appropriées et cliquez sur **Rechercher**.

Remarque : les valeurs de recherche des éléments de liste n'ont **pas** à correspondre exactement et ne sont **pas** sensibles aux majuscules. En outre, 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 Name, tous les noms qui commencent par un M s'affichent. De même, si vous tapez M sans le symbole % dans le champ Name, seuls ceux qui s'appellent M s'affichent.

4. Effectuez l'une des opérations suivantes :

- Pour trier la liste, cliquez sur l'en-tête de colonne approprié.
- Pour visualiser les informations relatives à un élément ou mettre ce dernier à jour, cliquez sur son nom.
- Pour supprimer un élément, sélectionnez la case à cocher située près de tous ceux que vous voulez supprimer, puis cliquez sur **Delete**. Dans le message, confirmez la liste des éléments à supprimer et cliquez sur **OK**.

3.1.6 Suppression d'éléments dans le NAC Manager

La suppression d'éléments dans le NAC Manager les supprime complètement du logiciel. Seuls les éléments qui ne sont pas en cours d'utilisation par un autre élément peuvent être supprimés. Par exemple, vous ne pouvez pas supprimer une ressource réseau appartenant à un modèle d'accès Agent Enforcer. Vous pouvez aussi utiliser l'icône de la poubelle pour supprimer des éléments sur une page.

Procédure

1. Cliquez sur le nom de zone approprié : **Manage**, **Enforce** ou **Configure System**.
2. Cliquez sur le nom de zone de l'élément que vous voulez supprimer.
3. Sélectionnez la case à cocher située près de chaque élément que vous voulez supprimer.
4. Cliquez sur **Delete**.
5. Dans le message, cliquez sur **OK** pour confirmer la suppression.

3.1.7 Verrouillage ou déverrouillage d'éléments dans le NAC Manager

Le verrouillage d'un élément dans le logiciel empêche d'autres administrateurs de le mettre à jour.

L'administrateur système peut déverrouiller tous les éléments. L'administrateur simple peut déverrouiller seulement les éléments qu'il a verrouillés.

Procédure

1. Cliquez sur le nom de zone approprié : **Manage**, **Enforce** ou **Configure System**.
2. Cliquez sur le nom de zone des éléments que vous voulez verrouiller ou déverrouiller.
3. Cliquez sur l'icône **Lock** ou **Unlock** située près de l'élément que vous voulez verrouiller ou déverrouiller.

L'icône de l'état en cours s'affiche.

Remarque : certains éléments comme les applications standard et les ressources réseau standard ne peuvent pas être verrouillés ou déverrouillés.

3.1.8 Utilisation des fonctions par clic droit dans le NAC Manager

Des fonctions de clic avec le bouton droit de la souris sont disponibles sur toutes les pages de liste et dans d'autres zones où les fonctions sont disponibles.

Procédure

1. Cliquez sur le nom de zone approprié : **Manage**, **Enforce** ou **Configure System**.
2. Cliquez sur le nom de zone de l'élément que vous voulez gérer.
3. Cliquez avec le bouton droit de la souris sur le nom du lien et sélectionnez la fonction appropriée. Pour plus d'informations sur les zones et les fonctions, consultez le tableau des fonctions par clic droit.

Fonctions par clic droit

Zone NAC Manager	Description
Standard pour toutes les zones	Toutes les pages de liste incluent les fonctions standard suivantes : Edit, View (disponible pour les éléments standard qui ne peuvent pas être modifiés), Copy, Rename, Delete, Lock/Unlock et View Audit Data. Remarque : il est possible que certaines fonctions ne soient pas disponibles pour tous les éléments d'une liste.
Modèles de configuration d'agent, Profils, Applications, Modèles d'accès Agent Enforcer, Modèles d'accès DHCP Enforcer et pages de liste des ressources réseau	Des pages de liste spécifiques ont toutes des fonctions standard, plus View Usage Details qui affiche des informations sur les stratégies, les profils ou les modèles d'accès dans lesquels l'élément sélectionné est utilisé.
Page des listes Accounts	La page des listes Accounts dispose de toutes les fonctions standard sauf la copie et le verrouillage/déverrouillage, plus l'activation/désactivation.

3.2 Aperçu de la zone Manage

La zone Manage contient tous les composants requis pour gérer les stratégies. Vous pouvez accéder aux zones suivantes depuis le menu Manage :

Zone et action	Description
Applications	
Utiliser les types d'application standard.	Les types d'application classifient les applications et établissent des comportements de stratégie par défaut pour toutes les applications associées au type d'application. Les types d'application standard sont déjà disponibles dans le logiciel.
Utiliser des applications standard.	Les applications sont des applications logicielles prises en charge par Sophos NAC. Les applications standard sont déjà disponibles dans le logiciel. Les applications sont liées à un type d'application, qui détermine comment l'application est évaluée lorsque le profil de l'application est ajouté à la stratégie.
Agent configuration templates	
Créer des modèles de configuration d'agent.	Les modèles de configuration d'agent définissent les paramètres facultatifs qui commandent la façon dont l'agent fonctionne sur les systèmes d'extrémité.
Profils	
Créer des profils pour les systèmes d'exploitation et/ou les applications, ou utiliser des profils exemples prédéfinis.	<p>Les profils vous permettent de définir les éléments que vous souhaitez voir évalués sur le système d'extrémité, comme les systèmes d'exploitation et les applications. Une fois créés, les profils peuvent être organisés et classés par ordre de priorité dans les stratégies. Pour plus d'informations sur les composants de profils, reportez-vous à la section Glossaire à la page 95.</p> <p>Astuces :</p> <ul style="list-style-type: none"> ■ Utilisez des profils prédéfinis comme guides. Vous pouvez enregistrer des profils prédéfinis en tant que nouveaux profils, puis personnaliser les messages, ajouter des conditions supplémentaires, changer les états de conformité, activer des actions correctives, etc. ou simplement utiliser les profils comme guides pour créer de nouveaux profils. ■ Utilisez des profils Windows Update prédéfinis pour fournir une évaluation des mises à jour du système d'exploitation Windows. Pour plus d'informations, reportez-vous à la section Utilisation des profils prédéfinis Windows Update à la page 36.
Policies	
Mettre à jour les stratégies.	<p>Les stratégies contrôlent l'accès aux ressources réseau de l'entreprise d'après les évaluations des profils sur le système d'extrémité. Les stratégies gèrent la configuration qui détermine l'état de conformité du système d'extrémité, les messages qui apparaissent, les actions correctives qui sont exécutées et les actions d'application qui sont prises. Pour plus d'informations sur les composants de stratégies, reportez-vous à la section Glossaire à la page 95.</p> <p>Astuces :</p> <ul style="list-style-type: none"> ■ Un nombre illimité de profils peut être ajouté à une stratégie. ■ Au minimum, au moins un profil de système d'exploitation doit être inclus dans une stratégie.

Zone et action	Description
	<ul style="list-style-type: none"> ■ Les stratégies doivent contenir les profils correspondants de chaque système d'exploitation que vous voulez évaluer sur les systèmes d'extrémité. ■ Utilisez les stratégies prédéfinies pour appliquer la conformité de la sécurité pour les systèmes d'extrémité à la fois administrés et non administrés. Pour plus d'informations, reportez-vous à la section Utilisation des stratégies prédéfinies à la page 28.

3.2.1 Utilisation des stratégies prédéfinies

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

Lors de l'évaluation de la conformité des systèmes d'extrémité, l'agent récupère la stratégie associée au groupe du système d'extrémité dans la Sophos Enterprise Console. Pour plus d'informations, reportez-vous à la section [Mise à jour des stratégies](#) à la page 28.

- **Default :** cette stratégie est utilisée si le Sophos Compliance Agent est installé sur un système d'extrémité et si 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.
- **Managed :** cette stratégie peut être utilisée pour les systèmes d'extrémité qui sont administrés avec la Sophos Enterprise Console et sur lesquels Sophos 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.
- **Unmanaged :** 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 Unmanaged.

Remarque : si l'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. Pour plus d'informations, reportez-vous à la section [Spécification des paramètres Enforcer](#) à la page 82.

3.2.2 Mise à jour des stratégies

Les stratégies contrôlent l'accès aux ressources réseau de l'entreprise d'après les évaluations des profils sur le système d'extrémité. Les stratégies gèrent la configuration qui détermine l'état de conformité du système d'extrémité, les messages qui apparaissent, les actions correctives qui sont exécutées et les actions d'application qui sont prises.

Important : toutes les stratégies et changements de stratégies sont effectifs immédiatement sur le réseau, mais aucune stratégie n'est appliquée sur le système d'extrémité tant que l'agent ne la récupère pas.

Procédure

1. 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 28.
2. Cliquez sur la liste **Policy Mode** pour sélectionner le mode de stratégie.
Les modes de stratégie déterminent quels modèles d'accès sont utilisés lors d'une évaluation de conformité. Les modes de stratégie sont Report Only, Remediate et Enforce. Pour plus d'informations, reportez-vous à la section [Glossaire](#) à la page 95.
3. Dans la zone de navigation gauche Agent, cliquez sur **Settings**.
4. Le cas échéant, spécifiez les paramètres de l'agent permanent. Ces paramètres s'appliquent seulement aux systèmes d'extrémité exécutant l'agent de quarantaine :
 - **Policy Refresh Interval** : identifie la fréquence avec laquelle l'agent récupère la stratégie. La valeur par défaut est 4 heures.
 - **Assess and Enforce Interval** : identifie la fréquence avec laquelle l'agent vérifie si le système d'extrémité est en conformité. La valeur par défaut est 4 heures.
 - **Report Interval** : identifie la fréquence avec laquelle l'agent envoie des données de rapport au serveur. La valeur par défaut est 8 heures.
5. Le cas échéant, sélectionnez le modèle de configuration d'agent dans la section Configuration Settings.
Si aucun modèle de configuration n'est sélectionné, l'agent utilisera les paramètres par défaut. Ces paramètres s'appliquent seulement aux systèmes d'extrémité exécutant l'agent de quarantaine. Pour plus d'informations, reportez-vous aux sections [Création de modèles de configuration d'agent](#) à la page 32 et [Visualisation des paramètres d'agent](#) à la page 33.
6. Le cas échéant, spécifiez les paramètres de l'agent de quarantaine. Ces paramètres s'appliquent seulement aux systèmes d'extrémité exécutant l'agent de quarantaine :
 - **Quarantine Override** : identifie si l'utilisateur peut remplacer la quarantaine sur le système d'extrémité. Si le remplacement de la quarantaine est paramétré sur True, l'utilisateur a le droit de remplacer la quarantaine de l'agent. Cette option permet à l'utilisateur de supprimer le système d'extrémité de la quarantaine même s'il n'est pas conforme. Si le remplacement est paramétré sur False, l'utilisateur ne peut pas remplacer la quarantaine de l'agent et le système d'extrémité reste en quarantaine jusqu'à ce qu'il soit en conformité avec la stratégie.

7. Le cas échéant, spécifiez les paramètres de l'agent DHCP. Ces paramètres s'appliquent seulement si vous mettez en place l'application du protocole DHCP :
 - **Agent Enforcement Action** : établit la méthode utilisée pour obtenir de nouvelles adresses IP pour le système d'extrémité. L'agent obtient de nouvelles adresses IP lorsqu'il démarre et initialise une évaluation de conformité, lorsque l'état de conformité du système d'extrémité change et lorsque les modèles d'accès DHCP Enforcer définis dans la stratégie du système d'extrémité changent. Les valeurs disponibles incluent :
 - **None** : les adresses IP du système d'extrémité ne sont ni publiées ni renouvelées. Sélectionnez **None** lorsque vous n'utilisez pas l'application du protocole DHCP.
 - **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. Vous **devez** sélectionner Release Renew lors de l'utilisation de l'application du protocole DHCP.

8. Procédez de l'une des manières suivantes :
 - Pour ajouter des profils dans la stratégie, cliquez sur **Add Profiles** dans la section inférieure gauche de la page, cliquez sur la liste **Profile Type** pour sélectionner le type de profil, sélectionnez les cases à cocher situées près des profils que vous voulez ajouter à la stratégie, et cliquez sur **OK**. Répétez cette opération autant que nécessaire pour ajouter des profils supplémentaires à la stratégie.

Important : Un nombre illimité de profils peut être ajouté à une stratégie. Au minimum, au moins un profil de système d'exploitation doit être inclus dans une stratégie. Les stratégies doivent contenir les profils correspondants de chaque système d'exploitation que vous voulez évaluer sur les systèmes d'extrémité.
 - Pour supprimer les profils de la stratégie, cliquez sur le type de profil approprié dans la zone de navigation gauche Profiles, puis cliquez sur l'icône de la **corbeille** située près des profils d'applications pour les supprimer de la stratégie.

9. Si vous avez plus d'un profil de système d'exploitation, vous pouvez classer par ordre de priorité les systèmes d'exploitation pour l'évaluation.

Les comportements de stratégie sont Required, Best et All. Pour plus d'informations, reportez-vous à la section [Glossaire](#) à la page 95.

10. Si vous avez sélectionné tous les profils d'applications, vous pouvez spécifier les systèmes d'exploitation sur lesquels l'application sera évaluée. Aussi, si vous avez plus d'un profil d'application, vous pouvez utiliser les flèches pour classer par ordre de priorité les applications pour évaluation.

Remarque : les cases grisées indiquent que l'évaluation d'une application sur un système d'exploitation particulier n'est pas prise en charge.

11. Dans la zone de navigation gauche Network Access, cliquez sur le type d'application pour lequel vous voulez vérifier ou changer les modèles d'accès. Pour ajouter des modèles d'accès pour un état d'accès particulier, cliquez sur l'onglet du mode de stratégie approprié, cliquez sur **Select**, sélectionnez les modèles d'accès et les états d'accès auxquels s'appliquent les modèles et cliquez sur **OK**. Vous pouvez aussi laisser les modèles d'accès en cours ou les supprimer.

En fonction de la configuration de votre réseau, il se peut que vous deviez spécifier plus d'un type d'application. Pour plus d'informations sur les types d'application, reportez-vous à la section [Visualisation des modes de stratégie et des états d'accès](#) à la page 31.

Remarque : par défaut, chaque stratégie est automatiquement chargée de modèles d'accès pour chacun des états d'accès, d'après les modèles d'accès prédéfinis dans le NAC Manager et leurs états de conformité associés. Assurez-vous que les modèles d'accès corrects sont appliqués à chaque état d'accès. Vous pouvez aussi soit mettre à jour les paramètres des modèles d'accès prédéfinis soit en créer de nouveaux et les ajouter aux stratégies à la place des modèles d'accès prédéfinis. Notez que si vous supprimez tous les modèles d'accès Agent Enforcer d'un état d'accès particulier, vous autorisez tout le trafic sortant pour cet état. Pour plus d'informations, reportez-vous aux sections [Création de modèles d'accès Agent Enforcer](#) à la page 50 et [Création de modèles d'accès DHCP Enforcer](#) à la page 51.

12. 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.

13. Cliquez sur **Save**.

3.2.3 Visualisation des modes de stratégie et des états d'accès

Le tableau suivant décrit les états d'accès disponibles pour chaque mode de stratégie par type d'application.

Pour plus d'informations, reportez-vous à la section [Mise à jour des stratégies](#) à la page 28.

Mode de stratégie	Description et états d'accès
Report Only	<p>Les systèmes d'extrémité sont évalués par rapport à la stratégie affectée et les informations de rapport sont générées dans le NAC Manager. Aucun message n'apparaît, aucune action corrective n'est effectuée et aucune action d'application n'est prise. Sélectionnez un modèle d'accès Enforcer qui permet l'accès au trafic provenant du système d'extrémité.</p> <p>Important : si vous appliquez un modèle d'accès Enforcer qui empêche l'accès au réseau en modes Report Only ou Remediate, tous les systèmes d'extrémité seront interdits d'accès quel que soit l'état en cours de leur conformité. Pour appliquer un état de conformité, vous devez impérativement changer le mode de stratégie sur Enforce.</p>
Remediate	<p>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</p>

Mode de stratégie	Description et états d'accès
	<p>apparaissent, les actions correctives sont effectuées ; en revanche, aucune action d'application n'est prise. Sélectionnez un modèle d'accès Enforcer qui permet l'accès au trafic provenant du système d'extrémité.</p> <p>Important : si vous appliquez un modèle d'accès Enforcer qui empêche l'accès au réseau en modes Report Only ou Remediate, tous les systèmes d'extrémité seront interdits d'accès quel que soit l'état en cours de leur conformité. Pour appliquer un état de conformité, vous devez impérativement changer le mode de stratégie sur Enforce.</p>
Enforce	<p>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. Lorsque le système d'extrémité est dans l'un des états suivants dans la stratégie affectée, les modèles d'accès associés dans cet état déterminent l'accès réseau.</p> <p>Etats d'agent :</p> <ul style="list-style-type: none"> ■ No Agent Tray : l'agent n'est pas exécuté sur le système d'extrémité. Ce statut peut être signalé par l'Agent Enforcer si l'utilisateur n'a pas de session ouverte sur Windows ou si l'application Agent de la zone de notification ne fonctionne plus. ■ User Override : l'utilisateur a remplacé la quarantaine de l'agent sur le système d'extrémité. ■ Policy Retrieval Error : une stratégie n'a pas pu être récupérée pour le système d'extrémité. Ce statut peut exister si l'agent est incapable de récupérer la stratégie depuis le NAC Server ; ou si l'état de conformité du système d'extrémité est obsolète d'après le champ Agent Policy Update Threshold configuré dans la zone Configure System > Enforcer Settings. <p>Enforcer State :</p> <ul style="list-style-type: none"> ■ 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. <p>Etats de conformité :</p> <ul style="list-style-type: none"> ■ Compliant : l'évaluation a déterminé que le système d'extrémité est conforme à la stratégie. ■ Partially Compliant : l'évaluation a déterminé que le système d'extrémité est partiellement conforme à la stratégie. ■ Non-Compliant : l'évaluation a déterminé que le système d'extrémité n'est pas conforme à la stratégie.

3.2.4 Création de modèles de configuration d'agent

Les modèles de configuration d'agent permettent à l'administrateur de définir les paramètres facultatifs qui commandent la façon dont l'agent fonctionne sur les systèmes d'extrémité. Les

modèles de configuration d'agent s'appliquent seulement aux systèmes d'extrémité exécutant l'agent de quarantaine.

Une fois que vous avez créé des modèles de configuration d'agent, vous pouvez les ajouter aux stratégies. Les agents peuvent ensuite récupérer la stratégie affectée lors de l'évaluation suivante et mettre en place les paramètres sur le système d'extrémité à cet instant. Pour plus d'informations, reportez-vous à la section [Mise à jour des stratégies](#) à la page 28.

Procédure

1. Cliquez sur **Manage > Agent Configuration Templates** . Puis cliquez sur **Create Agent Configuration Template** dans la section inférieure gauche de la page.
2. Saisissez un nom et une description de modèle de configuration d'agent.
3. Pour spécifier les paramètres d'agent, cliquez sur **Select**, sélectionnez les cases à cocher situées près des paramètres d'agent que vous voulez ajouter au modèle de configuration d'agent, cliquez sur **OK** et spécifiez les valeurs comme vous le souhaitez.

Les paramètres d'agent définissent les fonctionnalités de l'agent lorsque ce dernier fonctionne sur le système d'extrémité. Pour plus d'informations sur les paramètres d'agent spécifiques et les valeurs disponibles, reportez-vous à la section [Visualisation des paramètres d'agent](#) à la page 33.

4. Cliquez sur **Save**.

Remarque : une fois que le modèle de configuration d'agent est créé, vous pouvez visualiser les stratégies qui utilisent ce modèle depuis l'option de menu par clic droit dans la page de liste **Agent Configuration Templates** ou lors de la modification du modèle en cliquant sur le lien **View Usage Details**.

3.2.5 Visualisation des paramètres d'agent

Le tableau suivant décrit les paramètres d'agent disponibles.

Pour plus d'informations sur la création de modèles de configuration d'agent, reportez-vous à la section [Création de modèles de configuration d'agent](#) à la page 32.

Paramètre d'agent	Description et valeurs disponibles	Valeur par défaut
Log Lifetime	<p>Durée, en heures, de conservation des journaux Agent sur le système d'extrémité avant qu'ils ne soient effacés et redémarrés. Lorsqu'une session d'agent commence, tous les fichiers journaux dont la date est postérieure à la valeur de temps permise sont supprimés.</p> <p>Remarque : la journalisation affecte les performances ; c'est pourquoi il est conseillé d'activer la journalisation pour la résolution des problèmes seulement et de la désactiver lorsque la résolution des problèmes est terminée. Les fichiers journaux sont placés dans le dossier suivant du système d'extrémité : <i><lecteur></i>:\Documents and Settings\All Users\Application Data\Sophos\Sophos NAC\Logs ou, pour Vista, dans <i><lecteur></i>:\ProgramData\Sophos\Sophos NAC\Logs.</p>	24

Paramètre d'agent	Description et valeurs disponibles	Valeur par défaut
Logging	<p>Définit le niveau de journalisation pour l'agent. Les valeurs disponibles sont :</p> <ul style="list-style-type: none"> ■ Log Error and Warning : inclut les messages d'erreur et d'avertissement. ■ Log All Messages : inclut les messages d'erreur, d'avertissement et d'information. ■ Log All Messages and Brief Trace : inclut les messages d'erreur, d'avertissement, d'information et de suivi. <p>Remarque : la journalisation affecte les performances ; c'est pourquoi il est conseillé d'activer la journalisation pour la résolution des problèmes seulement et de la désactiver lorsque la résolution des problèmes est terminée. Les fichiers journaux sont placés dans le dossier suivant du système d'extrémité : <lecteur>:\Documents and Settings\All Users\Application Data\Sophos\Sophos NAC\Logs ou, pour Vista, dans <lecteur>:\ProgramData\Sophos\Sophos NAC\Logs.</p>	Log Error and Warning
Max Attempts	Nombre maximal de fois que l'agent tentera de communiquer avec le NAC Server pour une opération donnée (c'est-à-dire la récupération d'une stratégie, l'évaluation/l'application/la correction d'une stratégie et le rapport). L'agent réessaye de communiquer lors de son premier démarrage et au cours des intervalles d'évaluation continue ; il ne réessaye pas de communiquer lors d'une vérification de conformité lancée par l'utilisateur.	10
Retry Delay	Spécifie le temps d'attente (en secondes) de l'agent avant qu'il ne lance une autre tentative de communication avec le NAC Server. L'agent réessaye de communiquer lors de son premier démarrage et au cours des intervalles d'évaluation continue ; il ne réessaye pas de communiquer lors d'une vérification de conformité lancée par l'utilisateur.	15
Save Proxy Password	Enregistre le mot de passe du proxy utilisé pour les requêtes d'authentification de proxy subséquentes. Les valeurs disponibles sont Save et Do Not Save .	Do Not Save
Save Proxy Username	Enregistre le nom utilisateur du proxy utilisé pour les requêtes d'authentification de proxy subséquentes. Les valeurs disponibles sont Save et Do Not Save .	Do Not Save
Show Errors In Results	<p>Affiche/masque les messages d'erreur dans la boîte de dialogue Résultats. Les valeurs disponibles sont Show et Hide.</p> <p>Si la valeur est Show, les messages d'erreur apparaissent dans la boîte de dialogue Résultats et sont enregistrés dans le fichier errors.htm qui se trouve dans le dossier sur le système d'extrémité : <lecteur>:\Documents and Settings\All Users\Application Data\Sophos\Sophos NAC\Data ou, pour Vista, dans <lecteur>:\ProgramData\Sophos\Sophos NAC\Data. Si la valeur est Hide, les messages d'erreur sont uniquement enregistrés dans le fichier errors.htm.</p>	Show

Paramètre d'agent	Description et valeurs disponibles	Valeur par défaut
Show Exit	Affiche/masque l'option de menu Quitter. Les valeurs disponibles sont Show et Hide .	Hide
Show Extended Errors	Affiche/masque les messages d'erreur étendus de la boîte de dialogue Résultats associés aux échecs de communication du NAC Server. Les valeurs disponibles sont Show et Hide . Si la valeur est Show, des messages d'erreur étendus apparaissent dans la boîte de dialogue Résultats et sont enregistrés dans le fichier errors.htm qui se trouve dans le dossier sur le système d'extrémité : <lecteur>:\Documents and Settings\All Users\Application Data\Sophos\Sophos NAC\Data ou, pour Vista, dans <lecteur>:\ProgramData\Sophos\Sophos NAC\Data.	Show
Show Logging	Détermine si la case à cocher Activer la journalisation apparaît dans la boîte de dialogue A propos de. Les valeurs disponibles sont Show et Hide .	Show

3.2.6 Création de profils

Les profils vous permettent de définir les éléments que vous souhaitez voir évalués sur le système d'extrémité, comme les systèmes d'exploitation et les applications. Les profils définissent des conditions, des états de conformité, des messages et des actions correctives. Une fois créés, les profils peuvent être organisés et classés par ordre de priorité dans les stratégies.

Vous pouvez créer un profil pour un élément spécifique, puis désigner les service packs ou les fonctionnalités d'applications pour cet élément (en fonction de son type). Vous pouvez aussi créer plusieurs profils pour le même système d'exploitation ou la même application si vous voulez définir des états de conformité, des messages ou des actions correctives différentes pour l'élément.

3.2.7 Instructions générales sur les profils

Les instructions pour les profils incluent les éléments suivants :

- Un nombre illimité de profils peut être ajouté à une stratégie.
- Au minimum, au moins un profil de système d'exploitation doit être inclus dans une stratégie.
- Les stratégies doivent contenir les profils correspondants de chaque système d'exploitation que vous voulez évaluer sur les systèmes d'extrémité.
- Seul un système d'exploitation ou une application peut appartenir à un profil.
- Un système d'exploitation, un correctif ou une application peut appartenir à plusieurs profils.

3.2.8 Utilisation des profils prédéfinis Windows Update

Vous pouvez utiliser les profils prédéfinis pour fournir une évaluation des mises à jour du système d'exploitation Windows.

- **Profil Windows Update :** ce profil est utilisé pour s'assurer que l'outil Windows Update est installé et que les Mises à jour automatiques sont activées sur les systèmes d'extrémité administrés. Si les Mises à jour automatiques ne sont pas activées sur un système d'extrémité, l'action corrective Windows Update active ces Mises à jour automatiques sur le système d'extrémité. Ce profil est automatiquement ajouté aux stratégies Default et Managed. Ce profil est prévu pour être utilisé avec l'agent de quarantaine et les utilisateurs connus.
- **Profil Windows Update pour les systèmes d'extrémité non administrés :** ce profil est utilisé pour s'assurer que l'outil Windows Update est installé et que les Mises à jour automatiques sont activées sur les systèmes d'extrémité non administrés. Si les Mises à jour automatiques ne sont pas activées sur un système d'extrémité, un message apparaît indiquant que les Mises à jour automatiques Windows doivent être activées pour être conformes. Ce profil est automatiquement ajouté dans la stratégie Unmanaged. Ce profil est prévu pour une utilisation avec l'agent temporaire et les utilisateurs invités.

3.2.9 Création de profils de systèmes d'exploitation

La page Profiles vous permet de créer des profils de systèmes d'exploitation à utiliser dans les stratégies. Les profils de systèmes d'exploitation servent à organiser et à classer par ordre de priorité les systèmes d'exploitation et service packs associés que vous voulez évaluer sur le système d'extrémité. Dans les profils, vous pouvez définir les conditions qui déterminent l'état de conformité des systèmes d'extrémité ainsi que les messages à afficher sur le système d'extrémité.

Procédure

1. Cliquez sur **Manage > Profiles**. Puis cliquez sur **Create Profile** dans la section inférieure gauche de la page.
2. Saisissez un nom et une description de profil.
3. Cliquez sur **Select Profile Item**.
4. Dans la liste **Profile Type**, sélectionnez **Operating System**, puis sélectionnez le système d'exploitation pour lequel vous voulez créer ce profil, et cliquez sur **OK**.

Important : les profils de systèmes d'exploitation sont requis dans les stratégies. Si l'un des systèmes d'exploitation n'est pas installé sur le système d'extrémité, alors l'état de conformité de la condition Else du profil du système d'exploitation à la priorité la plus élevée est utilisé pour déterminer l'état de conformité et les actions du type de profil du système d'exploitation, et aucun profil supplémentaire n'est évalué pour cette stratégie.

5. Le cas échéant, cliquez sur la liste de la colonne **Compliance State** pour changer les états de conformité des conditions de systèmes d'exploitation suivantes. Pour plus d'informations, reportez-vous à la section [Détermination de l'état de conformité du système d'extrémité](#) à la page 49.

- **Installed** : si ce système d'exploitation est installé, cet état de conformité est appliqué à l'évaluation de stratégie du système d'extrémité et tout message configuré apparaît.
- **Else** : si aucun système d'exploitation est installé, l'état de conformité associé du profil de système d'exploitation à la priorité la plus élevée est appliqué à l'évaluation de stratégie du système d'extrémité, et tout message configuré apparaît.

6. Le cas échéant, cliquez sur la liste colonne **Message** et sélectionnez **Show Message** pour ajouter un message à une condition. Puis cliquez sur l'icône **Message**, saisissez le message dans toutes les langues applicables (huit sont prises en charge), et cliquez sur **OK**.

Le message joint apparaît sur le système d'extrémité seulement si la condition est remplie.

Remarque : l'agent sélectionne le meilleur langage possible pour afficher les messages sur un système d'extrémité. Sophos vous recommande de créer un message en anglais (langue par défaut) afin qu'en cas d'impossibilité d'afficher un message dans une autre langue, un message puisse toujours être affiché à l'utilisateur du système d'extrémité. En outre, les versions antérieures de l'agent affichent seulement les messages en anglais (langue par défaut). Pour plus d'informations sur les messages, reportez-vous au *Guide de configuration de l'agent*.

7. Cliquez sur **Add Service Packs**.

Remarque : les service packs sont évalués seulement si le système d'exploitation est installé sur le système d'extrémité.

8. Sélectionnez les service packs que vous voulez ajouter au profil, et cliquez sur **OK**.
9. Le cas échéant, cliquez sur la liste colonne **Compliance State** pour changer les états de conformité pour chaque condition de service pack.

- **Installed** : si un service pack particulier est installé, l'état de conformité associé est appliqué à l'évaluation de stratégie du système d'exploitation et tout message configuré apparaît.
- **Else** : si aucun service pack est installé, l'état de conformité associé du profil du service pack à la priorité la plus élevée (le plus récent) est appliqué à l'évaluation de stratégie du système d'extrémité, et tout message configuré apparaît.

10. Le cas échéant, cliquez sur la liste de la colonne **Message** et sélectionnez **Show Message** pour ajouter un message à une condition. Puis cliquez sur l'icône **Message**, saisissez le message dans toutes les langues applicables (huit sont prises en charge), et cliquez sur **OK**.

Le message joint apparaît sur le système d'extrémité seulement si la condition est remplie.

11. Cliquez sur **Save**.

Remarque : une fois que le profil est créé, vous pouvez visualiser les stratégies qui utilisent ce profil depuis l'option de menu par clic droit dans la page de liste **Profiles** ou lors de la modification du profil en cliquant sur le lien **View Usage Details**.

3.2.10 Création de profils d'applications

La page Profils vous permet de créer des profils d'applications à utiliser dans les stratégies. Les profils d'applications servent à organiser et à classer par ordre de priorité les applications et fonctionnalités associées que vous voulez évaluer sur le système d'extrémité. Dans les profils, vous pouvez définir les conditions qui déterminent l'état de conformité des systèmes d'extrémité ainsi que les messages à afficher ou les actions correctives à effectuer sur le système d'extrémité.

Procédure

1. Cliquez sur **Manage > Profiles** . Puis cliquez sur **Create Profile** dans la section inférieure gauche de la page.
2. Saisissez un nom et une description de profil.
3. Cliquez sur **Select Profile Item**.
4. Sélectionnez un type de profil dans la liste **Profile Type**, tapez ou sélectionnez les options de recherche appropriées, puis cliquez sur **Search**.
5. Sélectionnez l'application pour laquelle vous voulez créer ce profil, et cliquez sur **OK**.

Remarque : pour que tous les noms d'applications s'affichent correctement, vous devez installer les fichiers de prise en charge des langues d'Asie Orientale (via le **Panneau de configuration > Options régionales et linguistiques**) sur la machine depuis laquelle vous visualisez le NAC Manager.

6. Le cas échéant, cliquez sur la liste de la colonne **Compliance State** pour changer les états de conformité des conditions d'applications suivantes. Pour plus d'informations, reportez-vous à la section [Détermination de l'état de conformité du système d'extrémité](#) à la page 49.
 - **Installed** : si l'application est installée, cet état de conformité est appliqué à l'évaluation de stratégie du système d'extrémité et tout message configuré apparaît.
 - **Else** : si l'application n'est pas installée, cet état de conformité est appliqué à l'évaluation de stratégie du système d'extrémité et tout message configuré apparaît.
7. Le cas échéant, cliquez sur la liste de la colonne **Message** et sélectionnez **Show Message** pour ajouter un message à une condition. Puis cliquez sur l'icône **Message**, saisissez le message dans toutes les langues applicables (huit sont prises en charge), et cliquez sur **OK**.

Le message joint apparaît sur le système d'extrémité seulement si la condition est remplie.

Remarque : l'agent sélectionne le meilleur langage possible pour afficher les messages sur un système d'extrémité. Sophos vous recommande de créer un message en anglais (langue par défaut) afin qu'en cas d'impossibilité d'afficher un message dans une autre langue, un message puisse toujours être affiché à l'utilisateur du système d'extrémité. En outre, les versions antérieures de l'agent affichent seulement les messages en anglais (langue par défaut). Pour plus d'informations sur les messages, reportez-vous au *Guide de configuration de l'agent*.

8. Cliquez sur **Add Capabilities**.

Les fonctionnalités sont les fonctions d'une application pouvant être testées dans le cadre de l'évaluation de la conformité. Les fonctionnalités contiennent des règles utilisées pour l'évaluation, qui rassemblent les conditions, les états de conformité, les messages et les actions correctives (le cas échéant).

les fonctionnalités sont évaluées seulement si l'application est installée sur le système d'extrémité.

9. Sélectionnez les fonctionnalités que vous voulez ajouter au profil et cliquez sur **OK**.

Pour plus d'informations sur les fonctionnalités, reportez-vous à la section [Visualisation des fonctionnalités d'applications et des conditions](#) à la page 41.

10. Effectuez l'une des opérations suivantes pour chaque fonctionnalité :

- a) Cliquez sur la liste de la colonne **Condition** pour sélectionner des conditions ou saisissez les paramètres de la condition dans les champs prévus.

Pour plus d'informations sur les conditions spécifiques à une fonctionnalité d'application, reportez-vous à la section [Visualisation des fonctionnalités d'applications et des conditions](#) à la page 41.

- b) Cliquez sur la liste colonne **Compliance State** pour changer les états de conformité pour chaque condition.
- c) Cliquez sur la liste colonne **Message** et sélectionnez **Show Message** pour ajouter un message à une condition. Puis cliquez sur l'icône **Message**, saisissez le message dans toutes les langues applicables (huit sont prises en charge), et cliquez sur **OK**.

Le message joint apparaît sur le système d'extrémité seulement si la condition est remplie.

- d) Sélectionnez la case à cocher colonne **Remediation Action** pour appliquer une action corrective à une condition.

L'action est exécutée sur le système d'extrémité seulement si la condition est remplie. Les actions correctives ne sont pas disponibles pour toutes les applications ou fonctionnalités d'application. Les actions correctives suivantes sont disponibles :

- **Enable** : sur le système d'extrémité, active la protection en temps réel pour les applications Anti-Virus ou Anti-Spyware, active le pare-feu pour les applications Firewall ou active les mises à jour automatiques pour les applications du gestionnaire de correctifs. Cette action est disponible pour la fonctionnalité d'application Real-Time Protection ou Enabled.
- **Update** : met à jour le fichier signature sur le système d'extrémité. Cette action est disponible pour la fonctionnalité Signature Date ou Signature Grace Period.
- **Scan** : lance un contrôle du système d'extrémité. Cette action est disponible pour la fonctionnalité Scan Date ou Scan Grace Period.
- **Apply** : applique la stratégie de la Sophos Enterprise Console pour l'application Sophos Anti-Virus sur le système d'extrémité. Cette action est disponible pour la fonction d'application des stratégies de la SEC.

- e) Cliquez sur **New Condition** pour ajouter des conditions supplémentaires à la fonctionnalité d'application.

Les conditions disponibles dépendent des fonctionnalités que vous avez sélectionnées à l'étape 9 ; si vous n'avez pas sélectionné de fonctionnalité avec des conditions supplémentaires, ce bouton n'apparaît pas. Si vous ajoutez des conditions supplémentaires, vous pouvez utiliser les flèches de direction haut et bas pour classer à nouveau par ordre de priorité les conditions pour l'évaluation du système d'extrémité.

11. Cliquez sur **Save**.

Remarque : une fois que le profil est créé, vous pouvez visualiser les stratégies qui utilisent ce profil depuis l'option de menu par clic droit dans la page de liste **Profiles** ou lors de la modification du profil en cliquant sur le lien **View Usage Details**.

3.2.11 Visualisation des fonctionnalités d'applications et des conditions

Les tableaux suivants décrivent les conditions disponibles pour chaque fonctionnalité d'application par type de profil :

Pour plus d'informations sur la création de profils d'applications, reportez-vous à la section [Création de profils d'applications](#) à la page 38.

Remarque : la disponibilité des fonctionnalités d'une application et des actions correctives dépend de la conception du logiciel de cette application. Il se peut que certaines fonctionnalités et actions correctives ne soient pas disponibles pour certains systèmes d'exploitation prenant en charge l'application ou pour toutes les versions d'une application. Si une fonctionnalité n'est pas prise en charge, elle n'apparaît pas. Si une fonctionnalité est prise en charge sur certains systèmes d'exploitation seulement, seuls les systèmes d'exploitation pris en charge apparaissent. Si une action corrective est prise en charge sur certains systèmes d'exploitation seulement, les systèmes d'exploitation non pris en charge apparaissent avec un x.

Sophos Anti-Virus

Remarque : en plus des fonctionnalités standard des applications antivirus, antispyware, HIPS et IDS, Sophos Anti-Virus prend en charge les fonctionnalités suivantes. Les fonctionnalités disponibles dépendent de la version du logiciel.

Fonctionnalité d'application	Description et conditions disponibles
Adware/PUA	<p>Détermine si un adware ou une application potentiellement indésirable (PUA) est détecté sur le système d'extrémité. Les conditions disponibles sont :</p> <ul style="list-style-type: none"> ■ Detected/Not Detected : spécifie si un adware ou une PUA est détecté ou non ainsi que l'état de conformité associé et le message si la condition est remplie. ■ Else : désigne l'état de conformité associé et le message si la condition Detected/Not Detected n'est pas remplie.
Controlled Applications	<p>Détermine si une application contrôlée est détectée sur le système d'extrémité. Les applications contrôlées sont définies dans la stratégie de la Sophos Enterprise Console. Les conditions disponibles sont :</p> <ul style="list-style-type: none"> ■ Detected/Not Detected : spécifie si un adware ou une PUA est détecté ou non ainsi que l'état de conformité associé et le message si la condition est remplie. ■ Else : désigne l'état de conformité associé et le message si la condition Detected/Not Detected n'est pas remplie.

Fonctionnalité d'application	Description et conditions disponibles
Managed by SEC	<p>Détermine si Sophos Anti-Virus est administré par la Sophos Enterprise Console ou est installé sous la forme d'un produit autonome. Les conditions disponibles sont :</p> <ul style="list-style-type: none"> ■ Yes/No : spécifie si Sophos Anti-Virus est administré par la Sophos Enterprise Console ainsi que l'état de conformité associé et le message si la condition est remplie. ■ Else : désigne l'état de conformité associé et le message si la condition Yes/No n'est pas remplie.
SEC Policy	<p>Détermine si Sophos Anti-Virus est conforme à la stratégie de la Sophos Enterprise Console. Les conditions disponibles sont :</p> <ul style="list-style-type: none"> ■ Conforms/Does Not Conform : spécifie si Sophos Anti-Virus est conforme à la stratégie de la Sophos Enterprise Console ainsi que l'état de conformité associé et le message si la condition est remplie. ■ Else : désigne l'état de conformité associé et le message si la condition Conforms/Does Not Conform n'est pas remplie.
Suspicious Behavior	<p>Détermine si un comportement suspect est détecté sur le système d'extrémité. Les conditions disponibles sont :</p> <ul style="list-style-type: none"> ■ Detected/Not Detected : spécifie si un comportement suspect est détecté ou non ainsi que l'état de conformité associé et le message si la condition est remplie. ■ Else : désigne l'état de conformité associé et le message si la condition Detected/Not Detected n'est pas remplie.
Suspicious File	<p>Détermine si un fichier suspect est détecté sur le système d'extrémité. Les conditions disponibles sont :</p> <ul style="list-style-type: none"> ■ Detected/Not Detected : spécifie si un fichier suspect est détecté ou non ainsi que l'état de conformité associé et le message si la condition est remplie. ■ Else : désigne l'état de conformité associé et le message si la condition Detected/Not Detected n'est pas remplie.
Virus/Spyware	<p>Détermine si un virus ou un spyware est détecté sur le système d'extrémité. Les conditions disponibles sont :</p> <ul style="list-style-type: none"> ■ Detected/Not Detected : spécifie si un virus ou un spyware est détecté ou non ainsi que l'état de conformité associé et le message si la condition est remplie. ■ Else : désigne l'état de conformité associé et le message si la condition Detected/Not Detected n'est pas remplie.

Antispyware ou antivirus

Fonctionnalité d'application	Description et conditions disponibles
Last Scan Date	<p>Détermine si la date du dernier contrôle de l'application correspond à la date spécifiée dans la condition. La fonctionnalité Last Scan Date peut être utilisée à la place de la fonctionnalité Last Scan Grace Period. Les conditions disponibles sont :</p> <ul style="list-style-type: none"> ■ Date : désigne la date du dernier contrôle du système d'extrémité ainsi que l'état de conformité associé, le message et l'action si la condition est remplie. Les opérateurs incluent == (Egal à), != (Différent de), < (Inférieur à), <= (Inférieur ou égal à), > (Supérieur à), >= (Supérieur ou égal à). ■ Else : désigne l'état de conformité associé, le message et l'action si la condition Date n'est pas remplie.
Last Scan Grace Period	<p>Détermine si la date du dernier contrôle de l'application est actuelle dans l'intervalle de temps spécifié dans la condition. La fonctionnalité Last Scan Date Period peut être utilisée à la place de la fonctionnalité Last Scan Date. Les conditions disponibles incluent :</p> <ul style="list-style-type: none"> ■ Within : désigne le nombre de jours dans lequel doit figurer la date du dernier contrôle effectué sur le système d'extrémité pour qu'elle soit considérée comme actuelle, ainsi que l'état de conformité associé, le message et l'action si la condition est remplie. ■ Else : désigne l'état de conformité associé, le message et l'action si la condition Within n'est pas remplie.
Real-Time Protection	<p>Détermine si l'application protège activement le système d'extrémité. Les conditions disponibles sont :</p> <ul style="list-style-type: none"> ■ Enabled/Disabled : spécifie si la protection en temps réel de l'application sur le système d'extrémité est activée ou désactivée ainsi que l'état de conformité associé, le message et l'action si la condition est remplie. ■ Else : désigne l'état de conformité associé et le message si la condition Enabled/Disabled n'est pas remplie.
Signature Date	<p>Détermine si la date du fichier signature de l'application correspond à la date spécifiée dans la condition. La fonctionnalité Signature Date peut être utilisée à la place de la fonctionnalité Signature Grace Period. Les conditions disponibles sont :</p> <ul style="list-style-type: none"> ■ Date : désigne la date du fichier signature du système d'extrémité ainsi que l'état de conformité associé, le message et l'action si la condition est remplie. Les opérateurs incluent == (Egal à), != (Différent de), < (Inférieur à), <= (Inférieur ou égal à), > (Supérieur à), >= (Supérieur ou égal à).

Fonctionnalité d'application	Description et conditions disponibles
	<ul style="list-style-type: none"> ■ Else : désigne l'état de conformité associé, le message et l'action si la condition Date n'est pas remplie.
Signature Grace Period	<p>Détermine si la date du fichier signature de l'application est actuelle dans l'intervalle de temps spécifié dans la condition. La fonctionnalité Signature Grace Period peut être utilisée à la place de la fonctionnalité Signature Date. Les conditions disponibles incluent :</p> <ul style="list-style-type: none"> ■ Within : désigne le nombre de jours dans lequel doit figurer la date du fichier signature sur le système d'extrémité pour qu'elle soit considérée comme actuelle, ainsi que l'état de conformité associé, le message et l'action si la condition est remplie. ■ Else : désigne l'état de conformité associé, le message et l'action si la condition Within n'est pas remplie.
Version	<p>Détermine si la version de l'application présente sur le système d'extrémité remplit la condition.</p> <p>Remarque : la version est évaluée sur le système d'extrémité à l'aide du nombre de valeurs significatives spécifiées dans la condition. Par exemple, si vous créez une condition qui spécifie == 8 et que la version du système d'extrémité est 8.1, le logiciel compare 8.1 à 8 dans la condition (une valeur significative), et la condition est remplie. En revanche, si vous créez une condition qui spécifie == 8.0 et que la version du système d'extrémité est 8.1, le logiciel compare 8.1 à 8.0 dans la condition (deux valeurs significatives), et la condition n'est pas remplie.</p> <ul style="list-style-type: none"> ■ Si l'application a été définie pour spécifier une version dans le profil, les conditions disponibles dans le profil sont : <ul style="list-style-type: none"> ■ Version : désigne la version de l'application présente sur le système d'extrémité ainsi que l'état de conformité associé et le message si la condition est remplie. Les opérateurs incluent == (Egal à), != (Différent de), < (Inférieur à), <= (Inférieur ou égal à), > (Supérieur à), >= (Supérieur ou égal à). La version doit être au format N.n.n.n et est limitée à quatre valeurs significatives. ■ Else : désigne l'état de conformité associé et le message si la condition Version n'est pas remplie. ■ Si l'application a été définie avec la version spécifiée dans les règles de détection d'applications, les conditions disponibles dans le profil sont : <ul style="list-style-type: none"> ■ Pass/Fail : spécifie si l'évaluation sur le système d'extrémité réussit ou échoue si la version de l'application présente sur le système d'extrémité correspond à celle spécifiée dans les règles de détection d'applications et désigne l'état de conformité associé et le message si la condition est remplie. ■ Else : désigne l'état de conformité associé et le message si la condition Pass/Fail n'est pas remplie.

Evaluation, HIPS ou IDS

Fonctionnalité d'application	Description et conditions disponibles
Running	<p>Détermine si les services exécutables fonctionnent sur le système d'extrémité. Les conditions disponibles sont :</p> <ul style="list-style-type: none"> ■ Running/Not Running : spécifie si les services exécutables sur le système d'extrémité fonctionnent ou pas ainsi que l'état de conformité associé, le message et l'action si la condition est remplie. ■ Else : désigne l'état de conformité associé et le message si la condition Running/Not Running n'est pas remplie.
Version	<p>Détermine si la version de l'application présente sur le système d'extrémité remplit la condition.</p> <p>Remarque : la version est évaluée sur le système d'extrémité à l'aide du nombre de valeurs significatives spécifiées dans la condition. Par exemple, si vous créez une condition qui spécifie == 8 et que la version du système d'extrémité est 8.1, le logiciel compare 8.1 à 8 dans la condition (une valeur significative), et la condition est remplie. En revanche, si vous créez une condition qui spécifie == 8.0 et que la version du système d'extrémité est 8.1, le logiciel compare 8.1 à 8.0 dans la condition (deux valeurs significatives), et la condition n'est pas remplie.</p> <ul style="list-style-type: none"> ■ Si l'application a été définie pour spécifier une version dans le profil, les conditions disponibles dans le profil sont : <ul style="list-style-type: none"> ■ Version : désigne la version de l'application présente sur le système d'extrémité ainsi que l'état de conformité associé et le message si la condition est remplie. Les opérateurs incluent == (Egal à), != (Différent de), < (Inférieur à), <= (Inférieur ou égal à), > (Supérieur à), >= (Supérieur ou égal à). La version doit être au format N.n.n.n et est limitée à quatre valeurs significatives. ■ Else : désigne l'état de conformité associé et le message si la condition Version n'est pas remplie. ■ Si l'application a été définie avec la version spécifiée dans les règles de détection d'applications, les conditions disponibles dans le profil sont : <ul style="list-style-type: none"> ■ Pass/Fail : spécifie si l'évaluation sur le système d'extrémité réussit ou échoue si la version de l'application présente sur le système d'extrémité correspond à celle spécifiée dans les règles de détection d'applications et désigne l'état de conformité associé et le message si la condition est remplie. ■ Else : désigne l'état de conformité associé et le message si la condition Pass/Fail n'est pas remplie.

Chiffrement

Fonctionnalité d'application	Description et conditions disponibles
Full Disk Encryption	<p>Détermine si les disques durs sur le système d'extrémité sont cryptés. Les conditions disponibles sont :</p> <ul style="list-style-type: none"> ■ All Drives/At Least 1 Drive/No Drives : spécifie si tous les lecteurs, au moins 1 lecteur, ou aucun lecteur sur le système d'extrémité n'est crypté, et l'état de conformité et le message associés si la condition est remplie. ■ Else : désigne l'état de conformité associé et le message si les autres conditions ne sont pas remplies.
Pre-boot Authentication	<p>Détermine si l'application est activée pour authentifier l'utilisateur avant le démarrage du système d'extrémité. Les conditions disponibles sont :</p> <ul style="list-style-type: none"> ■ Enabled/Temporarily Disabled/Disabled : spécifie si l'authentification avant initialisation est activée, temporairement désactivée ou désactivée sur système d'extrémité ainsi que l'état de conformité associé, le message et l'action si la condition est remplie. ■ Else : désigne l'état de conformité associé, le message et l'action si les autres conditions ne sont pas remplies.
Version	<p>Détermine si la version de l'application présente sur le système d'extrémité remplit la condition.</p> <p>Remarque : la version est évaluée sur le système d'extrémité à l'aide du nombre de valeurs significatives spécifiées dans la condition. Par exemple, si vous créez une condition qui spécifie == 8 et que la version du système d'extrémité est 8.1, le logiciel compare 8.1 à 8 dans la condition (une valeur significative), et la condition est remplie. En revanche, si vous créez une condition qui spécifie == 8.0 et que la version du système d'extrémité est 8.1, le logiciel compare 8.1 à 8.0 dans la condition (deux valeurs significatives), et la condition n'est pas remplie.</p> <ul style="list-style-type: none"> ■ Si l'application a été définie pour spécifier une version dans le profil, les conditions disponibles dans le profil sont : <ul style="list-style-type: none"> ■ Version : désigne la version de l'application présente sur le système d'extrémité ainsi que l'état de conformité associé et le message si la condition est remplie. Les opérateurs incluent == (Egal à), != (Différent de), < (Inférieur à), <= (Inférieur ou égal à), > (Supérieur à), >= (Supérieur ou égal à). La version doit être au format N.n.n.n et est limitée à quatre valeurs significatives. ■ Else : désigne l'état de conformité associé et le message si la condition Version n'est pas remplie.

Fonctionnalité d'application	Description et conditions disponibles
	<ul style="list-style-type: none"> ■ Si l'application a été définie avec la version spécifiée dans les règles de détection d'applications, les conditions disponibles dans le profil sont : <ul style="list-style-type: none"> ■ Pass/Fail : spécifie si l'évaluation sur le système d'extrémité réussit ou échoue si la version de l'application présente sur le système d'extrémité correspond à celle spécifiée dans les règles de détection d'applications et désigne l'état de conformité associé et le message si la condition est remplie. ■ Else : désigne l'état de conformité associé et le message si la condition Pass/Fail n'est pas remplie.

Pare-feu

Fonctionnalité d'application	Description et conditions disponibles
Enabled	<p>Détermine si l'application protège activement le système d'extrémité. Les conditions disponibles sont :</p> <ul style="list-style-type: none"> ■ Enabled/Disabled : spécifie si le pare-feu sur le système d'extrémité est activé ou désactivé ainsi que l'état de conformité associé, le message et l'action si la condition est remplie. ■ Else : désigne l'état de conformité associé et le message si la condition Enabled/Disabled n'est pas remplie.
Running	<p>Détermine si les services exécutables fonctionnent sur le système d'extrémité. Les conditions disponibles sont :</p> <ul style="list-style-type: none"> ■ Running/Not Running : spécifie si les services exécutables sur le système d'extrémité fonctionnent ou pas ainsi que l'état de conformité associé, le message et l'action si la condition est remplie. ■ Else : désigne l'état de conformité associé et le message si la condition Running/Not Running n'est pas remplie.
Version	<p>Détermine si la version de l'application présente sur le système d'extrémité remplit la condition.</p> <p>Remarque : la version est évaluée sur le système d'extrémité à l'aide du nombre de valeurs significatives spécifiées dans la condition. Par exemple, si vous créez une condition qui spécifie == 8 et que la version du système d'extrémité est 8.1, le logiciel compare 8.1 à 8 dans la condition (une valeur significative), et la condition est remplie. En revanche, si vous créez une condition qui spécifie == 8.0 et que la version du système d'extrémité est</p>

Fonctionnalité d'application	Description et conditions disponibles
	<p>8.1, le logiciel compare 8.1 à 8.0 dans la condition (deux valeurs significatives), et la condition n'est pas remplie.</p> <ul style="list-style-type: none"> ■ Si l'application a été définie pour spécifier une version dans le profil, les conditions disponibles dans le profil sont : <ul style="list-style-type: none"> ■ Version : désigne la version de l'application présente sur le système d'extrémité ainsi que l'état de conformité associé et le message si la condition est remplie. Les opérateurs incluent == (Egal à), != (Différent de), < (Inférieur à), <= (Inférieur ou égal à), > (Supérieur à), >= (Supérieur ou égal à). La version doit être au format N.n.n.n et est limitée à quatre valeurs significatives. ■ Else : désigne l'état de conformité associé et le message si la condition Version n'est pas remplie. ■ Si l'application a été définie avec la version spécifiée dans les règles de détection d'applications, les conditions disponibles dans le profil sont : <ul style="list-style-type: none"> ■ Pass/Fail : spécifie si l'évaluation sur le système d'extrémité réussit ou échoue si la version de l'application présente sur le système d'extrémité correspond à celle spécifiée dans les règles de détection d'applications et désigne l'état de conformité associé et le message si la condition est remplie. ■ Else : désigne l'état de conformité associé et le message si la condition Pass/Fail n'est pas remplie.

Gestionnaire des correctifs

Fonctionnalité d'application	Description et conditions disponibles
Enabled	<p>Détermine si l'application protège activement le système d'extrémité. Les conditions disponibles sont :</p> <ul style="list-style-type: none"> ■ Enabled/Disabled : spécifie si les mises à jour automatiques de l'outil Windows Update sont activées ou désactivées sur le système d'extrémité ainsi que l'état de conformité associé, le message et l'action si la condition est remplie. ■ Else : désigne l'état de conformité associé et le message si la condition Enabled/Disabled n'est pas remplie.

3.2.12 Détermination de l'état de conformité du système d'extrémité

L'état de conformité est déterminé par la conformité ou non du système d'extrémité avec les profils dans la stratégie. Le logiciel évalue les conditions du profil en fonction du comportement de stratégie affecté pour ce type de profil. Puis il ramène toutes les informations d'évaluation NAC au niveau de la stratégie et affecte un état de conformité d'après l'état le moins conforme. Une fois qu'un état de conformité est déterminé, l'accès réseau basé sur cet état de conformité peut être appliqué à l'aide des modèles d'accès affectés dans la stratégie.

- **Compliant** : si cette condition est satisfaite au cours de la vérification, l'état est déterminé comme conforme.
- **Partially Compliant** : si cette condition est satisfaite au cours de la vérification, l'état est déterminé comme partiellement conforme.
- **Non-Compliant** : si cette condition est satisfaite au cours de la vérification, l'état est déterminé comme non conforme.

3.3 Aperçu de la zone Enforce

La zone Enforce contient tous les composants nécessaires pour paramétrer les ressources réseau, les paramètres d'accès réseau et les exemptions. Vous pouvez accéder aux zones suivantes depuis le menu Enforce :

Zone et action	Description
DHCP Configuration Wizard	
Exécuter l'assistant de configuration de DHCP.	L' assistant de configuration de DHCP vous aide à identifier les serveurs web proxy, les serveurs de correction et les serveurs DHCP Enforcer à utiliser avec les implémentations DHCP de Sophos NAC et configure automatiquement les modèles d'accès DHCP Enforcer par défaut avec vos définitions de serveurs.
Network resources réseau	
Créer des ressources réseau.	Les ressources réseau sont des applications ou des périphériques nécessaires pour la correction des systèmes d'extrémité ou ceux dont l'accès par les systèmes d'extrémité placés en quarantaine doit être refusé. Les ressources réseau peuvent être ajoutées aux modèles d'accès de l'Agent Enforcer ou du DHCP Enforcer. Remarque : les ressources réseau sont utilisées pour l'application de la quarantaine à base de clients à l'aide de l'agent de quarantaine ou pour l'application du protocole DHCP.
Agent Enforcer access templates	
Créer des modèles d'accès Agent Enforcer.	Les modèles d'accès Agent Enforcer vous permettent d'identifier les ressources réseau auxquelles les systèmes d'extrémité peuvent ou ne peuvent pas accéder lors de l'application de la quarantaine de type clients. Une fois créés, les modèles d'accès Agent Enforcer peuvent être affectés à des stratégies pour appliquer l'accès basé sur l'agent ou l'état de conformité du système d'extrémité.

Zone et action	Description
	<p>Remarque : les modèles d'accès Agent Enforcer s'appliquent seulement aux systèmes d'extrémité exécutant l'agent de quarantaine.</p>
DHCP Enforcer access templates	
<p>Créer des modèles d'accès DHCP Enforcer.</p>	<p>Les modèles d'accès DHCP Enforcer vous permettent de spécifier des paramètres d'accès nécessaires à la prise en charge de l'authentification et l'application du protocole DHCP. Une fois créés, les modèles d'accès DHCP Enforcer peuvent être affectés aux stratégies, aux exemptions et aux paramètres Enforcer.</p> <p>Remarque : les modèles d'accès DHCP Enforcer sont seulement utilisés avec les mises en place DHCP de Sophos NAC.</p>
Exemptions	
<p>Créer des exemptions.</p>	<p>Les exemptions identifient selon divers critères les systèmes d'extrémité dont la conformité n'a pas à être évaluée lors de la connexion au réseau. Les postes d'extrémités exemptés incluent soit ceux qui sont incapables d'exécuter l'agent, tels que les postes utilisant des systèmes d'exploitation autres que Windows soit ceux qui ne nécessitent pas d'évaluation de la conformité comme les serveurs, routeurs ou imprimantes.</p> <p>Remarque : les exemptions sont seulement utilisées avec l'application du protocole DHCP.</p>
<p>Désactiver ou activer des exemptions.</p>	<p>Les exemptions peuvent être désactivées ou activées par un administrateur système. La désactivation d'une exemption permet l'évaluation de la conformité du système d'extrémité. Si l'exemption est désactivée et si Sophos Compliance Agent n'est pas installé sur le système d'extrémité, ce dernier est considéré comme inconnu. L'activation d'une exemption empêche l'évaluation de la conformité du système d'extrémité.</p>

3.3.1 Création de modèles d'accès Agent Enforcer

La page Agent Enforcer Access Templates vous permet d'identifier les ressources réseau auxquelles les systèmes d'extrémité peuvent ou ne peuvent pas accéder lors de l'application de la quarantaine de type clients. Les modèles d'accès Agent Enforcer s'appliquent seulement aux systèmes d'extrémité exécutant l'agent de quarantaine.

Les ressources réseau définies dans le modèle d'accès Agent Enforcer régulent l'accès du système d'extrémité au réseau. Par exemple, si une évaluation de conformité indique qu'un système d'extrémité est non conforme, le modèle d'accès Agent Enforcer associé à l'état non conforme de la stratégie est appliqué et l'accès aux ressources réseau spécifiées sont autorisées ou refusées. Pour plus d'informations sur les ressources réseau, reportez-vous à la section [Création de ressources réseau](#) à la page 56. Une fois que vous avez créé un modèle d'accès, vous pouvez l'affecter à des stratégies. Pour plus d'informations, reportez-vous à la section [Mise à jour des stratégies](#) à la page 28 .

Procédure

1. Cliquez sur **Enforce > Agent Enforcer Access Templates** . Puis cliquez sur **Create Agent Enforcer Access Template** dans la section inférieure gauche de la page.
2. Saisissez un nom et une description de modèle d'accès Agent Enforcer.
3. Sélectionnez la case à cocher située près des états de conformité de modèles appropriés pour déterminer comment le modèle d'accès Agent Enforcer doit être affecté ou désigné en vue d'une sélection dans les stratégies.
4. Effectuez l'une des opérations suivantes pour spécifier les ressources réseau pour l'accès par les systèmes d'extrémité :
 - Cliquez sur **Select** pour ajouter des ressources réseau au modèle d'accès, sélectionnez les ressources réseau appropriées et cliquez sur **OK**.
 - Cliquez sur **Create** pour créer de nouvelles ressources réseau pour le modèle d'accès, rentrez les informations dans les champs appropriés et cliquez sur **Save**. Répétez cette étape si nécessaire pour créer des ressources réseau supplémentaires pour le modèle d'accès. Pour plus d'informations, reportez-vous à la section [Création de ressources réseau](#) à la page 56.
5. Sélectionnez le comportement d'accès de chaque ressource réseau. Les options sont les suivantes :
 - **Deny** : refuse tout trafic réseau provenant du système d'extrémité pour la ressource réseau.
 - **Permit** : autorise tout trafic réseau provenant du système d'extrémité pour la ressource réseau.
6. Si nécessaire, utilisez les flèches pour classer par ordre de priorité les ressources réseau.

Si plusieurs ressources réseau s'appliquent à un système d'extrémité, la première qui correspond déterminera l'accès réseau pour la session des systèmes d'extrémité. Sophos vous conseille de classer par ordre de priorité les ressources réseau les plus spécifiques/strictes, puis les moins spécifiques/strictes. Les ressources réseau exécutables sont évaluées avant les ressources réseau de ports/protocoles.
7. Cliquez sur **Save**.

Remarque : cliquez sur le lien **View Template Details** pour visualiser les applications et les ressources réseau, en priorité, associées au modèle d'accès Agent Enforcer. Une fois que le modèle d'accès Agent Enforcer est créé, vous pouvez visualiser les stratégies qui utilisent ce modèle depuis l'option de menu par clic droit dans la page de liste **Agent Enforcer Access Templates** ou lors de la modification du modèle en cliquant sur le lien **View Usage Details**.

3.3.2 Création de modèles d'accès DHCP Enforcer

La page DHCP Enforcer Access Templates vous permet de spécifier des paramètres d'accès nécessaires à la prise en charge de l'application du protocole DHCP. Les modèles d'accès DHCP Enforcer sont seulement utilisés avec les implémentations DHCP de Sophos NAC.

Si vous configurez l'application du protocole DHCP pour la première fois, Sophos vous conseille d'utiliser l'assistant de configuration DHCP. Pour plus d'informations, reportez-vous à la section [Exécution de l'assistant de configuration DHCP](#) à la page 54. Si vous utilisez une

configuration DHCP avancée, vous pouvez créer ou mettre à jour les modèles d'accès DHCP Enforcer existants.

Les ressources réseau définies dans le modèle d'accès DHCP Enforcer régulent l'accès du système d'extrémité au réseau. Par exemple, si une évaluation de conformité indique qu'un système d'extrémité est non conforme, le modèle d'accès DHCP Enforcer associé à l'état non conforme de la stratégie et qui correspond à l'adresse IP du serveur ou du relais DHCP est appliqué et l'accès aux ressources réseau spécifiées est autorisé ou refusé. Pour plus d'informations sur les ressources réseau, reportez-vous à la section [Création de ressources réseau](#) à la page 56. Une fois que vous avez créé un modèle d'accès, vous pouvez l'affecter à des stratégies, des exemptions ou des paramètres Enforcer. Pour plus d'informations, reportez-vous aux sections [Mise à jour des stratégies](#) à la page 28 , [Création d'exemptions](#) à la page 58 ou [Spécification des paramètres Enforcer](#) à la page 82.

Procédure

1. Cliquez sur **Enforce > DHCP Enforcer Access Templates** . Puis cliquez sur **Create DHCP Enforcer Access Template** dans la section inférieure gauche de la page.
2. Saisissez un nom et une description de modèle d'accès DHCP Enforcer.
3. Sélectionnez la case à cocher située près des états de conformité de modèles appropriés pour déterminer comment le modèle d'accès DHCP Enforcer doit être affecté ou désigné en vue d'une sélection dans les stratégies, les exemptions et les paramètres Enforcer.
4. Sélectionnez **Full Access** pour autoriser l'accès réseau complet aux systèmes d'extrémité ou **Restricted** pour désigner des ressources réseau spécifiques auxquelles l'accès est autorisé ou refusé.

5. Si vous avez sélectionné l'accès Restricted à l'étape 4, vous pouvez optionnellement sélectionner la case à cocher **Prevent LAN Access** pour empêcher les systèmes d'extrémité d'accéder au réseau local (LAN). En outre, sélectionnez **Permit** ou **Deny** pour désigner le type d'accès que vous voulez fournir. Si vous sélectionnez Permit, vous permettez l'accès seulement aux ressources réseau que vous spécifiez, le serveur NAC Sophos et le serveur de l'agent temporaire ; tout autre accès réseau est refusé. Si vous sélectionnez Deny, vous refusez l'accès seulement aux ressources réseau que vous spécifiez ; tout autre accès réseau est autorisé. Effectuez l'une des opérations suivantes pour spécifier les ressources réseau pour l'accès par les systèmes d'extrémité :

- Cliquez sur **Select** pour ajouter des ressources réseau au modèle d'accès, sélectionnez les ressources réseau appropriées et cliquez sur **OK**. Seules les ressources réseau de ports/protocoles avec des plages d'adresses IP spécifiques (non pas N'IMPORTE LESQUELLES) sont disponibles pour la sélection.
- Cliquez sur **Create** pour créer de nouvelles ressources réseau pour le modèle d'accès, rentrez les informations dans les champs appropriés et cliquez sur **Save**. Répétez cette étape si nécessaire pour créer des ressources réseau supplémentaires pour le modèle d'accès. Pour plus d'informations, reportez-vous à la section [Création de ressources réseau](#) à la page 56.

Important : lors de la restriction de l'accès avec l'option **Deny**, vous devez désactiver Proxy ARP sur votre réseau pour que le DHCP Enforcer limite correctement l'accès aux systèmes d'extrémité.

Remarque : si vous sélectionnez l'option **Permit** et si vous avez installé la Sophos Enterprise Console sur un serveur distinct de Sophos NAC, vous devez créer une ressource réseau pour le serveur de la Sophos Enterprise Console et l'ajouter à votre modèle d'accès DHCP Enforcer.

Remarque : chaque modèle d'accès DHCP Enforcer autorise un nombre défini d'itinéraires hôtes et d'itinéraires réseau qui sont déterminés par les désignations d'adresse IP/sous-réseau dans les ressources réseau. Si vous dépassez la limite, vous pouvez résoudre ce problème en supprimant les ressources réseau du modèle d'accès ou en supprimant des itinéraires des ressources réseau incluses dans le modèle d'accès.

6. Vous pouvez spécifier des options DHCP supplémentaires en cliquant sur **Advanced Options** dans la section inférieure gauche de la page. Les options avancées incluent :
 - **User Class** : cette option vous permet d'utiliser la classe utilisateur du client DHCP ou de la remplacer par une classe utilisateur spécifiée. Vous pouvez configurer votre serveur DHCP pour qu'il affecte des adresses IP en fonction de la classe utilisateur. Si elle est spécifiée, la classe utilisateur est appliquée aux systèmes d'extrémité en fonction de l'état de conformité du système d'extrémité auquel le modèle est associé et avant l'affectation des adresses IP.

Important :

 - Si elle est utilisée, la classe utilisateur est alphanumérique, sensible aux majuscules et doit correspondre à une classe utilisateur sur le serveur DHCP.
 - Si vous spécifiez une classe utilisateur et si l'agent de quarantaine n'a pas encore récupéré la stratégie d'après l'intervalle de rafraîchissement des stratégies, il se peut que l'agent n'utilise pas la classe utilisateur appropriée et, par conséquent, qu'il n'obtienne pas correctement les adresses IP tant que la stratégie correcte n'a pas été récupérée.
 - **Lease Duration** : cette option vous permet d'utiliser les paramètres de location du serveur DHCP ou d'affecter des paramètres de location.
 - **DNS Servers** : cette option vous permet de désigner des serveurs DNS principaux et secondaires. Cette option est seulement nécessaire si vous utilisez un portail captif. Vous pouvez acheminer les utilisateurs inconnus ou invités sur les serveurs DNS d'après leur état de conformité de système d'extrémité.
 - **DHCP Server IP Scopes** : cette option vous permet de spécifier pour quelles étendues IP le modèle d'accès sera utilisé. Sélectionnez la case à cocher **ANY** ou saisissez les adresses IP de début et de fin de l'étendue IP dans les champs prévus, et cliquez sur **Add**. Répétez cette opération autant de fois que nécessaire pour ajouter des étendues supplémentaires.
7. Cliquez sur **Save**.

Remarque : une fois que le modèle d'accès DHCP Enforcer est créé, vous pouvez visualiser les stratégies, les exemptions ou les états d'accès Enforcer qui utilisent ce modèle depuis l'option de menu par clic droit dans la page de liste **DHCP Enforcer Access Templates** ou lors de la modification du modèle d'accès en cliquant sur le lien **View Usage Details**.

3.3.3 Exécution de l'assistant de configuration DHCP

L'assistant de configuration DHCP vous aide à identifier les serveurs proxy, correctifs, de l'agent temporaire et DHCP Enforcer à utiliser avec les mises en application du protocole DHCP de Sophos NAC et configure automatiquement les modèles d'accès DHCP Enforcer par défaut avec vos définitions de serveurs. Si vous exécutez l'assistant pour mettre à jour les paramètres, vous allez effacer la configuration DHCP courante et remplacer les serveurs présents dans les modèles d'accès DHCP Enforcer par défaut par ceux que vous définissez dans l'assistant.

Pour plus d'informations sur la configuration de l'application du protocole DHCP, reportez-vous au *Guide de configuration DHCP de Sophos NAC*.

Procédure

1. Cliquez sur **Configure System > DHCP Configuration Wizard**. Cliquez sur **Next** pour continuer.
2. 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 4.

3. 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 en cours d'utilisation dans le modèle d'accès DHCP - Internet Access DHCP Enforcer par défaut.

4. 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 proxy sélectionnés remplaceront les serveurs en cours d'utilisation dans le modèle d'accès DHCP - Remediation Access DHCP Enforcer par défaut.

5. Procédez de l'une des manières suivantes :
 - Si vous avez installé l'agent temporaire, cliquez sur **Yes**, puis 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 7.

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.

6. 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**.
7. Définissez les serveurs qui seront utilisés pour l'application du protocole 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**.
8. Cliquez sur **Terminer**.

Remarque : par défaut, de nouveaux serveurs DHCP Enforcer sont paramétrés pour signaler seulement l'accès des systèmes d'extrémité inconnus. Pour appliquer l'accès réseau pour les systèmes d'extrémité inconnus, vous devez changer le mode des systèmes d'extrémité inconnus de chaque serveur DHCP Enforcer en **Enforce** sur la page **Configure System > Server Settings**. Pour plus d'informations, reportez-vous à la section [Création de serveurs DHCP Enforcer](#) à la page 84.

Remarque : par défaut, les stratégies sont paramétrées pour seulement signaler l'accès des systèmes d'extrémité. Pour appliquer l'accès réseau pour les systèmes d'extrémité administrés ou non administrés connus, vous devez pour chaque stratégie changer le mode de stratégie en **Enforce** sur la page **Manage > Policies**. Pour plus d'informations, reportez-vous à la section [Mise à jour des stratégies](#) à la page 28.

3.3.4 Création de ressources réseau

Les ressources réseau sont des applications ou des périphériques nécessaires pour la correction des systèmes d'extrémité ou ceux dont l'accès par les systèmes d'extrémité placés en quarantaine doit être refusé. Par exemple, vous pouvez, si vous le souhaitez, autoriser l'accès pour les applications logicielles antivirus ou aux serveurs de fichiers qui hébergent ces applications, ou bien bloquer sur le réseau les applications ou les systèmes de messagerie professionnels qui utilisent les adresses IP publiques. Les ressources réseau peuvent être ajoutées aux modèles d'accès de l'Agent Enforcer ou du DHCP Enforcer. Les modèles d'accès peuvent être affectés à des stratégies pour appliquer l'accès (en autorisant ou en refusant) basé sur l'état de conformité du système d'extrémité.

Procédure

1. Cliquez sur **Enforce > Network Resources**. Puis cliquez sur **Create Network Resource** dans la section inférieure gauche de la page.
2. Saisissez un nom et une description de ressource réseau.

3. Cliquez dans la liste **Network Resource Type** et sélectionnez **Port/Protocol** ou **Executable**. Concernant les ressources réseau exécutables utilisées dans les modèles d'accès Agent Enforcer, l'agent évalue le trafic provenant du système d'extrémité pour déterminer quels processus autoriser ou refuser. Concernant les ressources réseau de ports/protocoles utilisées dans les modèles d'accès Agent Enforcer ou DHCP Enforcer, l'Agent Enforcer ou le DHCP Enforcer, respectivement, évalue à quelles destinations l'accès est autorisé ou refusé pour un système d'extrémité.

Remarque : vous devez créer une ressource réseau distincte pour chaque exécutable d'application.

Remarque : seules les ressources réseau de ports/protocoles sont disponibles pour l'application de DHCP.

4. Procédez de l'une des manières suivantes :

- Si vous avez sélectionné Port/Protocol à l'étape 3, sélectionnez la catégorie de serveurs dans la liste **Server Category**. Puis cliquez sur l'option **ANY** pour créer une ressource réseau s'appliquant à tout port, ou cliquez sur l'option située près du champ prévu et saisissez un port spécifique dans le champ ; sélectionnez le protocole et cliquez sur **Add**. Répétez cette opération autant que nécessaire pour ajouter des ports et des protocoles supplémentaires.
- Si vous avez sélectionné Executable à l'étape 3, saisissez le nom du processus exécutable de l'application dans le champ **Name**.

Important :

- Le nom du processus exécutable **doit** être le nom qui apparaît dans l'onglet **Processus** du **Gestionnaire des tâches Windows**.
 - Les noms d'exécutables **doivent** posséder l'extension **.exe** à moins qu'un nom de processus ne contiennent pas d'extension ; **ne peuvent pas** dépasser 64 caractères en longueur ; **ne peuvent pas** utiliser les caractères suivants : \ / : * ? " < > et | ; **ne peuvent pas** contenir d'informations sur le chemin du fichier ; ne reconnaissent **pas** les caractères joker et seront **seulement** pris en charge pour les protocoles TCP et UDP.
 - Le logiciel détecte seulement les exécutables qui s'exécutent au niveau Winsock.
5. Optionnellement, pour désigner un serveur de destination, sélectionnez **IP Address** ou **Host Name** ; et saisissez l'adresse IP, le sous-réseau supplémentaire et la description, ou le nom d'hôte et la description dans les champs appropriés et cliquez sur **Add**.

Répétez cette étape autant que nécessaire pour ajouter des adresses IP et des sous-réseaux supplémentaires ou des noms d'hôtes.

Important : l'accès aux systèmes d'extrémité utilisant Windows 2000 sera refusé aux ressources réseau qui ont un masque de sous-réseau qui n'est **pas** 255.255.255.255 et qui sont utilisés dans les modèles d'accès DHCP Enforcer.

6. Cliquez sur **Save**.

Remarque : une fois que la ressource réseau est créée, vous pouvez visualiser les modèles d'accès qui utilisent cette ressource réseau depuis l'option de menu par clic droit dans la page de liste **Network Resources** ou lors de la modification de la ressource réseau en cliquant sur le lien **View Usage Details**.

3.3.5 Création d'exemptions

La page Exemptions vous permet d'identifier selon divers critères les systèmes d'extrémité dont la conformité n'a pas à être évaluée lors de la connexion au réseau. Les exemptions incluent les postes d'extrémité qui soit sont incapables d'exécuter l'agent, tels que les postes utilisant des systèmes d'exploitation autres que Windows soit ne nécessitent pas d'évaluation de la conformité comme les serveurs, routeurs ou imprimantes. En outre, pour effectuer un déploiement par phases dans toute l'entreprise, vous pouvez exempter des systèmes d'extrémité ou des réseaux sur lesquels vous ne souhaitez pas encore appliquer quoi que ce soit.

Remarque : les exemptions sont seulement utilisées avec l'application du protocole DHCP.

3.3.6 Création d'exemptions de critères DHCP

La page Exemptions vous permet d'identifier les systèmes d'extrémité dont la conformité n'a pas à être évaluée lors de la connexion au réseau. 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. Une fois que vous avez créé des exemptions, vous pouvez les classer par ordre de priorité sur la page de liste Exemptions.

Procédure

1. Cliquez sur **Enforce > Exemptions** . Puis cliquez sur **Create Exemption** dans la section inférieure gauche de la page.
2. Saisissez un nom et une description d'exemption.
3. Si vous voulez désactiver cette exemption, sélectionnez la case à cocher **Disable Exemption**.

La désactivation d'une exemption permet l'évaluation de la conformité du système d'extrémité. Si l'exemption est désactivée et si Sophos Compliance Agent n'est pas installé sur le système d'extrémité, ce dernier est considéré comme inconnu.

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 MAC 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. Sous Access Templates, cliquez sur **Select** pour ajouter des modèles d'accès DHCP Enforcer existants à l'exemption, sélectionnez les modèles appropriés et cliquez sur **OK**.

Si vous ne voyez pas le modèle d'accès DHCP Enforcer dont vous avez besoin, vous pouvez en créer un. Pour plus d'informations, reportez-vous à la section [Création de modèles d'accès DHCP Enforcer](#) à la page 51.

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.

3.3.7 Création d'exemptions par étendues IP

La page Exemptions vous permet d'identifier à l'aide des étendues IP les systèmes d'extrémité dont la conformité n'a pas à être évaluée lors de la connexion au réseau. Les exemptions par étendues IP sont des exemptions créées pour des segments du réseau. Les modèles d'accès DHCP Enforcer associés déterminent à la fois les étendues DHCP et l'action d'accès réseau appropriée à prendre. L'exemption par étendues IP est utile lors de l'exécution d'un déploiement par phases de l'application dans toute l'entreprise ; vous pouvez exempter des systèmes d'extrémité ou des réseaux que vous ne souhaitez simplement pas encore appliquer. Une fois que vous avez créé des exemptions, vous pouvez les classer par ordre de priorité sur la page de liste Exemptions.

Procédure

1. Cliquez sur **Enforce > Exemptions** . Puis cliquez sur **Create Exemption** dans la section inférieure gauche de la page.
2. Saisissez un nom et une description d'exemption.
3. Si vous voulez désactiver cette exemption, sélectionnez la case à cocher **Disable Exemption**.

La désactivation d'une exemption permet l'évaluation de la conformité du système d'extrémité. Si l'exemption est désactivée et si Sophos Compliance Agent n'est pas installé sur le système d'extrémité, ce dernier est considéré comme inconnu.

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 plus d'informations, reportez-vous à la section [Création de modèles d'accès DHCP Enforcer](#) à la page 51.

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

Si plusieurs étendues s'appliquent à une exemption particulière, la première étendue qui correspond sera utilisée. Sophos vous conseille 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.

3.3.8 Désactivation ou activation des exemptions

Les exemptions sont automatiquement activées lors de leur création, à moins que vous ne les désactiviez explicitement. La désactivation d'une exemption permet l'évaluation de la conformité du système d'extrémité. Si l'exemption est désactivée et si Sophos Compliance Agent n'est pas installé sur le système d'extrémité, ce dernier est considéré comme inconnu.

Procédure

1. Cliquez sur **Enforce > Exemptions**.
2. Cliquez sur la liste **Status** située près du nom de l'exemption que vous voulez activer ou désactiver, puis cliquez sur **Enabled** ou **Disabled**.

Remarque : pour utiliser une exemption prédéfinie comme une imprimante, changez son statut en Enabled.

3. Cliquez sur **Save**.

3.4 Aperçu de la zone Report

La zone Report contient tous les composants requis pour l'édition de rapports de conformité et de résolution des problèmes. Vous pouvez accéder aux zones suivantes depuis le menu Report :

Zone et action	Description
Compliance reports	
Utiliser des rapports de conformité pour visualiser la conformité des utilisateurs avec les stratégies.	<p>Les rapports de conformité sont composés des rapports Compliance Detail et Compliance Summary.</p> <ul style="list-style-type: none"> ■ Les rapports de conformité contiennent des informations sur les systèmes d'extrémité en conformité avec les stratégies et des chiffres détaillés sur le nombre de systèmes en conformité avec les stratégies pour une période donnée. Utilisez les informations d'évaluation associées aux enregistrements des rapports Compliance Detail pour visualiser des détails sur les évaluations de conformité effectuées sur un système.
Troubleshooting reports	

Zone et action	Description
<p>Utiliser des rapports de résolution des problèmes pour résoudre les problèmes d'accès, de conformité aux stratégies, de quarantaine et les exemptions.</p>	<p>Les rapports de résolution des problèmes sont constitués des rapports Agent Session, Non-Compliance Detail, Agent Enforcer, DHCP Enforcer et DHCP Exemption.</p> <ul style="list-style-type: none"> ■ Le rapport Agent Session indique toutes les sessions d'agent et évaluations qui ont eu lieu sur des systèmes d'extrémité pour une période donnée. ■ Le rapport Non-Compliance Detail affiche des informations sur les systèmes d'extrémité qui ne sont pas en conformité avec les stratégies. ■ Le rapport Agent Enforcer indique l'accès réseau à l'aide de l'application de la quarantaine de l'agent pour une période donnée. ■ Le rapport DHCP Enforcer indique l'accès réseau à l'aide de l'application du protocole DHCP pour une période donnée. ■ Le rapport DHCP Exemption indique les exemptions DHCP pour une période donnée. ■ Les détails d'évaluation sont disponibles dans les rapports Agent Session, Non-Compliance Detail, Agent Enforcer et DHCP Enforcer Troubleshooting. Utilisez les informations d'évaluation associées aux enregistrements du rapport pour visualiser des informations sur les évaluations de conformité effectuées sur un système.
Saved reports	
<p>Utiliser des rapports enregistrés pour facilement régénérer les rapports.</p>	<p>Les rapports enregistrés vous permettent d'enregistrer et de réutiliser des paramètres communs de rapports pour éviter d'avoir à saisir de nouveau les mêmes critères. Toute configuration de rapport peut être enregistrée et réutilisée sous la forme d'un rapport enregistré.</p>
Audits	
<p>Visualiser des audits pour rechercher des mises à jour d'évènements système.</p>	<p>Les audits fournissent une trace d'audit ou un historique des évènements qui ont eu lieu dans le système. Les évènements peuvent inclure des mises à jour aux stratégies courantes, la création de nouveaux modèles d'accès ou des opérations système comme l'ouverture ou la fermeture de comptes sur le NAC Manager.</p>

3.4.1 Impression de rapports

Vous pouvez imprimer un rapport que vous avez exécuté ou un enregistrement de rapport auquel vous accédez.

Procédure

1. Cliquez sur **Report > Compliance or Troubleshooting**.
2. Cliquez sur la liste **Report Type** et sélectionnez le nom du rapport que vous voulez imprimer.

3. 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 Computer Name, tous les noms d'ordinateurs qui commencent par un M s'affichent. De même, si vous tapez M sans le symbole % dans le champ Computer Name, seuls les noms qui s'appellent M s'affichent.

4. Cliquez sur **Run**.
5. Cliquez sur **Print**.

3.4.2 Exécution de rapports de conformité

Utilisez les rapports de conformité pour visualiser les systèmes d'extrémité qui sont en conformité avec les stratégies pendant une période donnée. Les rapports de conformité peuvent être utilisés pour évaluer les tendances dans la conformité des stratégies. Deux types de rapports de conformité sont disponibles :

- **Compliance Detail :** ce rapport contient des informations sur les systèmes d'extrémité en conformité avec les stratégies pour une période donnée, d'après la dernière session d'agent du système. Vous pouvez visualiser les informations d'évaluation dans le rapport Compliance Detail.
- **Compliance Summary :** ce rapport contient des chiffres détaillés sur le nombre de systèmes d'extrémité en conformité avec les stratégies pour une période donnée.

Procédure

1. Cliquez sur **Report > Compliance** .
2. Cliquez sur la liste **Report Type** et sélectionnez **Compliance Detail** ou **Compliance Summary**.
3. 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 Computer Name, tous les noms d'ordinateurs qui commencent par un M s'affichent. De même, si vous tapez M sans le symbole % dans le champ Computer Name, seuls les noms qui s'appellent M s'affichent.

4. Cliquez sur **Run**.

Pour plus d'informations sur les champs des résultats du rapport, reportez-vous au tableau des champs et des descriptions.

Champs et descriptions

Remarque : le rapport Compliance Summary ne contient pas tous les champs ci-dessous. Les numéros dans chaque champ qui apparaissent dans un rapport Compliance Summary représentent le nombre d'instances d'un élément donné.

Champ	Description
Compliance State	Etat de conformité du système d'extrémité, affecté lors de l'évaluation de la conformité. Pour plus d'informations, reportez-vous à la section Détermination de l'état de conformité du système d'extrémité à la page 49. 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.
Policy Name	Nom de la stratégie qui a été évaluée par l'agent.
Policy Version	Version de la stratégie qui a été évaluée par l'agent. Si la version de la stratégie est la plus récente, la valeur Latest apparaît. Remarque : chaque fois que la stratégie est mise à jour, le numéro de version est mis à jour par incrémentation de un.
Computer Name	Nom du système d'extrémité sur lequel l'agent est installé.
Agent ID	Identifiant de l'installation de l'agent ou du système d'extrémité à partir duquel la session est lancée. Remarque : l'identifiant de l'agent est un GUID généré par logiciel qui identifie de manière unique chaque installation d'agent.
Last Assessment Date/Time	Date et heure de la plus récente évaluation de conformité dans l'intervalle temporel utilisé dans le rapport. L'évaluation inclut les opérations qui évaluent et appliquent la stratégie sur le système d'extrémité. La fréquence de l'évaluation est basée sur l'intervalle d'évaluation et d'application défini dans la stratégie. Trois tirets (---) indiquent que la session d'agent a continué au-delà de la durée indiquée dans les options de recherche. Remarque : la date et l'heure proviennent du fuseau horaire du navigateur Web accédant au NAC Manager.
Associated Reports	Icône qui accède aux détails concernant l'évaluation de conformité associée avec cette entrée Compliance Detail. Pour plus d'informations, reportez-vous à la section Visualisation des informations d'évaluation à la page 75.

3.4.3 Exécution du rapport Agent Session

Utilisez le rapport Agent Session pour visualiser toutes les sessions d'agent et évaluations qui ont eu lieu sur des systèmes d'extrémité pour une période donnée. Le rapport Agent Session peut être utilisé pour résoudre les problèmes d'accès réseau ou de conformité aux stratégies. Ce rapport contient des informations sur la session d'agent sur le système d'extrémité, sur les évaluations effectuées sur le système et sur tout changement dans l'état de conformité. Vous

pouvez visualiser les enregistrements Agent Enforcer, les enregistrements DHCP Enforcer ou les détails d'évaluation du rapport Agent Session.

Remarque : dans certains cas, les données en temps réel doivent être fusionnées depuis plusieurs sources, aussi il est possible que les données soient incomplètes.

Procédure

1. Cliquez sur **Report > Troubleshooting**.
2. Cliquez sur la liste **Report Type** et sélectionnez **Agent Session**.
3. 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 Computer Name, tous les noms d'ordinateurs qui commencent par un M s'affichent. De même, si vous tapez M sans le symbole % dans le champ Computer Name, seuls les noms qui s'appellent M s'affichent.

4. Cliquez sur **Run**.

Pour plus d'informations sur les champs des résultats du rapport, reportez-vous au tableau des champs et des descriptions.

Champs et descriptions

Champ	Description
Entrée du rapport Summary	
Computer Name	Nom du système d'extrémité sur lequel l'agent est installé.
Agent ID	Identifiant de l'installation de l'agent ou du système d'extrémité à partir duquel la session est lancée. Remarque : l'identifiant de l'agent est un GUID généré par logiciel qui identifie de manière unique chaque installation d'agent.
MAC Address	Adresses MAC du système d'extrémité sur lequel l'agent est installé. Dans le rapport, chaque adresse MAC est affectée au même NIC que l'adresse IP située à côté.
IP Address	Adresses IP du système d'extrémité sur lequel l'agent est installé. Dans le rapport, chaque adresse IP est affectée au même NIC que l'adresse MAC située à côté. Trois tirets (---) indiquent que le NIC n'a pas d'adresse IP.
Operating System	Système d'exploitation installé sur le système d'extrémité.

Champ	Description
Session Start	Date et heure auxquelles sur un système d'extrémité, l'agent commence sa session avec Sophos NAC. Remarque : la date et l'heure proviennent du fuseau horaire du navigateur Web accédant au NAC Manager.
Session End	Date et heure auxquelles sur un système d'extrémité, l'agent commence sa session avec Sophos NAC. Trois tirets (---) signifient que la session d'agent n'est pas terminée. Remarque : la date et l'heure proviennent du fuseau horaire du navigateur Web accédant au NAC Manager.
Entrée du rapport Detailed	
Assessment Start	Date et heure de la première instance du résultat de l'évaluation de conformité dans l'intervalle temporel utilisé dans le rapport. L'évaluation inclut les opérations qui évaluent et appliquent la stratégie sur le système d'extrémité. La fréquence de l'évaluation est basée sur l'intervalle d'évaluation et d'application défini dans la stratégie. Remarque : la date et l'heure proviennent du fuseau horaire du navigateur Web accédant au NAC Manager.
Assessment End	Date et heure de la dernière instance du résultat de l'évaluation de conformité dans l'intervalle temporel utilisé dans le rapport. L'évaluation inclut les opérations qui évaluent et appliquent la stratégie sur le système d'extrémité. Trois tirets (---) signifient que l'évaluation de conformité n'est pas terminée. Remarque : la date et l'heure proviennent du fuseau horaire du navigateur Web accédant au NAC Manager.
Count	Nombre d'évaluations de conformité qui ont eu lieu sans changement dans les résultats d'évaluation. Ce nombre correspond au nombre de fois que l'agent a effectué l'évaluation de conformité, d'après l'intervalle d'évaluation et d'application défini dans la stratégie.
Compliance State	Etat de conformité du système d'extrémité, affecté lors de l'évaluation de la conformité. Pour plus d'informations, reportez-vous à la section Détermination de l'état de conformité du système d'extrémité à la page 49. 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.
Policy Name	Nom de la stratégie qui a été évaluée par l'agent.

Champ	Description
Policy Version	Version de la stratégie qui a été évaluée par l'agent. Si la version de la stratégie est la plus récente, la valeur Latest apparaît. Remarque : chaque fois que la stratégie est mise à jour, le numéro de version est mis à jour par incrémentation de un.
Associated Reports	Icônes qui permettent d'accéder aux enregistrements Agent Enforcer, DHCP Enforcer ou aux détails concernant l'évaluation de conformité associée à l'entrée de la session d'agent. Une icône apparaît seulement si un enregistrement associé est disponible. Pour plus d'informations, reportez-vous aux sections Exécution du rapport Agent Enforcer à la page 67, Exécution du rapport DHCP Enforcer à la page 69 ou Visualisation des informations d'évaluation à la page 75.

3.4.4 Exécution du rapport Non-Compliance Detail

Utilisez le rapport Non-Compliance Detail pour visualiser les systèmes d'extrémité non conformes ou partiellement conformes aux stratégies pendant une période donnée, d'après la dernière session d'agent d'un système d'extrémité. Le rapport Non-Compliance Detail peut être utilisé pour rapidement identifier les systèmes d'extrémité qui ne sont pas entièrement conformes aux stratégies et les raisons pour lesquelles ils ne le sont pas. Vous pouvez visualiser les informations d'évaluation dans le rapport Non-Compliance Detail.

Remarque : dans certains cas, les données en temps réel doivent être fusionnées depuis plusieurs sources, aussi il est possible que les données soient incomplètes.

Procédure

1. Cliquez sur **Report > Troubleshooting**.
2. Cliquez sur la liste **Report Type** et sélectionnez **Non-Compliance Detail**.
3. 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 Computer Name, tous les noms d'ordinateurs qui commencent par un M s'affichent. De même, si vous tapez M sans le symbole % dans le champ Computer Name, seuls les noms qui s'appellent M s'affichent.

4. Cliquez sur **Run**.

Pour plus d'informations sur les champs des résultats du rapport, reportez-vous au tableau des champs et des descriptions.

Champs et descriptions

Champ	Description
Entrée du rapport Summary	
Computer Name	Nom du système d'extrémité sur lequel l'agent est installé.
Compliance State	Etat de conformité du système d'extrémité, affecté lors de l'évaluation de la conformité. Pour plus d'informations, reportez-vous à la section Détermination de l'état de conformité du système d'extrémité à la page 49. Les états de conformité disponibles sont Partially Compliant (partiellement conforme) et Non-Compliant (non conforme). Trois tirets (---) signifient que l'agent n'a pas signalé d'état de conformité.
Associated Reports	Icône qui permet d'accéder aux informations concernant l'évaluation de conformité associée avec cette entrée Non-Compliance Detail. Pour plus d'informations, reportez-vous à la section Visualisation des informations d'évaluation à la page 75.
Entrée du rapport Detailed	
Profile Name	Nom du profil que l'agent a tenté de détecter sur le système d'extrémité. Le type de profil associé apparaît entre parenthèses.
Capability	Fonctionnalité de profil pour laquelle le système d'extrémité a été trouvé partiellement conforme ou non conforme.
Compliance State	Etat de conformité de la condition signalée seulement si la condition est remplie sur le système d'extrémité. Les états de conformité disponibles sont Partially Compliant (partiellement conforme) et Non-Compliant (non conforme). Trois tirets (---) signifient que l'agent n'a pas signalé d'état de conformité.

3.4.5 Exécution du rapport Agent Enforcer

Utilisez le rapport Agent Enforcer pour visualiser l'accès réseau à l'aide de l'application de la quarantaine de l'agent pour une période donnée. Le rapport Agent Enforcer peut être utilisé pour résoudre les problèmes de quarantaine sur un ou plusieurs systèmes d'extrémité. Ce rapport contient des informations sur l'état de conformité des systèmes d'extrémité, le modèle d'accès associé et la raison pour laquelle un modèle d'accès particulier a été appliqué. Vous pouvez visualiser les informations d'évaluation dans le rapport Agent Enforcer.

Remarque: dans certains cas, les données en temps réel doivent être fusionnées depuis plusieurs sources, aussi il est possible que les données soient incomplètes.

Procédure

1. Cliquez sur **Report > Troubleshooting**.
2. Cliquez sur la liste **Report Type** et sélectionnez **Agent Enforcer**.

- 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 Computer Name, tous les noms d'ordinateurs qui commencent par un M s'affichent. De même, si vous tapez M sans le symbole % dans le champ Computer Name, seuls les noms qui s'appellent M s'affichent.

- Cliquez sur **Run**.

Pour plus d'informations sur les champs des résultats du rapport, reportez-vous au tableau des champs et des descriptions.

Champs et descriptions

Champ	Description
Date/Time	Date et heure de changement de l'état d'application de Agent Enforcer. Remarque : la date et l'heure proviennent du fuseau horaire du navigateur Web accédant au NAC Manager.
Agent ID	Identifiant de l'installation de l'agent ou du système d'extrémité sur lequel le changement de l'état d'application a été signalé. Remarque : l'identifiant de l'agent est un GUID généré par logiciel qui identifie de manière unique chaque installation d'agent.
Computer Name	Nom du système d'extrémité sur lequel l'agent est installé.
Compliance State	Etat de conformité du système d'extrémité, affecté lors de l'évaluation de la conformité. Pour plus d'informations, reportez-vous à la section Détermination de l'état de conformité du système d'extrémité à la page 49. 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 Agent Enforcer associés à l'état de conformité des stratégies déterminent l'accès réseau.
Template Name (Version)	Nom et version du modèle d'accès qui détermine l'action prise par l'Agent Enforcer. Le modèle d'accès utilisé est basé sur la raison. Pour plus d'informations, reportez-vous à la section Création de modèles d'accès Agent Enforcer à la page 50. Les modèles d'accès disponibles incluent les modèles par défaut suivants ainsi que tous les modèles d'accès que vous avez créés : <ul style="list-style-type: none"> ■ Default - Agent and Internet Access Only : modèle d'accès Agent Enforcer utilisé pour autoriser l'accès à tous les produits Sophos et à Internet pour les réseaux internes qui utilisent des adresses IP privées et refuser l'accès à tout autre trafic sortant.

Champ	Description
	<ul style="list-style-type: none"> ■ Default - Agent Permit All : modèle d'accès Agent Enforcer utilisé pour autoriser tout trafic sortant ■ None : paramètre d'accès par défaut autorisant tout trafic sortant dans le cas où les modèles Default - Agent and Internet Access Only et Default - Agent Permit All sont supprimés de la stratégie et si aucun modèle spécifique aux entreprises n'est sélectionné. Le paramètre d'accès None garantit que l'agent peut accéder au serveur NAC.
Reason	<p>Raison pour laquelle un modèle d'accès particulier est affecté par l'Agent 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. Le modèle d'accès Agent Enforcer associé à l'état de conformité de stratégie détermine l'accès réseau. Il apparaît un lien qui permet d'accéder aux informations concernant l'évaluation de conformité associée avec cette entrée Agent Enforcer. ■ No Agent Tray : l'agent n'est pas exécuté sur le système d'extrémité. Ce statut peut être signalé par l'Agent Enforcer si l'utilisateur n'a pas de session ouverte sur Windows ou si l'application Agent de la zone de notification ne fonctionne plus. Le modèle d'accès Agent Enforcer de la stratégie associé à l'état No Agent Tray de l'agent détermine l'accès réseau. ■ Policy Retrieval Error : une stratégie n'a pas pu être récupérée pour le système d'extrémité. Ce statut peut exister si l'agent est incapable de récupérer la stratégie depuis le serveur NAC; ou si l'état de conformité du système d'extrémité est obsolète d'après le champ Agent Policy Update Threshold configuré dans la zone Configure System > Enforcer Settings. ■ Remediate : la stratégie est en mode Remediate. Le modèle d'accès Agent Enforcer associé au mode de stratégie Remediate détermine l'accès réseau. ■ Report Only : la stratégie est en mode Report Only. Le modèle d'accès Agent Enforcer associé au mode de stratégie Report Only détermine l'accès réseau. ■ User Override : l'utilisateur a remplacé la quarantaine de l'agent sur le système d'extrémité. Le modèle d'accès Agent Enforcer de la stratégie associé à l'état User Override Agent de l'agent détermine l'accès réseau.

3.4.6 Exécution du rapport DHCP Enforcer

Utilisez le rapport DHCP Enforcer pour visualiser l'accès réseau à l'aide de l'application du protocole DHCP pour une période donnée. Le rapport DHCP Enforcer peut servir à résoudre les problèmes d'accès au réseau. Ce rapport contient des informations sur l'état de conformité des systèmes d'extrémité, le modèle d'accès associé et la raison pour laquelle un modèle d'accès particulier a été appliqué. Vous pouvez exempter des périphériques et accéder aux détails de l'évaluation depuis le rapport DHCP Enforcer.

Remarque : dans certains cas, les données en temps réel doivent être fusionnées depuis plusieurs sources, aussi il est possible que les données soient incomplètes.

Procédure

1. Cliquez sur **Report > Troubleshooting**.
2. Cliquez sur la liste **Report Type** et sélectionnez **DHCP Enforcer**.
3. 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.

4. Cliquez sur **Run**.

Pour plus d'informations sur les champs des résultats du rapport, reportez-vous au tableau des champs et des descriptions. Pour plus d'informations sur l'exemption des périphériques de ce rapport, reportez-vous à la section [Création d'exemptions à partir de rapports](#) à la page 74.

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 State	Etat de conformité du système d'extrémité, affecté lors de l'évaluation de la conformité. Pour plus d'informations, reportez-vous à la section Détermination de l'état de conformité du système d'extrémité à la page 49. 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.
Template Name (Version)	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. Pour plus d'informations, reportez-vous à la section Création de modèles d'accès DHCP

Champ	Description
	<p>Enforcer à la page 51. 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 NAC Server 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 concernant l'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, les modèles d'accès Maintenance Mode/Enforcer Override aussi désignés dans cette zone déterminent l'accès réseau. ■ Exempted : le système d'extrémité est exempté d'après 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. ■ Remediate : la stratégie est en mode Remediate. Les modèles d'accès DHCP Enforcer associés au mode de stratégie Remediate déterminent l'accès réseau.

Champ	Description
	<ul style="list-style-type: none"> ■ 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 NAC Server 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 ne pouvaient pas 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.
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.

Champ	Description
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.

3.4.7 Exécution du rapport d'exemptions DHCP

Utilisez le rapport d'exemptions DHCP pour visualiser les exemptions DHCP pour une période donnée. Le rapport d'exemptions DHCP peut servir à résoudre les problèmes d'accès au réseau spécifique aux exemptions.

Remarque : dans certains cas, les données en temps réel doivent être fusionnées depuis plusieurs sources, aussi il est possible que les données soient incomplètes.

Procédure

1. Cliquez sur **Report > Troubleshooting**.
2. Cliquez sur la liste **Report Type** et sélectionnez **DHCP Exemption**.
3. 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.

4. Cliquez sur **Run**.

Pour plus d'informations sur les champs des résultats du rapport, reportez-vous au tableau des champs et des descriptions.

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.
Template Name (Version)	Nom du modèle d'accès qui a déterminé l'action prise par le DHCP Enforcer. Pour plus d'informations, reportez-vous à la section Création de modèles d'accès DHCP Enforcer à la page 51.

Champ	Description
Exemption Condition Name	Nom de l'exemption et critères d'exemption.
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.
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	
Returned User Class	Classe utilisateur DHCP, le cas échéant, qui est envoyée au serveur DHCP depuis le client DHCP.
Vendor Class	Classe du fournisseur du client DHCP.
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.

3.4.8 Création d'exemptions à partir de rapports

Vous pouvez créer des exemptions à partir d'un rapport DHCP Enforcer pour les systèmes signalés lors d'une application de DHCP.

Les exemptions apparaissent dans le rapport DHCP Enforcer en fonction de la raison "Exempted". Si vous exemptez des systèmes du rapport, ils apparaîtront comme non exemptés dans le rapport jusqu'à ce que le système tente de se connecter à nouveau au réseau. Pour plus d'informations sur les champs et sur les descriptions du rapport DHCP, reportez-vous à la section [Exécution du rapport DHCP Enforcer](#) à la page 69.

Procédure

1. Cliquez sur **Report > Troubleshooting**.
2. Cliquez sur la liste **Report Type** et sélectionnez **DHCP Enforcer**.
3. 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.

4. Cliquez sur **Run**.
5. Cliquez sur les cases à cocher situées près des systèmes que vous voulez exempter, puis cliquez sur **Exempt**.
6. Confirmez la liste des systèmes que vous voulez exempter, sélectionnez le modèle d'accès que vous voulez appliquer aux exemptions, et cliquez sur **OK**.
Pour administrer ou appliquer les modèles d'accès supplémentaires aux exemptions que vous avez créées, allez dans la zone **Enforce > Exemptions** . Pour plus d'informations, reportez-vous à la section [Création d'exemptions de critères DHCP](#) à la page 58.

3.4.9 Visualisation des informations d'évaluation

Utilisez les informations d'évaluation pour visualiser les informations sur les évaluations de conformité effectuées sur un système d'extrémité.

Vous pouvez visualiser les informations d'évaluation dans les rapports suivants : Compliance Detail, Agent Session, Non-Compliance Detail, Agent Enforcer ou DHCP Enforcer. Les informations d'évaluation qui apparaissent sont associées à l'entrée du rapport depuis lequel vous les avez visualisées. Les informations d'évaluation affichent les conditions des profils qui ont été testés sur le système d'extrémité, les résultats des conditions testées, l'état de conformité affecté basé sur l'évaluation, et toutes les actions prises sur le système d'extrémité.

Procédure

1. Cliquez sur **Report > Compliance or Troubleshooting** .
2. Cliquez sur la liste **Report Type** et sélectionnez **Compliance Detail, Agent Session, Non-Compliance Detail, Agent Enforcer, ou DHCP Enforcer**.
3. 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 Computer Name, tous les noms d'ordinateurs qui commencent par un M s'affichent. De même, si vous tapez M sans le symbole % dans le champ Computer Name, seuls les noms qui s'appellent M s'affichent.

4. Cliquez sur **Run**.
5. Dans le rapport Agent Session seulement, cliquez sur le **signe plus** situé près d'un rapport récapitulatif pour visualiser l'entrée du rapport détaillée associée.
6. Cliquez sur l'icône **Assessment Details** ou sur le lien **Assessment**, en fonction du rapport.

Pour plus d'informations sur les champs des résultats du rapport, reportez-vous au tableau des champs et des descriptions.

Champs et descriptions

Champ	Description
Informations d'évaluation du type de profil	
Profile Type	Type de profil que l'agent a tenté de détecter sur le système d'extrémité.
Compliance State	Etat de conformité du type de profil. Cet état de conformité est composé des profils évalués sur le système d'extrémité conjointement au comportement de stratégie qui est Require, Best ou All. Pour plus d'informations, reportez-vous à la raison de sélection ci-dessous. 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.
Informations d'évaluation du profil	
Profile Name	Nom du profil que l'agent a tenté de détecter sur le système d'extrémité.
Selected	Spécifie si le profil a été utilisé pour déterminer l'état de conformité du type de profil. Si la valeur est True, ce profil a été utilisé. Si la valeur est False, ce profil n'a pas été utilisé ; à la place, un autre profil a été utilisé pour déterminer l'état de conformité. Pour plus d'informations sur la manière dont les profils sont évalués sur le système d'extrémité, reportez-vous au champ Selection Reason ci-dessous.
Selection Reason	Indique pourquoi le profil a été utilisé ou non pour déterminer l'état de conformité du type de profil. Ceci dépend du comportement de stratégie qui détermine comment les profils sont évalués par rapport aux profils du même type sur le système d'extrémité. Les valeurs disponibles sont : <ul style="list-style-type: none"> ■ Required (Best) : indique si le profil de système d'exploitation requis est trouvé sur le système d'extrémité. Le profil du système d'exploitation est requis et est évalué comme meilleur profil. ■ Best : indique si le meilleur profil est trouvé sur le système d'extrémité. Chaque profil d'un type particulier dans une stratégie est évalué sur le système d'extrémité, la meilleure correspondance est déterminée, et seules les actions garanties associées au profil correspondant le mieux sont prises. Le comportement Best utilise le profil le plus conforme sur le système d'extrémité pour déterminer l'état de conformité du type de profil dans la stratégie. Sauf indication contraire, les profils d'application sont évalués de cette manière. ■ Best (No Match) : indique si aucun profil dans une évaluation Best n'est trouvé sur le système d'extrémité. Si aucun des profils évalués n'est installé sur le système d'extrémité, alors l'état de conformité de la condition Else du profil ayant la priorité la plus élevée est utilisé pour déterminer l'état de conformité et les actions du type de profil dans la stratégie. Si l'un des systèmes d'exploitation n'est pas installé sur le système d'extrémité, alors l'état de conformité de la condition Else du profil du système d'exploitation à la priorité la plus élevée est utilisé pour déterminer l'état de conformité et les actions du type de profil du système d'exploitation, et aucun profil supplémentaire n'est évalué pour cette stratégie.

Champ	Description
	<ul style="list-style-type: none"> ■ All : indique si tous les profils sont évalués sur le système d'extrémité. Tous les profils d'un type particulier dans une stratégie sont évalués sur le système d'extrémité, et les actions garanties associées à tous les profils sont prises. Le comportement All utilise le profil le moins conforme sur le système d'extrémité pour déterminer l'état de conformité du type de profil dans la stratégie. Les profils d'applications que vous voulez empêcher sur le système d'extrémité peuvent être évalués de cette manière.
Detected	Indique si l'élément de profil (système d'exploitation ou application) a été détecté sur le système d'extrémité. Si la valeur est True, l'élément de profil a été détecté. Si la valeur est False, l'élément de profil n'a pas été détecté.
Compliance State	Etat de conformité de profil. Cet état de conformité est composé des conditions de profil évaluées sur le système d'extrémité. Toutes les conditions de profil sont évaluées pour déterminer l'état de conformité des profils. 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.
Informations d'évaluation des fonctionnalités de profils	
Profil Condition	Affiche une condition qui était configurée dans le profil par rapport à l'élément en sortie qui était détectée sur le système d'extrémité. Le résultat peut être une version, un nombre ou une date, ou tout autre élément qui délimite la condition sur le système d'extrémité. Trois tirets (---) indiquent que la condition n'a pas de délimiteur.
Result	Résultat de l'évaluation de la condition. Si le résultat est True, la condition définie dans le profil a été remplie sur le système d'extrémité. Si le résultat est False, la condition définie dans le profil n'a pas été remplie sur le système d'extrémité.
Compliance State	Etat de conformité de la condition signalée seulement si la condition est remplie sur le système d'extrémité. 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.
Action Type	Type d'action corrective qui était effectuée sur le système d'extrémité. Des actions sont affichées ou effectuées sur le système d'extrémité seulement si la condition à laquelle l'action est associée est remplie. Les types d'actions disponibles sont : <ul style="list-style-type: none"> ■ Message : affiche un message sur le système d'extrémité. Cette action est disponible pour toutes les fonctionnalités. ■ Enable : sur le système d'extrémité, active la protection en temps réel pour les applications antivirus ou antispyware, active le pare-feu pour les applications Firewall ou active les mises à jour pour les applications du gestionnaire de correctifs. Cette action est disponible pour la fonctionnalité d'application Real-Time Protection ou Enabled.

Champ	Description
	<ul style="list-style-type: none"> ■ Update : met à jour le fichier signature sur le système d'extrémité. Cette action est disponible pour la fonctionnalité d'application Signature Date ou Signature Grace Period. ■ Scan : lance un contrôle sur le système d'extrémité. Cette action est disponible pour la fonctionnalité d'application Scan Date ou Scan Grace Period. ■ Apply : applique la stratégie de la Sophos Enterprise Console pour l'application Sophos Anti-Virus sur le système d'extrémité. Cette action est disponible pour la fonction d'application des stratégies de la SEC.
Action Value	Message affiché pour l'utilisateur sur le système d'extrémité. Un message apparaît sur le système d'extrémité seulement si la condition est remplie. Aucun autre type d'action n'affiche de valeur d'action.

3.4.10 Enregistrement de rapports

Vous pouvez enregistrer un rapport en personnalisant les critères de recherche et de tri d'un rapport existant afin qu'ils répondent à vos besoins. Les critères sont enregistrés lorsque le rapport est enregistré.

Procédure

1. Cliquez sur **Report > Compliance or Troubleshooting**.
2. Cliquez sur la liste **Report Type** et sélectionnez le nom du rapport que vous voulez enregistrer.
3. 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 Computer Name, tous les noms d'ordinateurs qui commencent par un M s'affichent. De même, si vous tapez M sans le symbole % dans le champ Computer Name, seuls les noms qui s'appellent M s'affichent.

4. Cliquez sur **Run**.
5. Cliquez sur **Save**.
6. Dans la boîte de dialogue, tapez le nom du rapport dans le champ **Report Name**.
7. Cliquez sur **Save**.

3.4.11 Exécution de rapports enregistrés

Saved reports vous permet d'enregistrer et de réutiliser des paramètres communs de rapports pour éviter d'avoir à saisir de nouveau les mêmes critères. Vous pouvez aussi mettre à jour les paramètres des rapports enregistrés sans avoir à enregistrer de nouveaux rapports.

Procédure

1. Cliquez sur **Report > Saved**.
2. Cliquez sur la liste **Saved Report** et sélectionnez le nom du rapport enregistré que vous voulez exécuter.
3. 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 Computer Name, tous les noms d'ordinateurs qui commencent par un M s'affichent. De même, si vous tapez M sans le symbole % dans le champ Computer Name, seuls les noms qui s'appellent M s'affichent.

4. Cliquez sur **Run**.

3.4.12 Suppression de rapports enregistrés

La suppression des rapports enregistrés les supprime complètement du logiciel.

Procédure

1. Cliquez sur **Report > Saved**.
2. Cliquez sur la liste **Saved Report** et sélectionnez le nom du rapport enregistré que vous voulez supprimer.
3. Cliquez sur **Delete**.
4. Dans le message, cliquez sur **OK** pour confirmer la suppression.

3.4.13 Visualisation des audits

La zone Audits fournit une trace d'audit ou un historique des événements qui ont eu lieu dans le système. Les événements peuvent inclure des mises à jour aux stratégies courantes, la création de nouveaux modèles d'accès ou des opérations système comme l'ouverture ou la fermeture de comptes sur le NAC Manager.

Procédure

1. Cliquez sur **Report > Audits**.
2. Saisissez ou sélectionnez les options de recherche appropriées dans les champs appropriés et cliquez sur **Search**.

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 Item Name, tous les noms d'éléments qui commencent par un M s'affichent.

3. Effectuez l'une des opérations suivantes :
 - Pour trier la liste, cliquez sur l'en-tête de colonne approprié.
 - Pour visualiser les informations relatives à un événement, cliquez sur le lien **Details**.

3.5 Aperçu de la zone Configure System

La zone Configure System contient tous les composants nécessaires pour configurer les composants du système NAC Manager. Vous pouvez accéder aux zones suivantes depuis le menu Configure System :

Zone et action	Description
Accounts	
Créer des comptes système.	Les comptes autorisent plusieurs niveaux d'accès au NAC Manager. Un administrateur système peut créer un nom et définir des rôles de sécurité pour les comptes système. Le nom et le mot de passe du compte sont utilisés pour ouvrir une session sur le NAC Manager. Les rôles de sécurité déterminent le niveau des droits pour chaque compte.
Désactiver ou activer des comptes.	Les comptes peuvent être désactivés ou activés par un administrateur système. La désactivation d'un compte empêche l'utilisateur de ce compte d'ouvrir une session sur le NAC Manager pour visualiser les informations système ou exécuter toutes les fonctions administratives. L'activation d'un compte permet à son utilisateur d'ouvrir une session sur le NAC Manager et de réaliser des opérations administratives affectées par le rôle de sécurité du compte.
Paramètres Enforcer	
Spécifier des paramètres pour Enforcer.	Les paramètres Enforcer spécifient des détails d'application pour les types Agent Enforcer et DHCP Enforcer. L'Agent Enforcer est utilisé pour l'application de la quarantaine de type client. Le DHCP Enforcer est utilisé avec les mises en place du protocole DHCP de Sophos NAC.
Paramètres du serveur	
Créer des serveurs DHCP Enforcer.	Utilisez cette zone pour définir les serveurs DHCP Enforcer à utiliser avec les mises en place DHCP de Sophos NAC.
Créer des serveurs d'agent temporaire.	Utilisez cette zone pour définir des serveurs qui hébergent l'agent temporaire afin que le DHCP Enforcer puisse accéder à ceux-ci.
Mettre à jour les paramètres du serveur proxy NAC.	Lors d'une installation NAC, vous pouvez configurer NAC pour qu'il utilise un serveur proxy afin d'accéder à Internet. L'accès à Internet est nécessaire pour télécharger les plus récentes informations de détection pour les applications de sécurité. Utilisez cette zone pour mettre à jour les paramètres de proxy et pour optionnellement mettre à jour les adresses IP NAC Server.
Informations du compte de téléchargement	
Mettre à jour les détails du compte de téléchargement.	Le nom utilisateur et le mot de passe du compte de téléchargement sont utilisés par NAC pour télécharger les plus récentes informations de détection pour les applications de sécurité.

3.5.1 Création de comptes

La zone Accounts permet à l'administrateur système de créer un nom et de définir des rôles de sécurité pour les comptes système. Le nom et le mot de passe du compte sont utilisés pour ouvrir une session sur le NAC Manager. Les rôles de sécurité déterminent le niveau des droits pour chaque compte.

Procédure

1. Cliquez sur **Configure System > Accounts** . Puis cliquez sur **Create Account** dans la section inférieure de la page.
2. Saisissez le nom du compte.
3. De manière facultative, sélectionnez la case à cocher **Disable Account** pour créer un compte désactivé.
4. Saisissez et confirmez le mot de passe du compte.

Remarque : si vous mettez à jour le mot de passe d'un compte existant, vous devez aussi taper votre mot de passe de compte. Ce champ garantit que seuls les administrateurs système avec des comptes valides peuvent mettre à jour les mots de passe du compte.

5. Sélectionnez un des rôles de sécurité suivants :

- **System Administrator** : détient les droits d'accès complets à toutes les zones du NAC Manager. L'administrateur système peut créer, mettre à jour ou supprimer des comptes.
- **Administrator** : détient les droits d'accès complets aux zones Manage, Enforce et Report du NAC Manager. Détient les droits d'accès en lecture seule à la zone Configure System du NAC Manager. Le rôle de sécurité Administrator n'a pas les droits de visualisation ou de gestion des comptes.
- **Help Desk** : détient les droits d'accès complets aux zones Report du NAC Manager. Détient les droits d'accès en lecture seule aux zones Manage, Enforce et Configure System du NAC Manager. Le rôle de sécurité Help Desk n'a pas les droits de visualisation ou de gestion des comptes.
- **Guest** : détient les droits d'accès en lecture seule à toutes les zones du NAC Manager. Le rôle de sécurité Guest n'a pas les droits de visualisation ou de gestion des comptes.

Remarque : tous les rôles de sécurité permettent d'accéder aux fonctionnalités de navigation pour utilitaires, y compris leurs propres mots de passe, aides en ligne et informations sur le NAC Manager.

6. Cliquez sur **Save**.

3.5.2 Désactivation ou activation des comptes

Les comptes sont automatiquement activés lors de leur création, à moins que vous ne les désactiviez explicitement. La désactivation d'un compte empêche l'utilisateur de ce compte d'ouvrir une session sur le NAC Manager pour visualiser les informations système ou exécuter toutes les fonctions administratives.

Procédure

1. Cliquez sur **Configure System > Accounts** .

2. Cliquez sur l'icône **Enabled Account** ou **Disabled Account** située près du nom du compte que vous voulez désactiver ou activer. L'icône de l'état en cours s'affiche.

3.5.3 Spécification des paramètres Enforcer

La page Enforcer Settings vous permet de configurer les paramètres qui spécifient comment l'application est effectuée pour le , le DHCP Enforcer ou l'Agent Enforcer. Le DHCP Enforcer est utilisé avec les mises en place du protocole DHCP de Sophos NAC. L'Agent Enforcer est utilisé pour l'application de la quarantaine de type client.

Procédure

1. Cliquez sur **Configure System > Enforcer Settings** .
2. Si vous utiliser l'Agent Enforcer, spécifiez le paramètre seuil suivant. Si vous utilisez aussi le le DHCP Enforcer, passez à l'étape suivante ; sinon, passez à l'étape 7 :
 - **Agent Policy Update Threshold** : identifie le temps nécessaire (en minutes, heures ou jours) à l'agent de quarantaine pour récupérer la stratégie avant que le système d'extrémité soit placé en quarantaine. Si le seuil est dépassé, le système d'extrémité est placé en quarantaine et une nouvelle récupération de stratégie est requise. En attendant, l'accès réseau est déterminé par le modèle d'accès Agent Enforcer associé à l'état d'accès Policy Retrieval Error de la stratégie. Ce seuil est utilisé pour l'application de l'agent. La valeur par défaut est 8 heures. La valeur minimum est 1.
Important : Le paramètre du seuil de mise à jour des stratégies doit toujours être **supérieure** à l'intervalle de rafraîchissement des stratégies spécifié pour chaque stratégie ; autrement, chaque fois que le seuil de mise à jour des stratégies est atteint, l'accès réseau est déterminé par l'état d'accès Policy Retrieval Error dans la stratégie et le système d'extrémité est placé dans la quarantaine.
3. Spécifiez les paramètres de seuil suivants pour le le DHCP Enforcer :
 - **DHCP Policy Update Threshold** : identifie le temps (en minutes, heures ou jours) entre le moment où la stratégie est récupérée par l'agent et le moment où elle expire. S'il expire, une nouvelle récupération de stratégie est requis. En attendant, l'accès réseau est déterminé par le modèle d'accès DHCP Enforcer associé à l'état d'accès Policy Retrieval Error de la stratégie. Ce seuil est utilisé pour la mise en application de DHCP. S'il est défini sur 0, ce seuil est désactivé. La valeur par défaut est 5 heures.
Remarque : il est recommandé que ce seuil soit au moins de 10 minutes **supérieur** à l'intervalle de rafraîchissement de stratégies spécifié pour chaque stratégie.
 - **Dissolvable Agent Compliance Threshold** : identifie le temps (en minutes, heures ou jours) après lequel l'enregistrement de conformité d'un système d'extrémité est considéré comme valide par le DHCP Enforcer. Si le seuil est dépassé, le système d'extrémité non administré est considéré comme inconnu tant qu'une évaluation de conformité n'est pas exécutée sur le système. En attendant, l'accès réseau est déterminé par les modèles d'accès Unknown Endpoint spécifiés à l'étape 5. S'il est défini sur 0, ce seuil est désactivé. La valeur par défaut est 12 heures.

4. Sélectionnez les paramètres appropriés du serveur DHCP Enforcer :
 - **Report Exemptions** : case à cocher qui détermine si le le DHCP Enforcer doit signaler les exemptions. Si elle est sélectionnée, les systèmes d'extrémité définis comme des exemptions sont exemptés et signalés, puis apparaissent sur les rapports d' ou d'exemption DHCP. Si elle n'est pas sélectionnée, les systèmes d'extrémité définis comme exemptions sont uniquement exemptés. Pour plus d'informations, reportez-vous aux sections [Exécution du rapport d'exemptions DHCP](#) à la page 73.
 - **Exempt DHCP Reservations** : case à cocher qui détermine si les systèmes d'extrémité réservés configurés sur le serveur DHCP sont exemptés. Si elle est sélectionnée, les systèmes d'extrémité réservés sont exemptés à partir de l'application. Toutefois, si un agent est installé sur un système d'extrémité, le modèles d'accès associé à l'état d'accès du système d'extrémité sera affectée en tant que système d'extrémité réservé quelle que soit sa désignation.
 - **Override DHCP Enforcer**: case à cocher qui détermine si le le DHCP Enforcer effectue l'application d'après les stratégies de sécurité définies. Si elle est sélectionnée, l'application est désactivée et l'accès réseau est déterminé par les modèles d'accès Maintenance Mode/Enforcer Override spécifiés à l'étape 5 ; par contre, ces modèles d'accès sont utilisés seulement si le système d'extrémité n'est pas une exemption définie.
5. Pour ajouter ou modifier les modèles d'accès pour un état d'accès particulier, cliquez sur **Select** sous les modèles d'accès DHCP Enforcer, sélectionnez les cases à cocher à côté des modèles d'accès et à côté des états d'accès auxquels s'appliquent les modèles et cliquez sur **OK**. Vous pouvez aussi laisser le modèle d'accès par défaut ou le supprimer. Les états d'accès suivants sont disponibles :
 - **Unknown Endpoint** : détermine l'accès au réseau lorsqu'il n'existe aucun enregistrement de conformité. Les systèmes d'extrémité inconnus ne sont pas administrés par la Sophos Enterprise Console, sont non exemptés et soit n'ont pas exécuté l'agent temporaire soit ont dépassé le seuil de conformité de l'agent temporaire (Dissolvable Agent Compliance Threshold) défini à l'étape 2. Vous pouvez sélectionner des modèles d'accès à utiliser pour les systèmes d'extrémité lorsque le serveur DHCP est en mode Report Only ou Enforce pour les systèmes d'extrémité inconnus. Pour plus d'informations, reportez-vous à la section [Création de serveurs DHCP Enforcer](#) à la page 84.
 - **Maintenance Mode/Enforcer Override** : détermine l'accès réseau lorsque le système est en mode de maintenance ou lorsque la mise en application sur le DHCP Enforcer a été désactivé via la case à cocher Override DHCP Enforcer.
 - **Default** : détermine l'accès réseau si si un modèle d'accès associé est introuvable.
6. Si nécessaire, utilisez les flèches pour attribuer une priorité aux modèles d'accès.

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**.

3.5.4 Création de serveurs DHCP Enforcer

Les serveurs DHCP Enforcer sont utilisés pour l'application pour les implémentations DHCP de Sophos NAC. Pour plus d'informations sur la configuration de l'application de DHCP, reportez-vous au *Guide de configuration DHCP de Sophos NAC*.

Procédure

1. Cliquez sur **Configure System > Server Settings**. Cliquez sur **Create Alert** dans la section inférieure gauche de la page.
2. Saisissez un nom et une description de serveur.
3. Cliquez sur la liste **Server Type** et sélectionnez **DHCP Agent Server**.
4. Saisissez le nom d'hôte ou les adresses IP du serveur, et cliquez sur **Add**. Si vous saisissez un nom d'hôte, le NAC Manager tente de le résoudre aux adresses IP correctes. Si c'est pas possible, vous devez saisir les adresses IP correctes.
5. Saisissez et confirmez la clé partagée du serveur.

Important : la clé partagée doit correspondre à ce que vous avez saisi lors de l'installation de DHCP Enforcer sur le serveur.

6. Sélectionnez le mode des systèmes d'extrémité inconnus pour désigner si le serveur DHCP Enforcer doit signaler l'accès des systèmes d'extrémité inconnus ou l'appliquer.

L'option **Report Only** vous permet de déployer les serveurs DHCP Enforcer sans affecter l'accès réseau. Une fois que vous avez créé des exemptions DHCP et que vos utilisateurs invités utilisent l'agent temporaire, vous pouvez changer le mode des systèmes d'extrémité inconnus en **Enforce** pour activer l'application de DHCP.

Les systèmes d'extrémité ne sont pas administrés par la Sophos Enterprise Console, non exemptés et soit n'ont pas exécuté l'agent temporaire soit ont dépassé le seuil de conformité de l'agent temporaire.

Remarque : d'après le mode des systèmes d'extrémité, les modèles d'accès Unknown Endpoint désignés dans la zone **Configure System > Enforcer Settings** déterminent l'accès réseau. Pour plus d'informations, reportez-vous à la section [Spécification des paramètres Enforcer](#) à la page 82.

7. Cliquez sur **Save**.

3.5.5 Création de serveurs d'agent temporaire

Les serveurs d'agent temporaire sont utilisés pour héberger l'agent temporaire. Une fois défini, le DHCP Enforcer peut autoriser l'accès à ces serveurs.

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.

Procédure

1. Cliquez sur **Configure System > Server Settings**. Cliquez sur **Create Alert** dans la section inférieure gauche de la page.
2. Saisissez un nom et une description de serveur.
3. Cliquez sur la liste **Server Type** et sélectionnez **Dissolvable Agent Server**.

4. Saisissez le nom d'hôte ou les adresses IP du serveur, et cliquez sur **Add**. Si vous saisissez un nom d'hôte, le NAC Manager tente de le résoudre aux adresses IP correctes. Si c'est pas possible, vous devez saisir les adresses IP correctes.
5. Cliquez sur **Save**.

3.5.6 Mise à jour des paramètres du serveur proxy NAC

Lors d'une installation NAC, vous pouvez configurer NAC pour qu'il utilise un serveur proxy afin d'accéder à Internet. L'accès à Internet est nécessaire pour télécharger les plus récentes informations de détection pour les applications de sécurité. Utilisez cette zone pour mettre à jour les paramètres de proxy et pour optionnellement mettre à jour les adresses IP NAC Server.

Procédure

1. Cliquez sur **Configure System > Server Settings**.
2. Cliquez sur le nom du NAC Server pour mettre à jour ses paramètres de serveur.
3. Optionnellement, saisissez le nom d'hôte ou les adresses IP du serveur, et cliquez sur **Add**. Si vous saisissez un nom d'hôte, le NAC Manager tente de le résoudre aux adresses IP correctes. Si c'est pas possible, vous devez saisir les adresses IP correctes.

Important : comme les adresses IP définissent la connexion entre les agents et le NAC Server, assurez-vous qu'elles sont correctes. Si elles ne sont pas correctes, les agents ne pourront pas communiquer avec le NAC Server.

4. Cliquez sur la liste **Proxy Settings** pour sélectionner l'option de serveur proxy appropriée :
 - **No Proxy :** le NAC Server n'utilise pas de serveur proxy pour accéder à Internet.
 - **Use Proxy :** le NAC Server utilise un serveur proxy pour accéder à Internet. Les paramètres du serveur proxy sont initialement définis dans l'installation NAC et peuvent être mis à jour comme vous le souhaitez.
 - **Use SEC Proxy Settings :** le NAC Server utilise, pour l'accès à Internet, les paramètres proxy définis dans la Sophos Enterprise Console. Cette option est disponible seulement si la Sophos Enterprise Console est installée sur le même serveur que NAC. Si cette option est sélectionnée, les paramètres du serveur proxy doivent être mis à jour dans la Sophos Enterprise Console.
5. Mettez à jour les paramètres du serveur proxy.

Remarque : il est obligatoire d'indiquer l'adresse et le port du serveur proxy. Le nom utilisateur, le mot de passe et le mot de passe de confirmation sont nécessaires seulement lors de l'utilisation d'un proxy authentifié.

6. Cliquez sur **Save**.

3.5.7 Mise à jour des informations du compte de téléchargement

Le nom utilisateur et le mot de passe du compte de téléchargement sont utilisés par NAC pour télécharger les plus récentes informations de détection pour les applications de sécurité. Le nom utilisateur et le mot de passe saisis au cours de l'installation de NAC doivent correspondre à ceux qui vous ont été fournis par Sophos. En cas de saisie incorrecte au cours de l'installation de NAC, vous avez la possibilité de les corriger sur la page des détails du compte de téléchargement.

Procédure

1. Cliquez sur **Configure System > Download Account Details** .
2. Mettez à jour le nom utilisateur et/ou le mot de passe.
Si vous mettez à jour un mot de passe existant, vous devez confirmer le nouveau mot de passe.
3. Cliquez sur **Save**.

4 Outils NAC

4.1 Outil de chargement

Installé avec Sophos NAC , l'outil de chargement permet à l'administrateur d'importer des applications et des types d'application nouvelles et mises à jour dans leurs bases de données bases de données NAC.

4.1.1 Importation d'applications

Il existe deux moyens d'importer des applications à l'aide de l'outil de chargement. Vous pouvez utiliser le fichier EXE de définitions d'applications qui appelle l'outil de chargement et importe automatiquement les applications ou bien une ligne de commandes pour importer les applications à l'aide d'un fichier import.xml. Sophos conseille d'utiliser le fichier EXE de définitions d'applications car il appelle automatiquement l'outil de chargement et rend l'importation d'applications et de types d'applications plus simple qu'avec une ligne de commandes. Sophos met le fichier EXE de définitions d'applications à la disposition de toutes les entreprises.

4.1.2 Importation d'applications à l'aide du fichier EXE de définitions d'applications

1. Téléchargez depuis le site Web de Sophos le fichier EXE de définitions d'applications.
2. Copiez le fichier EXE téléchargé de définitions d'applications sur le serveur NAC de Sophos.
3. Cliquez deux fois sur le fichier EXE pour importer les applications et les types d'applications mises à jour.

Remarque : le fichier EXE appelle l'outil de chargement et installe automatiquement les applications et types d'applications mis à jour.

4.1.3 Importation manuelle d'applications à l'aide d'un fichier import.xml

1. Faites-vous envoyer un fichier import.xml mis à jour par un représentant Sophos.
2. Copiez le fichier import.xml sur le serveur NAC de Sophos.

- Depuis une invite de commandes, exécutez l'outil de chargement pour importer les nouvelles définitions en saisissant : **C:\Program Files\Sophos\NAC\Loader\Loader.exe C:\import.xml.**

Remarque :

- Les commandes ne sont pas sensibles aux majuscules. Les paramètres de commandes utilisent les barres obliques avant / puis le nom du paramètre suivi de manière facultative de deux-points et d'une valeur de paramètre. Par exemple, /ID:id. Les valeurs de paramètre peuvent contenir des barres obliques arrière \ et des espaces ; en revanche, toute valeur de paramètre DOS qui contient un espace nécessite des guillemets, par exemple : "C:\temp\my key.xml".
- L'outil de chargement suppose que vous avez ouvert une session dans Windows à l'aide d'un compte Windows disposant des droits d'accès SQL. Si vous n'avez pas ouvert de session dans Windows avec un compte disposant des droits d'accès SQL, vous pouvez exécuter l'outil de chargement du type suivant pour un compte SQL : Chargeur /L:SQL /ID:ID /PW:PW /F:import.xml (où ID et PW sont l'identification et le mot de passe d'un compte SQL valide).
- En plus des commandes DOS détaillées dans la section suivante, vous pouvez visualiser des options supplémentaires dans l'outil de chargement en tapant : loader /?.
- Par défaut, toutes les erreurs qui apparaissent sont aussi écrites dans le journal des événements.

4.1.4 Commandes DOS de l'outil de chargement

Le tableau suivant énumère les commandes DOS qui peuvent être utilisées avec l'outil de chargement. Ces commandes peuvent être utilisées pour charger des applications dans les bases de données, exporter des applications depuis les bases de données ou valider un fichier import.xml avant d'importer. Pour utiliser ces commandes, transférez-les dans l'outil de chargement sous la forme de paramètres de lignes de commandes. Par exemple, la première commande du tableau est exécutée en tapant ceci dans la ligne de commande : **Loader /F:import.xml.**

Commandes	Descriptions
/F:import.xml	Charge toute application ou tout type d'application depuis le fichier XML spécifié.
/F:imp*.xml	Charge les applications ou les types d'applications depuis plusieurs fichiers.

4.2 Outil de journalisation

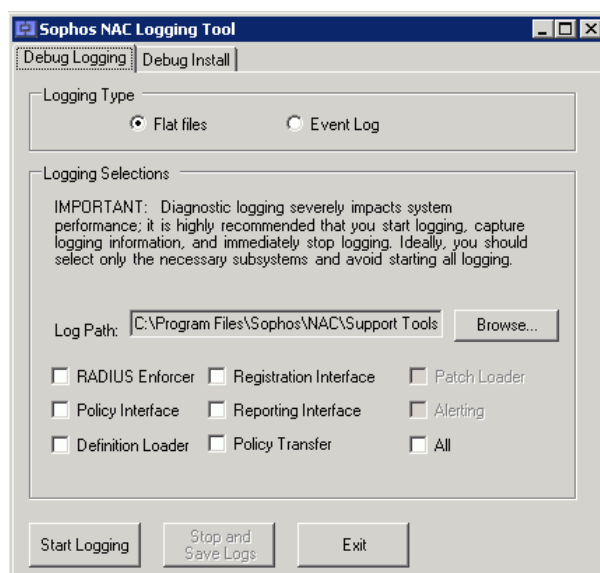
L'outil de journalisation vous permet d'activer l'installation et la journalisation du sous-système afin de procéder à une résolution assistée des problèmes. L'onglet Debug Logging vous permet d'identifier la méthode de journalisation et l'emplacement des fichiers mais aussi de démarrer

et arrêter manuellement la journalisation pour des sous-systèmes sélectionnés. L'onglet Debug Install vous permet d'identifier le fichier d'installation à diagnostiquer et l'emplacement du fichier de journalisation. La journalisation est paramétrée à un niveau maximum ; les informations enregistrées dépendent du type de journalisation effectuée.

Important : Sophos vous conseille d'utiliser cet outil afin de résoudre les problèmes uniquement, de préférence à l'aide d'instructions d'un représentant Sophos et de ne pas laisser la journalisation activée car elle peut sévèrement affecter les performances du système.

4.2.1 Journalisation du sous-système du NAC Server de Sophos

1. Recherchez l'outil de journalisation sur le NAC Server de Sophos. L'emplacement par défaut de cet outil est C:\Program Files\Sophos\NAC\Support Tools.
2. Cliquez deux fois sur le fichier **LoggingUtil.exe**.



3. Sur l'onglet **Debug Logging**, sélectionnez le type et les options de journalisation appropriés, puis cliquez sur **Start Logging**.

Pour plus d'informations sur chaque champ, reportez-vous à la section [Champs et descriptions de l'onglet Debug Logging](#) à la page 90.

Remarque : une fois que vous cliquez sur le bouton **Start Logging**, vous ne pouvez pas sélectionner ou désélectionner de sous-systèmes supplémentaires. Vous devez arrêter la journalisation, changer vos options de journalisation et recommencer.

4. Effectuez les tâches appropriées sur le NAC Server de Sophos pour lequel vous voulez capturer les informations de journalisation.

- Une fois les tâches appropriées exécutées, cliquez sur **Stop and Save Logs** pour enregistrer les informations de journalisation dans les fichiers journaux appropriés.

Les fichiers sont enregistrés sur le chemin que vous avez indiqué dans le champ **Log Path**. Le chemin par défaut du journal est : C:\Program Files\Sophos\NAC\Support Tools\Logs. Pour plus d'informations sur le type de fichiers journaux et sur ce qu'ils contiennent, reportez-vous à la section [Fichiers journaux](#) à la page 92.

Remarque : **Stop and Save Logs** est grisé lorsque la journalisation est désactivée.

4.2.2 Champs et descriptions de l'onglet Debug Logging

La journalisation de diagnostics affecte sévèrement les performances du système. Il est fortement recommandé de commencer la journalisation, d'enregistrer les informations de journalisation et d'arrêter immédiatement la journalisation. Idéalement, sélectionnez seulement les sous-systèmes nécessaires et évitez de commencer toute journalisation.

Remarque : la journalisation est paramétrée à un niveau maximum et englobe les messages d'erreur journal, d'avertissement, d'information, de suivi complet et de pile des appels.

Champs	Descriptions
Type de journalisation	
Flat File	Paramètre la journalisation pour générer des fichiers plats. Un fichier plat est créé pour chaque sous-système que vous sélectionnez.
Event Log	Paramètre la journalisation pour l'ajout des informations du sous-système dans le journal des événements (Event Log) sur le serveur NAC Server.
Options de journalisation	
Log Path	Paramètre le chemin où les fichiers journaux générés sont placés.
RADIUS Enforcer	Paramètre la journalisation du NAC Server. Cette option est seulement utilisée pour l'application du protocole DHCP. Le NAC Server est le composant logiciel qui vérifie les résultats de conformité de l'agent au nom du DHCP Enforcer.
Policy Interface	Paramètre la journalisation du service d'interface de stratégie. L'interface de stratégie est le composant côté serveur qui récupère la stratégie pour l'agent et vérifie la validité de la demande d'agent.
Definition Loader	Paramètre la journalisation du chargeur de définitions. Le chargeur de définitions est l'outil côté serveur responsable de la détection des applications de sécurité, de la détection de la version des signatures, de la version du moteur de contrôle, de la date du dernier contrôle, de la protection en temps réel, de la détection activée et des actions correctives automatiques.

Champs	Descriptions
Registration Interface	<p>Paramètre la journalisation du service d'interface d'enregistrement.</p> <p>L'interface d'enregistrement est le composant côté serveur qui fournit les services d'enregistrement à l'agent. L'interface d'enregistrement procède à l'authentification de l'utilisateur à chaque fois que l'agent s'enregistre pour la première fois ou à chaque fois qu'il se réenregistre.</p>
Reporting Interface	<p>Paramètre la journalisation du service d'interface de rapports.</p> <p>L'interface de rapports est le composant côté serveur qui accepte les données de rapports de l'agent. L'interface de rapports vérifie également la validité de la demande de l'agent.</p>
Policy Transfer	<p>Paramètre la journalisation du service de transfert de stratégie.</p> <p>Le transfert de stratégie est le composant côté serveur qui transfère les données du stock de données de stratégie vers le stock de données de rapport afin que les informations de stratégie mises à jour soient répliquées dans les rapports.</p>
All	Paramètre la journalisation de tous les sous-systèmes NAC.

4.2.3 Journalisation de l'installation du NAC Server de Sophos

Cet outil doit seulement être utilisé pour résoudre les problèmes d'installation. Tentez tout d'abord d'installer le NAC de Sophos. Si vous recevez des erreurs lors de l'installation initiale, vous pouvez utiliser cet outil pour capturer les informations de journalisation concernant l'installation.

1. Recherchez l'outil de journalisation sur le NAC Server de Sophos. L'emplacement par défaut de cet outil est C:\Program Files\Sophos\NAC\Support Tools.
2. Cliquez deux fois sur le fichier **LoggingUtil.exe**.
3. Cliquez sur l'onglet **Debug Install**.
4. Sélectionnez le chemin approprié du fichier d'installation que vous voulez dépanner où vous souhaitez que les fichiers journaux soient placés, puis cliquez sur **Start Install**.

Pour plus d'informations sur chaque champ, reportez-vous à la section [Champs et descriptions de l'onglet Debug Install](#) à la page 91.

Remarque : une fois l'installation terminée, les fichiers sont enregistrés dans le chemin que vous avez indiqué dans le champ **Log Path**. Le chemin par défaut du journal est : C:\Program Files\Sophos\NAC\Support Tools\Logs. Pour plus d'informations sur le type de fichiers journaux et sur ce qu'ils contiennent, reportez-vous à la section [Fichiers journaux](#) à la page 92.

4.2.4 Champs et descriptions de l'onglet Debug Install

La journalisation est paramétré à un niveau maximum déterminé par Microsoft® Windows® Installer.

Champs	Descriptions
Install File Path	Sélectionne le chemin vers le fichier d'installation.
Log Path	Paramètre le chemin où sont placés les fichiers journaux générés pendant l'installation.

4.2.5 Fichiers journaux

Le chemin par défaut du fichier journal est : C:\Program Files\Sophos\NAC\Support Tools\Logs sur le serveur Sophos NAC Server. Ce chemin peut être changé avant de générer les fichiers journaux. Chaque fois qu'une journalisation est lancée, tous les fichiers existants dans le chemin spécifié portant le même nom sont remplacés.

Champs	Descriptions
AppEvent.xml	Fichier contenant les événements d'applications exportés depuis le journal des événements présent sur le NAC Server de Sophos. Lorsque l'option Event Log est sélectionnée comme type de journalisation, les informations du journal des sous-systèmes sont incluses dans ce fichier.
SystemEvent.xml	Fichier contenant les événements système exportés depuis le journal des événements présent sur le NAC Server de Sophos. Les informations du service d'authentification Internet (IAS) sont incluses dans ce fichier journal.
Systeminfo.nfo	Fichier contenant les informations relatives au matériel et au système d'exploitation sur le NAC Server de Sophos.
UserInfo.txt	Fichier contenant les informations relatives au compte, telles que le nom et les droits de ce compte, pour les utilisateurs ayant ouvert une session sur le NAC Server de Sophos ainsi que les informations relatives au compte sous lequel les sous-systèmes installés fonctionnent.
<Sous-système>.xml	Fichier contenant les informations de journalisation des sous-systèmes de Sophos NAC. Lorsque l'option Flat File est sélectionnée comme type de journalisation, les sous-systèmes du NAC Server sont tous enregistrés dans un fichier plat distinct, comme ci-dessous : <ul style="list-style-type: none"> ■ Interface de stratégie : PolicyInterfaceLog.xml ■ Chargeur de définitions : CurrentDefsLoaderLog.xml ■ Interface d'enregistrement : RegistrationInterfaceLog.xml ■ Interface de rapports : ReportingInterfaceLog.xml ■ Transfert de stratégie : PolicyTransferLog.xml

Champs	Descriptions
Install<dateheure>.log	Fichier de sortie de Microsoft Windows Installer contenant les informations sur l'installation. Ce fichier est généré seulement pour les fonctions de l'onglet Debug Install.
SophosNACLogs.zip	Fichier contenant tous les fichiers journaux de l'onglet Debug Logging.
InstallLogs.zip	Fichier contenant tous les fichiers journaux de l'onglet Debug Install.

4.3 Outil mode de maintenance

Utilisez l'outil mode de maintenance lorsque vous effectuez la maintenance de la base de données et/ou rencontrez des problèmes de réseau ou de base de données. Cet outil est un outil par lignes de commande utilisé pour activer ou désactiver le mode de maintenance. L'outil interrompt les services Sophos NAC appropriés afin que vous puissiez effectuer la maintenance requise. Dès que vous êtes prêt à retourner en mode production, arrêtez l'outil mode de maintenance. L'outil redémarre automatiquement les services qui ont été arrêtés.

Lorsque Sophos NAC est en mode de maintenance, l'Compliance Agent Sophos reconnaît le mode et fonctionne sans erreur, interruption ou indication du mode de maintenance aux utilisateurs. L'agent enregistre toutes les informations d'évaluation et de rapport localement jusqu'à ce que le logiciel revienne en mode production. Aussi, l'agent continue l'évaluation par rapport à la stratégie en mémoire cache, et si la quarantaine de l'agent est utilisée, le système d'extrémité peut quand même être placé en quarantaine d'après les règles de la stratégie en mémoire cache. De plus, si vous utilisez l'application du protocole DHCP, les modèles d'accès DHCP Enforcer et les exemptions sont placés en mémoire cache et toutes les requêtes DHCP font l'objet d'une réponse à l'aide des modèles d'accès et des exemptions placés en mémoire cache.

Remarque : il n'est pas nécessaire d'utiliser cet outil lors d'une mise à niveau de NAC.

L'installation de NAC met le NAC Server en mode de maintenance et met le serveur hors du mode de maintenance lorsque l'installation se termine.

4.3.1 Exécution de l'outil mode de maintenance

1. Depuis une invite de commandes sur le serveur NAC de Sophos, allez dans le répertoire C:\Program Files\Sophos\NAC\Support Tools.
2. Saisissez **MaintMode.exe /start**. Cette commande place Sophos NAC en mode de maintenance.
3. Tapez **MaintMode.exe /stop**. Cette commande remet Sophos NAC en mode production.

4.3.2 Commandes de l'outil mode de maintenance

Les commandes ne sont pas sensibles aux majuscules. Les paramètres des commandes utilisent les barres obliques avant / puis le nom du paramètre. Toute valeur de paramètre DOS contenant un espace nécessite des guillemets.

Commandes	Descriptions
MaintMode.exe /start.	Démarre l'outil mode de maintenance
MaintMode.exe /stop.	Arrête l'outil mode de maintenance
MaintMode.exe /E:silent	Indique qu'aucun message n'est écrit dans la boîte de dialogue de la ligne de commande. Les messages d'erreur sont toujours écrits dans le journal des événements.
MaintMode.exe /E:error	Indique que seules les erreurs sont écrites dans la console. Les messages d'erreur sont toujours écrits dans le journal des événements.
MaintMode.exe /E:warn	Indique que les erreurs et les avertissements sont écrits dans la console. Les messages d'erreur sont toujours écrits dans le journal des événements.
MaintMode.exe /E:info	Indique que les erreurs, les avertissements et les messages d'information sont écrits dans la console. Les messages d'erreur sont toujours écrits dans le journal des événements.
MaintMode.exe /?	Affiche la fenêtre d'aide de l'outil mode de maintenance.

5 Glossaire

Voici le glossaire Sophos NAC.

Agent de quarantaine	L'agent de quarantaine évalue les systèmes d'extrémité afin de déterminer s'ils sont en conformité avec la stratégie NAC. Ces évaluations sont effectuées avant l'autorisation d'accès au réseau puis régulièrement suite à l'autorisation d'accès au réseau. L'agent nécessite peu ou pas d'intervention de la part de l'utilisateur. L'agent de quarantaine dispose d'une fonction de quarantaine qui garantit son application et qui limite l'accès des systèmes d'extrémité à des zones spécifiques du réseau lorsque ceux-ci ne sont pas en conformité avec la stratégie NAC. product="sophosnacadvanced"
Agent Enforcer	L'Agent Enforcer est le type d'application protégeant le réseau avec une évaluation de type client et une application de quarantaine sur les systèmes d'extrémité exécutant l'agent de quarantaine.
Agent temporaire	L'agent temporaire évalue les systèmes d'extrémité pour déterminer s'ils sont en conformité avec la stratégie NAC avant d'autoriser l'accès au réseau. L'agent temporaire doit s'exécuter depuis un navigateur. L'agent temporaire s'adresse aux utilisateurs, comme les sous-traitants ou les invités, qui n'ont pas installé ou ne peuvent pas installer l'agent sur un système d'extrémité mais qui doivent quand même accéder à des ressources réseau spécifiques. L'agent temporaire est utilisé avec l'application du protocole DHCP.
Application	Les applications sont des applications logicielles prises en charge par Sophos NAC. Les applications définissent les fonctionnalités, les conditions associées, les états de conformité et les actions possibles. Les applications sont liées à un type d'application, qui détermine comment l'application est évaluée lorsque le profil de l'application est ajouté à la stratégie.
Assistant de configuration DHCP	L'assistant de configuration de DHCP vous aide à identifier les serveurs proxy, de correction, d'agent temporaire et DHCP Enforcer à utiliser avec les mises en place DHCP de Sophos NAC.
Audits	Les audits sont une trace ou un historique des événements qui ont eu lieu dans le système. Les événements peuvent inclure des mises à jour aux stratégies courantes, la création de nouveaux modèles d'accès ou des opérations système comme l'ouverture ou la fermeture de comptes sur le NAC Manager.
Comportement de stratégie	Le comportement de stratégie détermine comment les profils sont évalués par rapport aux profils du même type sur le système d'extrémité. Les options sont Required, Best et All. Pour plus d'informations, reportez-vous aux définitions du

	comportement de stratégie Required, du comportement de stratégie Best et du comportement de stratégie All.
Comportement de stratégie All	Tous les profils d'un type particulier dans une stratégie sont évalués sur le système d'extrémité, et les actions garanties associées à tous les profils sont prises. Le comportement All utilise le profil le moins conforme sur le système d'extrémité pour déterminer l'état de conformité du type de profil dans la stratégie. Les profils d'applications que vous voulez empêcher sur le système d'extrémité peuvent être évalués de cette manière.
Comportement de stratégie Best	Chaque profil d'un type particulier dans une stratégie est évalué sur le système d'extrémité, la meilleure correspondance est déterminée, et seules les actions garanties associées au profil correspondant le mieux sont prises. Le comportement Best utilise le profil le plus conforme sur le système d'extrémité pour déterminer l'état de conformité du type de profil dans la stratégie. Sauf indication contraire, les profils d'application sont évalués de cette manière. Si aucun des profils évalués n'est installé sur le système d'extrémité, alors l'état de conformité de la condition Else du profil ayant la priorité la plus élevée est utilisé pour déterminer l'état de conformité et les actions du type de profil dans la stratégie.
Comportement de stratégie Required	Un profil de système d'exploitation est requis et il est évalué comme meilleur profil. Si l'un des systèmes d'exploitation n'est pas installé sur le système d'extrémité, alors l'état de conformité de la condition Else du profil du système d'exploitation à la priorité la plus élevée est utilisé pour déterminer l'état de conformité et les actions du type de profil du système d'exploitation, et aucun profil supplémentaire n'est évalué pour cette stratégie.
Compte	Un compte est constitué d'un nom d'ouverture de session et d'un rôle de sécurité pour un utilisateur. Le nom et le mot de passe du compte sont utilisés pour ouvrir une session sur le NAC Manager. Les rôles de sécurité déterminent le niveau des droits pour chaque compte.
Condition	Les conditions sont des déclarations utilisées lors de l'évaluation pour déterminer l'état de conformité associé et les actions à prendre sur le système d'extrémité.
DHCP Enforcer	Le DHCP Enforcer est le type d'application qui protège le réseau pour les mises en place DHCP de Sophos NAC.
Enforcer Settings	Les paramètres Enforcer spécifient des informations d'application pour les types d'application DHCP Enforcer et Agent Enforcer.
Etat d'accès	Les états d'accès correspondent à tout état auquel un modèle d'accès peut être appliqué, déterminant ainsi l'accès réseau.

Les modèles d'accès Agent Enforcer peuvent être appliqués aux états d'accès dans les stratégies. Les modèles d'accès DHCP Enforcer peuvent être appliqués aux états d'accès dans les stratégies, les exemptions et les paramètres Enforcer.

Etat de conformité L'état de conformité est déterminé par l'évaluation des résultats de détection sur le système d'extrémité par rapport aux conditions définies du profil. L'état de conformité est ensuite mappé sur les modèles d'accès appropriés de la stratégie pour déterminer l'accès réseau effectivement accordé au système d'extrémité. Un état de conformité peut être conforme, partiellement conforme ou non conforme.

Exemption Les exemptions identifient selon divers critères les systèmes d'extrémité dont la conformité n'a pas à être évaluée lors de la connexion au réseau. Les exemptions incluent les postes d'extrémité qui soit sont incapables d'exécuter l'agent, tels que les postes utilisant des systèmes d'exploitation autres que Windows soit ne nécessitent pas d'évaluation de la conformité comme les serveurs, routeurs ou imprimantes. En outre, pour effectuer un déploiement échelonné dans toute l'entreprise, vous pouvez exempter des systèmes d'extrémité ou des réseaux sur lesquels vous ne souhaitez pas encore appliquer quoi que ce soit.

Fonctionnalité Les fonctionnalités sont les fonctions d'une application pouvant être testées dans le cadre de l'évaluation de la conformité. Les fonctionnalités contiennent des règles utilisées pour l'évaluation, qui sont constituées de conditions, d'états de conformité, de messages et d'actions correctives.

Message Message d'information ou d'erreur affiché sur le système d'extrémité lors d'une évaluation de conformité. Des messages apparaissent sur le système d'extrémité seulement si la condition à laquelle le message est associée est remplie. Des messages sont disponibles pour toutes les fonctionnalités.

Mode de maintenance/Désactivation Enforcer Etat d'accès défini dans la zone **Configure System > Enforcer Settings** area qui détermine l'accès réseau lorsque le système est en mode de maintenance ou le DHCP Enforcer a été désactivé.

Mode de stratégie 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.

Mode de stratégie Remediate Le mode de stratégie Remediate spécifie que les systèmes d'extrémité sont évalués par rapport à la stratégie affectée et

	<p>les informations de rapport sont générées dans le NAC Manager. Les messages apparaissent, les actions correctives sont effectuées ; en revanche, aucune action d'application n'est prise.</p>
Mode de stratégie Report Only	<p>Le mode de stratégie Report Only 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. Aucun message n'apparaît, aucune action corrective n'est effectuée et aucune action d'application n'est prise.</p>
Modèles d'accès	<p>Les modèles d'accès déterminent l'accès réseau lorsqu'ils sont associés avec des états d'accès dans les stratégies, exemptions et paramètres Enforcer (en fonction du type d'application).</p>
Action corrective	<p>L'action exécutée sur le système d'extrémité lors d'une évaluation de la conformité pour mettre le système d'extrémité en conformité avec la stratégie. Les actions correctives ne sont pas disponibles pour toutes les applications ou fonctionnalités d'application.</p>
Modèles de configuration d'agent	<p>Les modèles de configuration d'agent définissent les paramètres facultatifs qui commandent la façon dont l'agent de quarantaine fonctionne sur les systèmes d'extrémité.</p>
No Agent Tray	<p>Etat d'accès défini dans la stratégie qui détermine l'accès réseau lorsque l'agent ne fonctionne pas sur le système d'extrémité. Ce statut peut être signalé par l'Agent Enforcer si l'utilisateur n'a pas de session ouverte sur Windows ou si l'application Agent de la zone de notification ne fonctionne plus.</p>
Par défaut	<p>Etat d'accès défini dans la zone Configure System > Enforcer Settings qui détermine l'accès réseau si un modèle d'accès associé est introuvable.</p>
Paramètres d'agent	<p>Les paramètres d'agent définissent les fonctionnalités de l'agent lorsque ce dernier fonctionne sur le système d'extrémité. Vous pouvez spécifier des paramètres d'agent lorsque vous créez des modèles de configuration d'agent.</p>
Policy Retrieval Error (DHCP)	<p>Etat d'accès défini dans la stratégie qui détermine l'accès réseau lorsque l'état de conformité du système est obsolète d'après le champ DHCP Policy Update Threshold configuré dans la zone Configure System > Enforcer Settings .</p>
Policy Retrieval Error (Agent)	<p>Etat d'accès défini dans la stratégie qui détermine l'accès réseau lorsqu'une stratégie n'a pas pu être récupérée pour le système d'extrémité. Cet état peut exister si l'agent n'est pas en mesure de récupérer la stratégie du serveur Sophos NAC ; ou si l'état de conformité du système d'extrémité n'est pas à jour d'après le champ Agent Policy Update Threshold configuré dans la zone Configure System > Enforcer Settings .</p>

Profil	Les profils vous permettent de définir les éléments que vous souhaitez voir évalués sur le système d'extrémité, comme les systèmes d'exploitation et les applications. Les profils définissent des conditions, des états de conformité, des messages et des actions correctives. Une fois créés, les profils peuvent être organisés et classés par ordre de priorité dans les stratégies.
Règle de détection	Une règle de détection spécifie les valeurs de registre, les processus ou les fichiers qui seront évalués sur le système d'extrémité afin de déterminer si une application est installée, en cours d'exécution ou si elle a une version ou une valeur spécifique.
Ressource réseau	Les ressources réseau sont des applications ou des périphériques nécessaires pour la correction des systèmes d'extrémité ou ceux dont l'accès par les systèmes d'extrémité doit être refusé. Les ressources réseau peuvent être ajoutées soit aux modèles d'accès de l'Agent Enforcer soit à ceux du DHCP Enforcer.
Rôle de sécurité	Les rôles de sécurité déterminent le niveau de droits pour chaque compte NAC Manager et sont affectés lorsque le compte est créé.
Session d'agent	Une session d'agent est le temps pendant lequel l'agent est actif sur le système d'extrémité et accède à Sophos NAC.
Stratégie	Les stratégies contrôlent l'accès aux ressources réseau de l'entreprise d'après les évaluations des profils sur le système d'extrémité. Les stratégies gèrent la configuration qui détermine l'état de conformité du système d'extrémité, les messages qui apparaissent, les actions correctives qui sont exécutées et les actions d'application qui sont prises.
Système d'extrémité administré	Un système d'extrémité administré est un système administré avec la Sophos Enterprise Console et sur lequel le Sophos Compliance Agent est installé. Un système d'extrémité administré utilise l'agent de quarantaine à évaluer pour la conformité et avoir l'accès réseau.
Système d'extrémité non administré	Un système d'extrémité non administré est un système non administré par la Sophos Enterprise Console qui se trouve à l'extérieur de l'entreprise. Un système d'extrémité non administré utilise l'agent temporaire à évaluer pour la conformité et avoir l'accès réseau.
Système d'extrémité	Un système d'extrémité est une machine tentant de se connecter au réseau. Un système d'extrémité peut exécuter l'agent, être exempté et sans agent ou inconnu.
Système inconnu	Etat d'accès défini dans la zone Configurer System > Enforcer Settings qui détermine l'accès réseau lorsqu'aucun

	<p>enregistrement de conformité existe. Les systèmes d'extrémité ne sont pas administrés par la Sophos Enterprise Console, non exemptés et soit n'ont pas exécuté l'agent temporaire soit ont dépassé le seuil de conformité de l'agent temporaire. Vous pouvez sélectionner des modèles d'accès à utiliser pour les systèmes d'extrémité inconnus lorsque le serveur DHCP est en mode de système d'extrémité inconnu Report Only ou Enforce.</p>
Type d'application	<p>Les types d'application classifient les applications et établissent des comportements de stratégie par défaut pour toutes les applications associées au type d'application.</p>
Type de profil	<p>Les types de profils classent les profils par catégories. Les profils sont placés dans des stratégies et évalués les uns par rapport aux autres sur les systèmes d'extrémité en fonction du type et de son comportement de stratégie associé.</p>
User Override	<p>Etat d'accès défini dans la stratégie qui détermine l'accès réseau lorsque l'utilisateur a annulé la quarantaine de l'agent sur le système d'extrémité. Si l'utilisateur annule l'état de la quarantaine, ce dernier est désactivé.</p>
Stratégie Managed	<p>La stratégie prédéfinie Managed est utilisée pour les systèmes d'extrémité qui sont administrés avec la Sophos Enterprise Console et sur lesquels un 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.</p>
Stratégie par défaut	<p>La stratégie par défaut prédéfinie est utilisée si un système d'extrémité est pourvu de l'agent et si 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.</p>
Stratégie Unmanaged	<p>La stratégie Unmanaged prédéfinie est 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 Unmanaged.</p>

6 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

7 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.

Index

A

actions correctives 16, 40, 77
activation
 comptes 81
 exemptions 60
adresse MAC 58, 74
affectation de modèles d'accès 31, 58, 59, 83
Agent configuration templates 27
 création 33
 enregistrement comme nouveau 24
 suppression 25
 verrouillage ou déverrouillage 25
 visualisation des paramètres d'agent pour 33
 visualisation ou recherche 24
Agent Enforcer 31, 50, 82
ajout
 éléments aux profils 36, 38
 profils aux stratégies 30
annulation de la quarantaine 8
aperçu, système 21, 27, 49, 60, 80
applications 24, 27
assistant de configuration de DHCP 49
Assistant de configuration DHCP 54
astuces
 applications 27
 profils 27, 35
 stratégies 27
audits 61, 79

B

bon usage
 modèle d'accès 17
 NAC Manager général 4
 politique 6
 profil 10

C

classe d'éditeur 58
classe utilisateur 51, 58
comportement de stratégie 30, 76
comptes 80
 création 81
 désactivation ou activation 81

comptes (*suite*)
 informations du compte de téléchargement 86
 suppression 25
 visualisation ou recherche 24
conditions 13, 37, 38, 40, 41, 77
configuration
 application du protocole DHCP 54
 de l'agent 29, 33
création
 Agent configuration templates 33
 comptes 81
 exemptions 58, 59
 exemptions à partir de rapports 74
 modèles d'accès 50, 51
 profils 35, 36, 38
 ressources réseau 20, 56
 serveurs DHCP Enforcer 84
 serveurs web d'agent temporaire 84

D

définitions des termes 95
déploiement de Network Access Control 4
désactivation
 comptes 81
 exemptions 60
détermination de l'état de conformité 49
déverrouillage d'éléments 25
DHCP Enforcer 31, 51, 58, 59, 82

E

éléments de liste 24
enregistrement comme nouveau 6, 24
état de conformité du système d'extrémité 49
états d'accès 31, 83
états de conformité 13, 19, 31, 37, 38, 40, 49, 50, 51, 62, 64, 66, 67, 69, 75, 77
étendues IP 51, 59
événements système 79
exécution de rapports 62, 64, 66, 67, 69, 73, 75, 79
exemptions 50
 création 58, 59
 création à partir de rapports 74
 désactivation ou activation 60
 édition de rapports 73, 83
 enregistrement comme nouveau 24
 suppression 25
 verrouillage ou déverrouillage 25

exemptions (*suite*)

visualisation ou recherche 24

F

fonctionnalités 12, 39, 41, 77

fonctionnalités de Sophos Anti-Virus 41

G

glossaire 95

I

icônes

comptes 22

états de conformité des modèles 22

exemptions 23

fonctions communes 22

profils d'applications 23

profils et stratégies 23

rapports 24

impression de rapports 61

informations d'évaluation 75

informations du compte de téléchargement 80, 86

M

messages 15, 37, 38, 40, 77

mise à jour

informations du compte de téléchargement 86

paramètres du serveur proxy NAC 85

stratégies 28

mode de stratégie 7, 29, 31

mode de stratégie Enforce 32

mode de stratégie Remediate 31

mode de stratégie Report Only 31

modèles d'accès 49

bon usage 17

création 50, 51

enregistrement comme nouveau 24

suppression 25

test pour une application exacte 5

vérification dans la stratégie 9

verrouillage ou déverrouillage 25

visualisation ou recherche 24

modèles d'accès prédéfinis 18

N

NAC Manager 21

enregistrement d'éléments comme nouveaux 24

icônes 21

suppression d'éléments 25

utilisation des fonctions par clic droit 26

verrouillage ou déverrouillage d'éléments 25

visualisation ou recherche d'éléments de liste 24

O

options de menu 21, 27, 49, 60, 80

outil de chargement 87

Outil de chargement

commandes DOS 88

importation d'applications 87

outil de journalisation 88

Outil de journalisation

fichiers journaux 92

journalisation de l'installation NAC 91

journalisation du serveur NAC 89

outil mode de maintenance 93

Outil mode de maintenance

commandes 94

exécution de l'outil 93

outils

outil de chargement 87

outil de journalisation 88

outil mode de maintenance 93

P

page d'accueil 21

Paramètres d'agent

dans les modèles de configuration d'agent 33

dans les stratégies 29

paramètres de location DHCP 51

paramètres du serveur 80

paramètres du serveur proxy 85

paramètres du serveur proxy NAC 85

Paramètres Enforcer 80, 82

profils 27, 76

bon usage 10

Bon usage sur les fonctionnalités 12

création 35, 36, 38

enregistrement comme nouveau 24

profils (*suite*)

- instructions 35
- suppression 25
- utilisation des prédéfinis Windows Update 36
- verrouillage ou déverrouillage 25
- visualisation des fonctionnalités d'applications et des conditions pour 41
- visualisation ou recherche 24

profils d'applications 38

profils de systèmes d'exploitation 36

profils prédéfinis 11, 36

profils Windows Update 27, 36

proxy authentifié 85

R

rapport Agent Enforcer 67

rapport Agent Session 64

rapport d'exemptions DHCP 73

rapport DHCP Enforcer 69, 74

rapport Non-Compliance Detail 66

rapports 60

enregistrement 78, 79

impression 61

informations d'évaluation 75

rapport Agent Enforcer 67

rapport Agent Session 64

rapport d'exemptions DHCP 73

rapport DHCP Enforcer 69, 74

rapport Non-Compliance Detail 66

rapports de conformité 62

suppression des enregistrés 79

rapports de conformité 62

rapports détaillés 62

rapports enregistrés 61

enregistrement 78

exécution 79

suppression 79

rapports récapitulatifs 62

recherche d'éléments de liste 24

ressources réseau 49, 50, 51

création 20, 56

enregistrement comme nouveau 24

suppression (personnalisée seulement) 25

verrouillage ou déverrouillage (personnalisé seulement) 25

visualisation ou recherche 24

ressources réseau de ports/protocoles 56

ressources réseau exécutables 56

rôles de sécurité 81

S

serveurs

Agent temporaire 84

DHCP Enforcer 84

serveur proxy NAC 85

serveurs DHCP Enforcer 84

serveurs DNS 51

serveurs web d'agent temporaire 84

Sophos Enterprise Console 28, 41

Spécification des paramètres Enforcer 82

stratégies 27

bon usage 6

mise à jour 28

utilisation de prédéfinies 28

verrouillage ou déverrouillage 25

visualisation des modes de stratégie et des états d'accès pour 31

visualisation ou recherche 24

stratégies prédéfinies 28

support technique 101

suppression d'éléments 25, 79

systèmes d'extrémité administrés 28, 36

systèmes d'extrémité non administrés 28, 36

T

types d'application 27, 31, 50, 51, 58, 82

types de profils 30, 36, 38, 76

U

utilisation

profils Windows Update prédéfinis 36

stratégies prédéfinies 28

utilisation des fonctions par clic droit 26

V

verrouillage d'éléments 6, 25

visualisation

audits 79

éléments de liste 24

fonctionnalités d'applications et conditions 41

informations d'évaluation 75

modes de stratégie et états d'accès 31

Paramètres d'agent 33

visualisation de la page d'accueil 21