

SOPHOS

Sophos NAC Advanced Guide de bon usage

Version du produit : 3.2

Date du document : mars 2011



Table des matières

1	À propos de ce document.....	3
2	Bon usage général.....	4
3	Bon usage des stratégies.....	9
4	Bon usage des profils.....	14
5	Bon usage concernant les applications.....	23
6	Bon usage des modèles d'accès.....	30
7	Bon usage concernant l'enregistrement.....	35
8	Annexe : cas de figure de mise en application.....	41
9	Support technique.....	49
10	Mentions légales.....	50

1 À propos de ce document

Ce document décrit le bon usage en matière de déploiement et de configuration de Sophos NAC Advanced à l'aide du Compliance Manager. Ce document est organisé de la même façon que les menus du Compliance Manager.

1.1 À qui s'adresse ce document ?

Ce document s'adresse aux généralistes en informatique travaillant au sein de petites et moyennes entreprises. Ce document peut également intéresser les spécialistes de l'informatique travaillant au sein d'entreprises disposant de plus de 25 000 systèmes d'extrémité. Si vous avez plus de 1000 systèmes d'extrémité, nous vous recommandons d'utiliser les Sophos Professional Services. Nos consultants Professional Services travaillent conjointement avec votre équipe de sécurité informatique pour mettre au point et mettre en place un plan de déploiement de vos logiciels.

2 Bon usage général

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

2.1 Test et déploiement de Sophos NAC Advanced

Avant de déployer Sophos NAC Advanced, testez minutieusement vos stratégies, profils, applications et modèles d'accès.

Processus	Étapes
Déterminer les profils des entreprises, la messagerie, les stratégies et l'application.	<ol style="list-style-type: none"> 1. Détermination des systèmes d'exploitation, des correctifs et des applications qui nécessitent le contrôle d'accès réseau. 2. Détermination de la messagerie et des actions d'actualisation de ces systèmes d'exploitation, correctifs et applications. 3. Détermination de la mise en application nécessaire et des modèles d'accès.
<p>Utiliser le Compliance Manager pour créer des profils, des modèles d'accès, une stratégie et des groupes prêts à l'emploi en production. Utiliser le mode de stratégie Report Only pour évaluer la conformité de l'entreprise.</p> <p>Passer en revue les rapports du Compliance Manager pour déterminer l'état de conformité actuel de l'entreprise.</p>	<ol style="list-style-type: none"> 1. Création de profils prêts à l'emploi en production ou mise à jour de ceux qui sont préconfigurés par les logiciels afin qu'ils soient prêts pour la production. Remarque : les profils prêts à l'emploi en production doivent contenir les systèmes d'exploitation, les correctifs et les applications ainsi que la messagerie et les actions d'actualisation nécessaires. 2. Création de modèles d'accès prêts à l'emploi en production. 3. Création d'une stratégie, ajout des profils et des modèles d'accès prêts à l'emploi en production et sélection du mode de stratégie Report Only. 4. Création de groupes et association de tous les groupes avec la stratégie. 5. Utilisation des rapports du Compliance Manager pour déterminer l'état de conformité actuel de l'entreprise. Remarque : ce processus permet d'avoir un aperçu réaliste de la conformité des utilisateurs vis-à-vis de la stratégie .
Mettre en place l'actualisation sur un groupe test pour vérifier que la messagerie et les actions d'actualisation sont correctes pour vos utilisateurs.	<ol style="list-style-type: none"> 1. Ouverture de la stratégie existante et utilisation du bouton Save As New pour créer une stratégie d'actualisation. 2. Changement du mode de stratégie en Remediate. 3. Création d'un groupe test et association de la stratégie au groupe test.

Processus	Étapes
	4. Vérification avec le groupe test que la messagerie et les actions d'actualisation sont appropriées.
Mettre en place la stratégie d'actualisation pour tous les utilisateurs.	<ol style="list-style-type: none"> 1. Utilisation du Compliance Manager pour appliquer la stratégie d'actualisation à tous les groupes. 2. Utilisation des rapports du Compliance Manager pour déterminer l'état de conformité actuel de l'entreprise. <p>Remarque : avec le temps, les ordinateurs d'extrémité non conformes et partiellement conformes doivent être actualisés pour améliorer l'état de conformité global.</p>
Mettre en place l'application sur un groupe test pour vérifier que les actions d'accès et la messagerie sont corrects pour vos utilisateurs.	<ol style="list-style-type: none"> 1. Ouverture de la stratégie d'actualisation et utilisation du bouton Save As New pour créer une stratégie d'application. 2. Changement du mode de stratégie en Enforce. 3. Association de la stratégie avec le groupe test. 4. Vérification avec le groupe test que la messagerie, l'actualisation et les actions d'application sont appropriées.
<p>Mettre en place l'application pour tous les utilisateurs.</p> <p>Remarque : vous pouvez créer plusieurs stratégies pour des groupes spécifiques. Il est préférable d'avoir plusieurs stratégies pour des groupes qui exécutent différentes applications et différents systèmes d'exploitation.</p>	<ol style="list-style-type: none"> 1. Utilisation du Compliance Manager pour appliquer la stratégie de mise en application à tous les groupes. 2. Utilisation des rapports du Compliance Manager pour déterminer l'état de conformité actuel de l'entreprise. <p>Remarque : avec le temps, les ordinateurs d'extrémité non conformes doivent être actualisés ou l'accès au réseau sera refusé à leurs utilisateurs.</p>

2.1.1 Utilisation d'un groupe test

Bon usage	Description
<p>Utiliser un groupe test.</p> <p>Si le groupe est associé à plusieurs groupes de sécurité Active Directory ou Windows NT, le premier groupe de sécurité auquel le groupe correspond est utilisé. Avant de tester des stratégies avec</p>	<p>Vérifiez que le groupe test assure la couverture autour des applications antivirus et des fichiers signatures, des applications de pare-feu personnelles, des applications antispyware, des correctifs et des systèmes d'exploitation dont votre entreprise a besoin.</p> <p>Lorsque vous mettez à jour une stratégie ou en créer une nouvelle, associez-la au groupe de test.</p>

Bon usage	Description
<p>un groupe test, vérifiez que le groupe test est classé correctement par ordre de priorité dans le Compliance Manager.</p> <p>Remarque : si vous utilisez le logiciel sous la forme d'un proxy RADIUS (en configurant le logiciel en mode proxy devant un autre serveur RADIUS), le nom du groupe doit correspondre à la valeur renvoyée du serveur RADIUS pour que l'utilisateur reçoive la stratégie correcte.</p>	<p>Faites en sorte que le groupe de test :</p> <ul style="list-style-type: none"> ■ Vérifie que les évaluations du système d'extrémité ont lieu et produisent des informations de rapport correctes. ■ Vérifie que l'application correcte a lieu pour la stratégie. ■ Vérifie que la messagerie correcte a lieu pour les profils qui sont évalués. ■ Vérifie que les messages soient compréhensibles aux utilisateurs.

2.1.2 Test des applications avant la création d'une application dans le Compliance Manager

Bon usage	Description
<p>Tester les applications avant d'en créer une dans le Compliance Manager.</p>	<p>Si vous créez une application et n'êtes pas sûr des informations que vous devez détecter sur le système d'extrémité, vous pouvez :</p> <ol style="list-style-type: none"> 1. Charger les applications que vous voulez détecter sur une machine test. 2. Rechercher les clés de registre associées. 3. Rechercher les processus en cours d'exécution associés dans le Gestionnaire des tâches Microsoft Windows. 4. Vérifier les informations d'applications sur toutes les plates-formes de système d'exploitation pour vous assurer d'avoir les clés de registre et les processus en cours d'exécution corrects pour chaque système d'exploitation. <p>Important : si vous utilisez une date dans une détection de registre, assurez-vous que l'application est détectée sur le système d'extrémité à l'aide du format de date correct. Vous pouvez sélectionner soit le paramètre régional du système qui détermine le format de date d'après la langue du système soit Anglais (États-Unis). Pour déterminer quel format utiliser, nous vous conseillons d'installer l'application sur les systèmes d'exploitation internationaux que vous avez l'intention de prendre en charge, d'exécuter l'application de l'éditeur et de déterminer comment les dates changent ou sont stockées pour</p>

Bon usage	Description
	chaque système d'exploitation, car celles-ci peuvent être différentes.

2.1.3 Test des modèles d'accès pour des paramètres de mise en application exacts

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

2.2 Utilisation du bouton Save As New

Bon usage	Description
Utiliser le bouton Save As New pour enregistrer une stratégie, un profil ou un modèle d'accès existant sous un nouveau nom et effectuer les mises à jour.	L'enregistrement sous la forme d'un nouvel élément vous permet de dupliquer une stratégie, un profil ou un modèle d'accès si vous ne voulez 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 seront appliqués la prochaine fois que l'agent récupérera une stratégie. En résumé, utilisez le bouton Save As New sauf si vous voulez que les changements soient effectifs immédiatement.

2.3 Utilisation de la fonction de verrouillage

Bon usage	Description
Verrouiller les stratégies, les profils, les applications, les modèles d'accès et les ressources réseau pour empêcher les changements involontaires.	<p>Le verrouillage de ces éléments du Compliance 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>

3 Bon usage des stratégies

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

- **Default Policy:** la stratégie par défaut définit la stratégie utilisée si un utilisateur n'appartient à aucun groupe ou si l'utilisateur appartient à un groupe auquel aucune stratégie n'a encore été affectée.
- **Policy Mode:** le mode de stratégie détermine la manière dont la stratégie évalue l'ordinateur d'extrémité, génère des rapports d'information dans le Compliance Manager et détermine si un message doit être envoyé à l'utilisateur, si des actions d'actualisation doivent être effectuées et/ou si des actions de mise en application doivent être prises.
- **Profiles:** les profils vous permettent de définir les éléments que vous souhaitez évaluer sur l'ordinateur d'extrémité, comme les systèmes d'exploitation et les applications.
- **Access Templates:** les modèles d'accès déterminent comment l'accès réseau est accordé aux ordinateurs d'extrémité.

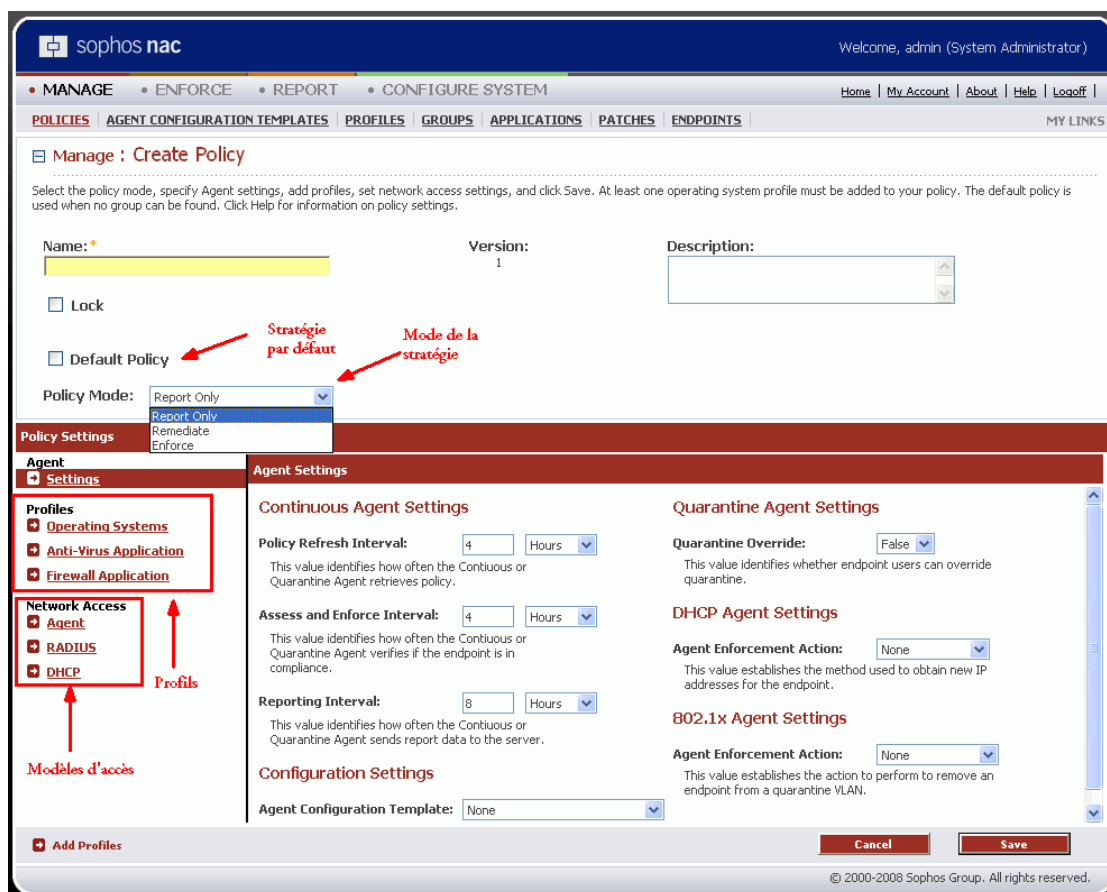


Schéma 1 : exemple de conventions des stratégies

3.1 Instructions générales sur les stratégies

Cette section vous indique le bon usage général des stratégies s'appliquant à toutes les mises en place de Sophos NAC Advanced.

3.1.1 Utilisation de la stratégie par défaut

Bon usage	Description
Utiliser la stratégie par défaut	<p>Si l'agent est installé sur un système d'extrémité mais son utilisateur n'appartient à aucun groupe ou le groupe auquel l'utilisateur appartient n'est pas associé à une stratégie, la stratégie par défaut est affectée à cet utilisateur. La stratégie par défaut est aussi utilisée lorsque l'agent temporaire n'exige pas d'enregistrement. 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 du Compliance Manager déterminent l'accès réseau.</p> <p>Remarque : spécifiez les paramètres Enforcer sur la page Configure System > Enforcer Settings du Compliance Manager.</p>

3.1.2 Définition du mode de stratégie approprié

Important : vous devez vérifier que les modèles d'accès appropriés des modes 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, changez 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 d'actualisation afin de les mettre en conformité avec les stratégies définies.	Le mode Remediate permet aux entreprises de signaler les utilisateurs non conformes et d'effectuer des actions d'actualisation afin de les mettre en conformité avec les stratégies définies. Ce mode est utilisé lorsque les actions de création de rapports et d'actualisation sont importantes mais que l'application n'est pas requise. Ce mode est aussi un moyen de se mettre en conformité à la stratégie avant d'activer l'application.
Utiliser le mode Enforce pour signaler, actualiser 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 permet aux entreprises de signaler, actualiser et appliquer la mise en conformité du réseau. Les modèles d'accès (Agent, RADIUS 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.

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

Bon usage	Description
Définir la fonction Quarantine Override (annulation de la quarantaine) 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 Quarantine Override sur True permet à l'utilisateur de retirer le système d'extrémité de la quarantaine même si ce dernier n'est pas conforme.

3.2 Profils dans la stratégie

Les profils vous permettent de définir les éléments que vous souhaitez évaluer sur l'ordinateur d'extrémité, comme les systèmes d'exploitation, les correctifs et les applications.

3.2.1 Gestion des stratégies contenant seulement les profils nécessaires

Bon usage	Description
Gérer les stratégies qui contiennent seulement les profils nécessaires. Supprimer des profils les correctifs qui sont déjà dans les services packs requis. Supprimer les profils obsolètes de toutes les stratégies.	Gestion des stratégies contenant seulement les profils antivirus, de pare-feu personnel, antispyware, de correctif et de système d'exploitation nécessaires afin qu'elles soient plus faciles à gérer et à prendre en charge.

3.2.2 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 en premier, puis les classer par ordre de priorité.	Les stratégies doivent contenir les profils de chaque système d'exploitation que vous voulez évaluer. Classez par ordre de priorité le système d'exploitation le plus important. 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

Bon usage	Description
	<p>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 Windows XP en premier, et assurez-vous que la condition Else dans le profil Windows XP est défini sur Non-Compliant (non conforme) 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.	<p>Par exemple, si vous avez plusieurs profils antivirus dans la stratégie, classez par ordre de priorité l'application antivirus la plus importante.</p> <p>Remarque : le classement par ordre de priorité n'est pas nécessaire pour les profils de correctifs. Tous les profils de correctifs dans une stratégie sont évalués sur le système d'extrémité, et les actions garanties associées à tous les profils de correctifs sont prises. Sophos NAC Advanced utilise le profil de correctif le moins conforme pour déterminer l'état de conformité des correctifs.</p>

3.3 Modèles d'accès dans la stratégie

Les modèles d'accès déterminent comment l'accès réseau est accordé aux systèmes d'extrémité. Les stratégies doivent seulement contenir des modèles d'accès pour les types d'application mis en place.

3.3.1 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.	Gestion des stratégies qui contiennent les modèles d'accès pour les types d'application mis en place. Ce bon usage facilite la résolution des problèmes d'accès réseau quel que soit le mode de la stratégie.

Bon usage	Description
<p>Vérifier que les modèles d'accès appropriés sont affectés à la stratégie.</p>	<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> <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, changez 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.

3.3.2 Configuration de l'agent pour afficher l'icône de la quarantaine

Bon usage	Description
<p>Configurer l'agent de quarantaine pour afficher l'icône de la quarantaine aux utilisateurs si le modèle d'accès partiellement conforme met en quarantaine les utilisateurs lorsqu'ils sont partiellement conformes.</p>	<p>Si vous ne configurez pas l'agent de quarantaine pour afficher l'icône de la quarantaine, l'utilisateur est placé en quarantaine sans aucune indication.</p> <p>Remarque: configurez l'icône de la quarantaine pour indiquer quand vous configurez le modèle de configuration d'agent dans le Compliance Manager. Une fois que vous créez des modèles de configuration d'agents, vous pouvez les ajouter aux stratégies. Exécutez cette opération avant d'activer l'application.</p>

4 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 l'ordinateur d'extrémité, comme les systèmes d'exploitation, les correctifs et les applications. Les profils définissent des conditions, des états de conformité, des messages et des actions d'actualisation. 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 profils sont placés dans des stratégies sur le type de profil. Les types de profils sont Anti-Spyware Application, Anti-Virus Application, Assessment Application, Firewall Application, HIPS Application, IDS Application, Operating System, Patch et Patch Manager. Les types de profils incluent aussi tous les types d'applications personnalisées qui sont créées.
- **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:** zone de liste indiquant si oui ou non un message apparaît pour l'utilisateur.
- **Message Icon:** icône qui affiche la fenêtre Message pour que vous puissiez créer des messages.
- **Condition:** déclarations utilisées lors de l'évaluation pour déterminer la conformité de l'ordinateur 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 de l'ordinateur 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 Advanced détermine qu'un ordinateur d'extrémité est conforme au profil antivirus, mais non conforme au 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:** paramètre qui teste la version.

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

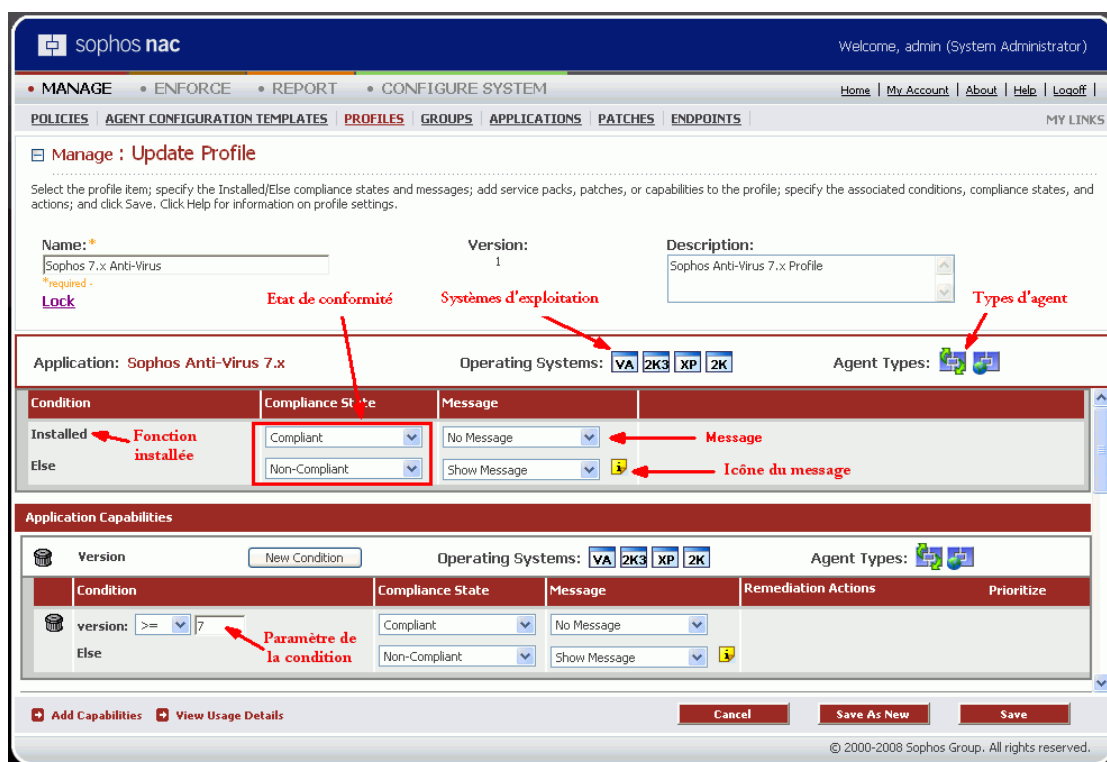


Schéma 2 : exemple de conventions de profils

4.1 Instructions générales sur les profils

Cette section vous indique le bon usage général des profils s'appliquant à toutes les mises en place de Sophos NAC Advanced.

4.1.1 Utilisation des profils prédéfinis pour créer des profils prêts pour la production

Bon usage	Description
Utiliser des profils prédéfinis comme guides.	<p>Utilisez des profils prédéfinis :</p> <ul style="list-style-type: none"> ■ Pour les démonstrations, les pilotes ou les tests de viabilité, 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, changer les actions, etc. ou simplement utiliser les profils comme un guide pour en créer des nouveaux. <p>Utilisez le profil Windows Update pour les ordinateurs d'extrémité administrés pour vous assurer que l'outil Windows Update est installé sur ceux-ci et que les mises à jour automatiques sont activées.</p>

4.1.2 Utilisation des noms de produits principaux pour identifier les applications

Bon usage	Description
Les noms de produits principaux peuvent être différents des noms des produits commercialisés.	Les applications sont répertoriées dans le Compliance Manager sous le nom du produit principal. Parfois, l'application est commercialisée sous un nom différent. Vérifiez le produit effectivement installé pour déterminer le nom du produit principal ou contactez l'éditeur pour vérifier ce nom. Nous vous conseillons de tester une stratégie en mode Report Only pour vous assurer que vous avez la configuration de stratégie correcte.

4.1.3 Gestion des profils de correctifs différente d'autres types de profils

Bon usage	Description
Les profils de correctifs sont gérés différemment des profils de système d'exploitation ou d'application.	<p>Les correctifs définissent les mises à jour logicielles pour les systèmes d'exploitation. Vous pouvez créer des correctifs personnalisés qui vous permettent d'évaluer la conformité par rapport aux personnalisations des systèmes d'exploitation ou utiliser les correctifs prédéfinis qui sont disponibles et automatiquement ajoutés au logiciel.</p> <p>Voici de astuces pour les profils de correctifs :</p> <ul style="list-style-type: none"> ■ Créez des profils de correctifs qui contiennent les correctifs de sécurité les plus importants. ■ N'incluez pas de correctifs dans les profils s'ils font déjà partie de service packs ou d'un profil de système d'exploitation. ■ Lors de la création de profils de correctifs, méfiez-vous des dépendances de correctifs. Une dépendance exige qu'une application ou un service spécifique soit installé(e) sur le système d'extrémité avant que le correctif ne soit installé. Vous pouvez restreindre la liste des correctifs par dépendance lors de la création des profils de correctifs.
Regrouper les correctifs dans les profils en fonction du niveau de criticité.	Regroupez les correctifs dans les profils en fonction de la criticité afin de pouvoir contrôler plus précisément l'état de conformité. Par exemple, vous pouvez vous assurer que les systèmes d'extrémité sans les correctifs les plus critiques installés sont non conformes tandis que ceux sans des correctifs moins critiques sont partiellement conformes.

Bon usage	Description
Ne pas inclure le même correctif dans deux profils différents qui utilisent des états de conformité différents.	Sophos NAC Advanced évalue tous les profils de correctifs dans la stratégie pour déterminer la conformité du système d'extrémité. Par conséquent, placer deux profils de correctifs dans une stratégie qui contient des correctifs qui se chevauchent et des états de conformité en conflit, comme conforme et non conforme, peut avoir des résultats imprévisibles.

4.2 Création de profils

Cette section présente le bon usage en matière d'ajout de fonctionnalités, d'actions d'actualisation et de messages aux profils.

4.2.1 Ajout de fonctionnalités aux profils

Les fonctionnalités sont les fonctions d'une application qui peuvent être testées pour leur conformité. Sophos NAC Advanced 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 vous 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. Nous vous conseillons 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 nécessite l'exécution d'un contrôle du système par une application antivirus une fois par semaine ou vous pouvez aussi avoir une stratégie de sécurité qui considère le contrôle en temps réel comme une protection appropriée. 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.

Bon usage	Description
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 une seule fois, 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.
Utiliser toutes les fonctionnalités disponibles pour des évaluations de systèmes d'extrémité plus sûres.	Utilisez toutes les fonctionnalités disponibles (à l'exclusion des fonctionnalités Grace Period et Date), si possible, afin que l'évaluation des systèmes d'extrémité soit plus sûre. Éliminez uniquement des fonctionnalités du profil si elles affectent le déploiement de Sophos NAC Advanced ou votre activité professionnelle.

4.2.2 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.	Si une condition est trouvée : <ul style="list-style-type: none"> ■ Utilisation de Compliant pour autoriser l'accès réseau. ■ Utilisation de 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 d'actualisation. ■ Utilisation de Non-Compliant pour refuser ou limiter l'accès réseau, afficher des messages et exécuter des actions d'actualisation. <p>La conformité des ordinateurs d'extrémité est déterminée par l'évaluation des profils couplée au comportement de la stratégie. Plusieurs profils sont remontés jusqu'au niveau de la stratégie pour déterminer la conformité globale. L'état le moins conforme détermine la conformité globale. Une fois que la conformité est déterminée, l'accès réseau est appliqué à l'aide des modèles d'accès affectés dans la stratégie.</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 ordinateur d'extrémité n'est pas à jour depuis 5 jours, mais seulement refuser l'accès réseau lorsque le fichier signature n'est pas à jour depuis 10 jours. Pour ce cas, ajoutez une nouvelle condition selon laquelle, après 5 jours, l'ordinateur d'extrémité est conforme, un avertissement s'affiche et l'accès réseau est autorisé. Ajoutez une autre condition selon laquelle, après 10 jours, l'ordinateur d'extrémité est partiellement conforme, un avertissement s'affiche et l'accès réseau est autorisé. Si le fichier signature de l'ordinateur d'extrémité n'est pas à jour depuis plus de 10 jours, un

Bon usage	Description
	<p>avertissement s'affiche et l'accès réseau est autorisé. Ce cas de figure donne aux utilisateurs cinq jours pour télécharger le fichier signature à jour avant qu'il ne devienne non conforme.</p>
<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 d'actualisation 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 ordinateurs d'extrémité non conformes.</p>
<p>Veiller à ce que les états de conformité, messages et actions d'actualisation 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 l'ordinateur d'extrémité des actions d'actualisation différentes.</p> <p>Par exemple, l'ordre par défaut peut indiquer que si un pare-feu est activé (Enabled), l'ordinateur d'extrémité est conforme (Compliant) ; Else (dans ce cas, signifiant que le pare-feu est non activé (Not Enabled)), l'ordinateur 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), l'ordinateur d'extrémité est non conforme (Non-Compliant) ; Else (signifiant que le pare-feu est activé (Enabled)), l'ordinateur d'extrémité est conforme (Compliant).</p>
<p>Utiliser des conditions et des états de conformité qui prennent en charge les stratégies de sécurité de votre entreprise.</p>	<p>Par exemple, vous pouvez avoir un stratégie de sécurité qui considère un ordinateur d'extrémité comme non conforme si la protection en temps réel n'est pas activée ou comme partiellement conforme si la protection en temps réel n'est pas activée et qui vous alerte sur cet état. 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, créez une alerte et exécutez une action d'actualisation sur le système 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 de l'ordinateur 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 de l'ordinateur</p>

Bon usage	Description
	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.
Pour les applications antivirus et antispyware, tester l'utilisation de l'opérateur == dans les fonctionnalités de date.	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 à), veillez à ce que la date renvoyée de l'ordinateur 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 l'ordinateur 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.

4.2.3 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 : il est possible que certains ordinateurs d'extrémité se connectant au réseau n'appartiennent pas à l'entreprise. Dans ce cas, les avertissements doivent être rédigés de manière adéquate car ces ordinateurs d'extrémité peuvent utiliser des applications non administrées différentes ou non prises en charge.

Bon usage	Description
Créer des messages et les supprimer à l'aide du mode de stratégie Report Only.	Création d'un profil pour lequel le message est presque le même que celui du profil utilisé en production. Vous pouvez supprimer des messages en sélectionnant le mode de stratégie Report Only. Lorsque vous voulez afficher les messages et exécuter des actions d'actualisation, mais ne souhaitez 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 Test et déploiement de Sophos NAC Advanced 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 Advanced va mettre la signature à jour immédiatement.
Créer tous les messages en anglais, puis créer les messages	L'agent sélectionne la langue la plus adaptée pour afficher les messages. Le message en anglais s'affiche s'il ne peut pas

Bon usage	Description
correspondants dans toutes les langues prises en charge.	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 fenêtre de message vide apparaît à l'utilisateur. Par ailleurs, les rapports du Compliance Manager affichent des messages en anglais et si aucun message n'existe, le champ message est vide.

4.2.4 Utilisation des actions d'actualisation

La disponibilité des actions d'actualisation dépend de la conception du logiciel de cette application. Il se peut que certaines actions d'actualisation 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 d'actualisation 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 d'actualisation et les supprimer à l'aide du mode de stratégie Report Only.	Création d'un profil pour lequel les actions d'actualisation sont aussi proches que possible du prêt pour la production. Vous pouvez supprimer des actions d'actualisation en sélectionnant le mode de stratégie Report Only. Lorsque vous voulez afficher les messages et exécuter des actions d'actualisation, mais ne souhaitez 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 Test et déploiement de Sophos NAC Advanced à la page 4.
Lors de l'exécution des actions d'actualisation, 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, l'ordinateur d'extrémité doit être hors conformité pour que les actions d'actualisation soient exécutées. Si vous créez une condition avec un état de conformité partiellement conforme, vous pouvez fournir des actions d'actualisation pour vous assurer que les ordinateurs d'extrémité sont à jour et considérés comme non conformes seulement lorsqu'ils sont sérieusement obsolètes.
Utiliser toutes les actions d'actualisation fournies lorsque cela est possible pour une évaluation plus sûre des systèmes d'extrémité.	Éliminez seulement des actions d'actualisation du profil si vous estimez qu'elles peuvent causer un problème lors du déploiement.
Éviter les actions d'actualisation si elles affectent les tâches essentielles sur un système d'extrémité.	Pour éviter cette utilisation, vous pouvez créer des profils distincts sans actions d'actualisation pour des utilisateurs spécifiques, temporairement dessélectionner des actions

Bon usage	Description
	<p>d'actualisation dans des profils existants ou changer la stratégie de l'utilisateur en mode de stratégie Report Only.</p> <p>Par exemple, si un ingénieur technico-commercial s'occupe d'un problème sur le site du client et rencontre des problèmes avec un pare-feu bloquant le trafic, il peut temporairement désactiver le pare-feu. Si le profil est défini pour automatiquement activer le pare-feu, l'ingénieur peut faire face à des temps d'arrêt en tentant de traiter le problème. Dans ce cas, vous pouvez avoir un profil particulier pour ingénieurs technico-commerciaux qui n'active pas le pare-feu et un autre profil pour le reste des utilisateurs qui active le pare-feu.</p> <p>Enfin, vous devez évaluer à quelle point une action d'actualisation perturbe les utilisateurs et évaluer les risques de non-exécution de l'action d'actualisation par rapport aux risques de non-exécution des tâches essentielles par votre personnel.</p>

5 Bon usage concernant les applications

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

- **Applications** : les applications définissent les logiciels, leurs fonctionnalités, leurs conditions associées et leurs possibles actions d'actualisation. Sophos NAC Advanced inclut des applications prédéfinies. Vous pouvez également créer des applications personnalisées aux besoins de votre entreprise.
- **Application Types** : les types d'application classifient les applications et établissent des comportements de stratégie par défaut pour toutes les applications associées au type d'application. Vous pouvez créer des types d'application personnalisés ou utiliser les types d'application prédéfinis.

Les types d'application prédéfinis sont Anti-Spyware Application, Anti-Virus Application, Assessment Application, Firewall Application, HIPS Application, IDS Application et Patch Manager Application.

5.1 Création de types d'application

Lorsque vous créez des types d'application, vous pouvez définir comment vous voulez que les applications de ce type soient évaluées en sélectionnant le comportement Best ou All.

Remarque : les applications prédéfinies ont une méthode d'évaluation par défaut qui peut être changée dans la stratégie.

- **Use Best Profile** : 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 qui est le **plus** conforme sur le système d'extrémité pour déterminer l'état de conformité pour le 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.
- **Use All Profiles** : 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 meilleur comportement utilise le profil qui est le **moins** conforme sur le système d'extrémité pour déterminer l'état de conformité pour le type de profil dans la stratégie. Les profils de correctifs sont évalués de cette manière. Les profils d'applications que vous voulez empêcher sur le système d'extrémité peuvent être évalués de cette manière.

Par exemple, si vous créez un type d'application appelé "Peer-to-Peer Application" conçu pour contenir des applications peer-to-peer et refuser l'accès réseau si ces applications fonctionnent, vous pouvez spécifier par défaut un comportement de stratégie All. L'accès réseau sera refusé aux systèmes d'extrémité avec des applications peer-to-peer en cours d'exécution.

5.1.1 Création de types d'application

Bon usage	Description
Créer de nouveaux types d'application lorsque vous avez une nouvelle classification d'applications.	Les types d'application vous permettent d'organiser les applications en catégories. La création de types d'application vous permet de contrôler le comportement de stratégie par défaut (Use Best Profile/Use All Profile) lorsque plusieurs applications de ce type sont ajoutées à une stratégie.
Pour les applications que vous ne voulez pas exécuter sur un système d'extrémité, créez des types d'application avec le comportement Use All Profile.	Le comportement Use All Profile garantit que votre stratégie est appliquée si une des applications ou un des composants définis est détecté. En outre, en paramétrant vos profils d'applications avec les messages et les actions d'actualisation appropriés, vous pouvez vous assurer que l'opportunité a bien été donnée à l'utilisateur de résoudre tous les problèmes avant la nouvelle tentative d'accès au réseau.
Pour les applications que vous voulez exécuter sur un système d'extrémité, créez des types d'application avec le comportement Use Best Profile.	Le comportement Use Best Profile garantit que votre stratégie est appliquée si aucun ou aucune des applications ou composants définis n'est détecté(e). En outre, en paramétrant vos profils d'application avec les messages et les actions d'actualisation appropriés, vous pouvez vous assurer que l'utilisateur reçoit seulement les messages et les actions d'actualisation appartenant à l'application ou au composant que le système doit exécuter.

5.2 Création d'applications

Cette section vous indique le bon usage de la création d'applications s'appliquant à toutes les mises en place de Sophos NAC Advanced.

5.2.1 Création d'application distinctes pour plusieurs systèmes d'exploitation

Lors de la création d'applications pour plusieurs systèmes d'exploitation, vous pouvez :

- Créer des applications distinctes pour chaque système d'exploitation.
- Créer une seule application qui inclut de règles individuelles de détection d'applications pour chaque système d'exploitation classées par groupe de détection et ajouter des évaluations OR à chaque groupe de détection.

Bon usage	Description
Créer des applications distinctes lorsque les règles de détection sont	À moins que toutes les règles de détection soient les mêmes pour une application quel que soit le système d'exploitation,

Bon usage	Description
différentes pour chaque système d'exploitation.	nous vous conseillons de créer pour chaque système d'exploitation des applications distinctes qui définissent des règles de détection individuelles pour ce système d'exploitation.
Créer des applications distinctes lorsque vous définissez des versions dans les règles de détection d'applications (et non dans le profil) et lorsque vous avez des versions différentes d'une application sur le même système d'exploitation.	Si vous définissez des versions dans les règles de détection d'applications (et non dans le profil), créez des applications distinctes pour chaque version d'application sur le même système d'exploitation pour faciliter la maintenance et l'ajout de stratégies. Pour plus d'informations sur la définition des versions dans le profil, reportez-vous à la section Utilisation de la valeur Specify in Profile à la page 26.

5.2.2 Utilisation de plusieurs règles de détection d'applications pour définir une application

Bon usage	Description
Utiliser plusieurs règles de détection d'applications pour définir une application.	Utilisation d'autant de règles de détection d'applications que possible pour identifier et détecter plus précisément une application. Par exemple, si une application a une clé de registre et une version de fichier, créez des règles de détection d'applications pour les deux.

5.2.3 Utilisation de la fonctionnalité d'application appropriée pour la détection

Bon usage	Description
Utiliser la fonctionnalité d'application appropriée pour la détection	<ul style="list-style-type: none"> ■ Créez une fonctionnalité Installed pour chaque application. Une fonctionnalité Installed doit exécuter un test qui garantit que l'application est installée. ■ Si l'application a des processus en cours d'exécution qui indiquent que l'application fonctionne correctement, vous devez créer une fonctionnalité Running. ■ Si l'application a une version disponible, vérifiez que la version correcte est installée, ensuite vous devez créer une fonctionnalité Version. ■ Si l'application a des valeurs supplémentaires que vous voulez tester et si elles ne conviennent pas dans l'une des autres fonctionnalités ou si vous avez déjà créé une fonctionnalité d'un type particulier, vous pouvez créer une fonctionnalité Value pour tester des valeurs supplémentaires.

5.2.4 Création de fonctionnalités distinctes pour appliquer différents états de conformité ou messages

Bon usage	Description
Créer des fonctionnalités distinctes pour les règles de détection lorsque vous voulez appliquer des états de conformité ou des messages différents.	Pour pouvoir définir un état de conformité ou afficher des messages pour une règle de détection spécifique, vous devez créer une fonctionnalité distincte pour cette règle de détection. Si vous créez une fonctionnalité avec plusieurs règles de détection, vous pouvez seulement définir un état de conformité et appliquer un message à cette série de règles de détection dans le profil.

5.2.5 Utilisation de la valeur Specify in Profile

Lors de l'utilisation de fonctionnalités qui prennent en charge des valeurs non booléennes (c'est-à-dire, Version et Value), l'agent peut déterminer l'état d'installation et opérationnel d'une application à l'aide d'une valeur prédéterminée.

Important : si vous utilisez une date dans une détection de registre, assurez-vous que l'application est détectée sur le système d'extrémité à l'aide du format de date correct. Vous pouvez sélectionner soit le paramètre régional du système qui détermine le format de date d'après la langue du système soit Anglais (Etats-Unis). Nous vous recommandons d'installer

l'application sur les systèmes d'exploitation internationaux que vous avez l'intention de prendre en charge, d'exécuter l'application de l'éditeur et de déterminer comment les dates changent ou sont stockées pour chaque système d'exploitation, car celles-ci peuvent être différentes.

Bon usage	Description
Lors de la création d'applications, utiliser l'option "Specify in Profile" pour la valeur plutôt que l'option "Specify Now".	L'option "Specify in Profile" nécessite moins de maintenance de l'application si une valeur change. En outre, les applications peuvent être changées une fois qu'elles sont associées aux profils. Par conséquent, l'option "Specify Now" doit seulement être utilisée si une valeur ne change jamais.

5.2.6 Création de règles de détection avec une version correcte

Bon usage	Description
Lors de la définition des règles de détection avec des versions, s'assurer que le numéro de version contient le nombre correct de valeurs significatives.	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.

5.3 Exemples d'application

Cette section fournit des exemples d'application pour une application peer-to-peer et une application de messagerie instantanée. Il s'agit d'applications standard que les entreprises ne souhaitent peut-être pas voir utiliser par leurs employés.

5.3.1 Exemple Kazaa

Kazaa est une application peer-to-peer que les entreprises ne souhaitent peut-être pas voir utiliser par leurs employés. Une règle de détection d'applications peut être créée pour déterminer si le processus kazaa.exe fonctionne. S'il fonctionne, l'accès réseau peut être refusé au système d'extrémité.

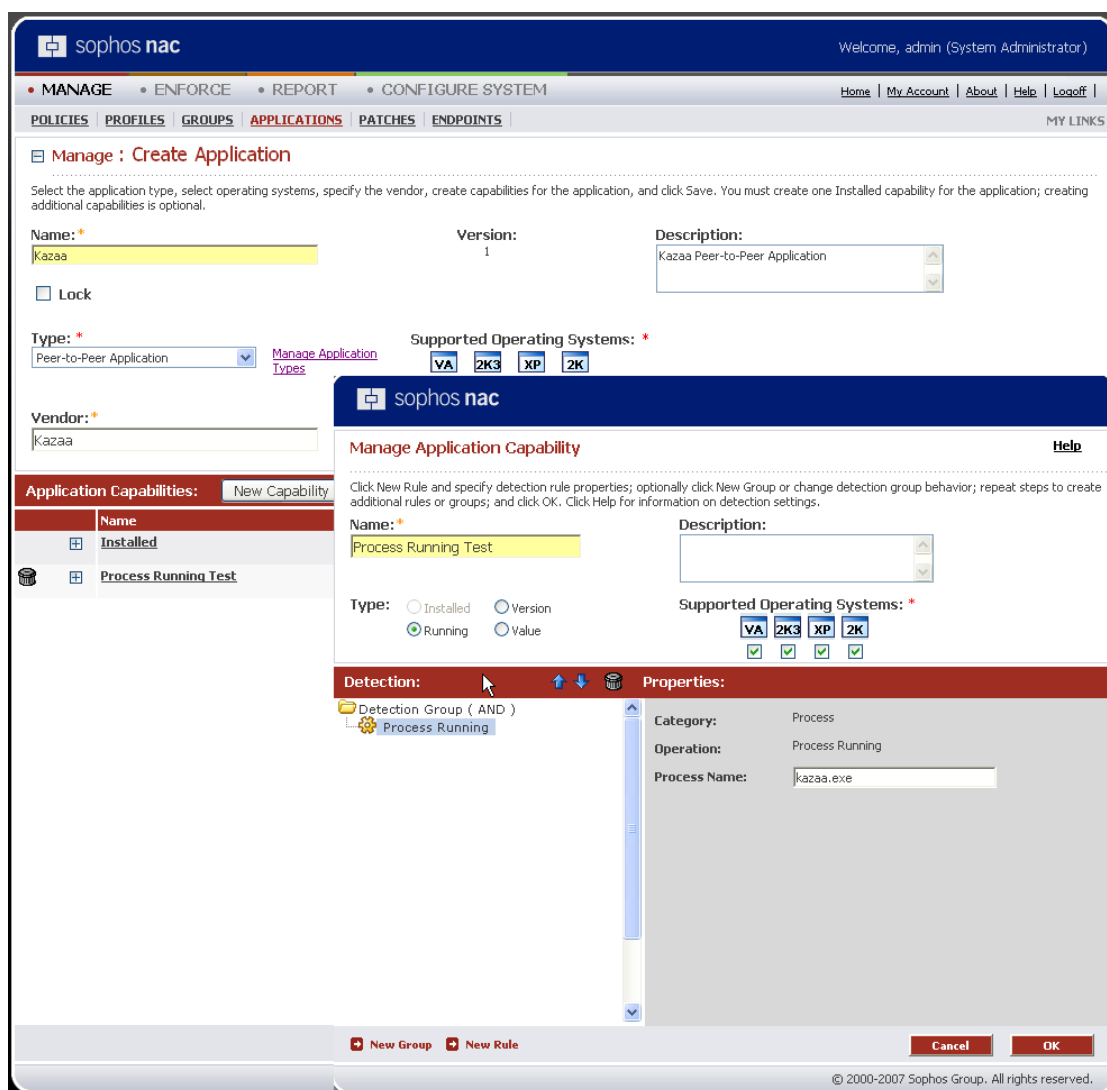


Schéma 3 : exemple Kazaa

5.3.2 Exemple America Online (AOL) Instant Messenger

AOL[®] Instant Messenger est une application peer-to-peer dont les entreprises peuvent autoriser l'utilisation à leurs employés, mais seulement s'ils utilisent une version spécifique de l'application. Une règle de détection d'applications peut être créée pour déterminer si le processus aim.exe est en cours d'exécution et si oui ou non il s'agit d'une version approuvée. Si le processus est en cours d'exécution et s'il ne s'agit pas de la version correcte, l'accès réseau peut être refusé au système d'extrémité.

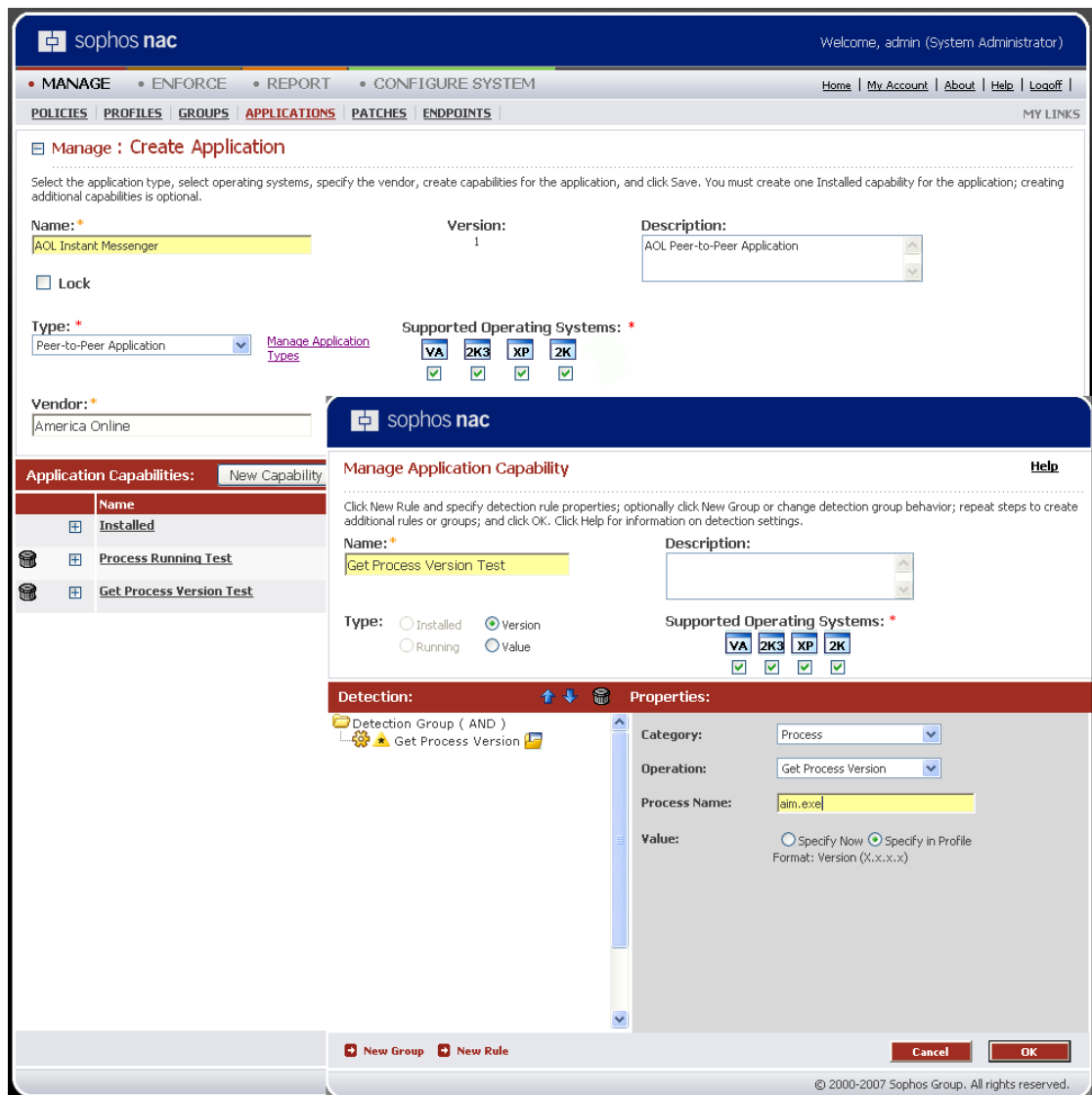


Schéma 4 : exemple AOL

6 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 Advanced prend en charge la mise en application de l'agent, de RADIUS, et du protocole DHCP. Lorsque des modèles d'accès sont appliqués aux états d'accès conformes, partiellement conformes ou non conformes dans le Compliance Manager, l'accès au 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 Compliance Manager.

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

- **Network Resources:** 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 s'appliquent uniquement aux systèmes d'extrémité exécutant l'agent de quarantaine.
- **Access Enforcer Access Templates:** 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.
- **RADIUS Enforcer Access Templates:** les modèles d'accès RADIUS Enforcer vous permettent de spécifier des paramètres d'accès nécessaires à la prise en charge de la mise en application de RADIUS. RADIUS est un protocole qui fournit des services d'authentification, d'autorisation et de comptabilité sur les réseaux. Les modèles d'accès RADIUS Enforcer sont seulement utilisés avec la mise en application de RADIUS. L'application RADIUS Enforcer est utilisée avec un réseau privé virtuel (VPN), 802.1x, Cisco NAC et avec les mises en place étendues de RADIUS.
- **DHCP Enforcer Access Templates:** les modèles d'accès DHCP Enforcer vous permettent de spécifier les paramètres d'accès nécessaires à la prise en charge de l'application DHCP. DHCP est un protocole qui affecte automatiquement des adresses IP sur les réseaux. Les modèles d'accès DHCP Enforcer sont seulement utilisés avec la mise en application du protocole DHCP.
- **Exemptions:** les **exemptions** identifient selon divers critères les systèmes d'extrémité dont la conformité n'a pas besoin d'être évaluée lors de la connexion au réseau. Les systèmes d'extrémité exemptés incluent ceux qui soit ne sont pas en mesure d'exécuter l'agent, soit n'ont pas besoin d'évaluation de conformité comme les serveurs, les routeurs, les imprimantes ou les systèmes d'extrémité jugés "sains". Les exemptions sont uniquement utilisées avec la mise en application de RADIUS ou du protocole DHCP.

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

Bon usage	Description
Créer un modèle d'accès proche semblable à l'environnement de production.	Utilisez le paramètre Policy Mode dans la stratégie pour augmenter peu à peu l'impact sur l'utilisateur. Vous pouvez simplement activer la mise en application à l'aide d'un paramètre, tout en apportant des changements futures minimales aux modèles d'accès. Pour plus d'informations, reportez-vous à la section Définition du mode de stratégie approprié à la page 10.
Créer tous les modèles d'accès avant la création ou la mise à jour des stratégies.	Lorsque vous êtes prêt, vous pouvez créer ou mettre à jour les stratégies qui contiennent les modèles d'accès que vous avez créés. En sélectionnant des états de conformité modèles lorsque vous créez des modèles d'accès, les modèles d'accès sont automatiquement ajoutés aux nouvelles stratégies.

6.2 Utilisation de modèles d'accès prédéfinis comme guides

Bon usage	Description
Utiliser des modèles d'accès prédéfinis comme guides	Utilisez les modèles d'accès système prédéfinis : <ul style="list-style-type: none"> ■ Pour les démonstrations, les pilotes ou les tests de viabilité, 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.
En cas de non utilisation des modèles d'accès prédéfinis, veiller à les supprimer de la stratégie ou des états d'accès des paramètres Enforcer. Puis ajouter les nouveaux modèles d'accès.	Si vous ne voulez pas utiliser des modèles d'accès prédéfinis, vous pouvez les supprimer ou dessélectionner les états de conformité modèles dans les modèles d'accès. Cette action empêche les modèles d'accès d'être automatiquement ajoutés aux nouvelles stratégies.

6.3 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
<p>Classer par ordre de priorité tout d'abord les ressources réseau, modèles d'accès et exemptions les plus spécifiques/strictes, puis les moins spécifiques/strictes.</p>	<ul style="list-style-type: none"> ■ Network Resources: si plusieurs ressources réseau s'appliquent à un ordinateur d'extrémité, la première qui correspond déterminera l'accès réseau. Les ressources réseau exécutables sont évaluées avant les ressources réseau de ports/protocoles. ■ Access Templates: 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 ordinateur 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 client RADIUS, du serveur DHCP ou du relais DHCP est utilisé.

6.4 Spécification des états de conformité des modèles

Bon usage	Description
<p>Ne pas sélectionner les états de conformité de modèles en conflit.</p>	<p>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.</p> <p>Pour plus d'informations sur les cas de figure d'application spécifiques, reportez-vous à la section Annexe : cas de figure de mise en application à la page 41.</p>
<p>Sélectionner seulement les états de conformité modèles si vous voulez que le modèle d'accès soit automatiquement ajouté aux nouvelles stratégies.</p>	<p>Si vous voulez contrôler l'ajout des modèles d'accès aux nouvelles stratégies, ne sélectionnez pas les états de conformité modèles.</p> <p>Pour les mises en place plus importantes, vous pouvez, si vous le voulez, sélectionner un état de conformité pour ajouter automatiquement des modèles d'accès aux nouvelles stratégies. Les stratégies existantes ne sont pas affectées lorsque vous créez de nouveaux modèles d'accès.</p>

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: Description:

Template Compliance States: (Used when creating policy)

Compliant
 Partially Compliant
 Non-Compliant

Lock

Schéma 5 : exemple d'état de conformité modèle

6.5 Spécification des 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	<p>Si vous utilisez la mise en application de RADIUS ou la mise en application du protocole DHCP, spécifiez les modèles d'accès appropriés pour l'état d'accès par défaut (Default) sur la page Configure System > Enforcer Settings du Compliance Manager.</p> <p>L'état d'accès par défaut est essentiellement un dernier recours pour l'affectation des modèles d'accès. Par conséquent, nous vous conseillons 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 ordre de priorité les modèles d'accès les plus spécifiques/stricts et identifiez le modèle d'accès à la plus basse priorité avec les paramètres ANY - Deny All.</p>

6.6 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

Bon usage	Description
	<p>reconnaissent pas les caractères joker et seront seulement pris en charge pour les protocoles TCP et UDP.</p> <ul style="list-style-type: none"> ■ Le logiciel détecte seulement les exécutable qui s'exécutent au niveau Winsock.

6.7 Utilisation des modèles d'accès avec les exemptions pour contrôler le déploiement de Sophos NAC Advanced

Bon usage	Description
<p>En cas d'utilisation de la mise en application de RADIUS ou du protocole DHCP, utilisez les modèles d'accès et les exemptions pour effectuer le déploiement par étapes de l'application.</p>	<p>Utilisation des modèles d'accès RADIUS ou DHCP Enforcer avec les exemptions pour simplifier le déploiement de Sophos NAC Advanced dans des sous-groupes du réseau et sur les dispositifs d'application. Vous pouvez définir moins de modèles d'accès, puis définir des exemptions pour distinguer les segments du réseau qui ne sont pas encore prêts à être mis en application. De cette manière, vous pouvez déployer la mise en application comme d'habitude et cibler des périphériques ou des sous-groupes de périphériques particuliers à exempter lorsque nécessaire et uniquement si nécessaire. La mise en application du protocole DHCP évalue toujours les exemptions en premier.</p>

7 Bon usage concernant l'enregistrement

Cette section présente le bon usage pour l'enregistrement. L'enregistrement à Sophos NAC Advanced améliore la sécurité et simplifie le processus d'authentification. Le processus d'enregistrement de l'agent de conformité inclut la prise en charge de l'authentification RSA en deux facteurs et exploite les paramètres challenge-réponse du serveur RSA existant de l'entreprise. Nous conseillons aux entreprises d'utiliser ces méthodes de bon usage pour s'assurer que l'opération d'enregistrement des utilisateurs se déroulent comme prévue.

La configuration de l'enregistrement est un processus en deux parties. L'enregistrement doit être configuré à la fois dans le Compliance Manager et dans l'agent. Si le paramètre d'enregistrement du Compliance Manager n'est pas synchronisé avec le mode d'enregistrement d'agent, la fonction d'enregistrement ne fonctionnera pas comme prévue.

Enregistrement de l'agent de conformité

Paramètre d'enregistrement du Compliance Manager

Utilisez la zone **Configure System > Agent Registration** du Compliance Manager pour spécifier le paramètre d'enregistrement du Compliance Manager. Les paramètres d'enregistrement disponibles dans le Compliance Manager sont :

- **Every:** l'agent demande à l'utilisateur de s'enregistrer avec un nom utilisateur et un mot de passe selon l'intervalle de temps spécifié pour toutes les sessions de l'agent.
- **Once:** l'agent demande à l'utilisateur de s'enregistrer une fois avec un nom utilisateur et un mot de passe. Les sessions suivantes de l'agent exigent que l'utilisateur utilise seulement son nom utilisateur.
- **Never:** l'agent n'invite pas à l'enregistrement ou ne demande pas à l'utilisateur de s'enregistrer avec un mot de passe. Si vous voulez que l'utilisateur s'enregistre à l'aide des codes d'accès de domaine Windows qu'il utilise pour ouvrir une session sur son ordinateur d'extrémité, sélectionnez le paramètre d'enregistrement **Never** et définissez le paramètre **Register** dans le modèle de configuration de l'agent sur **Use Computer Logon**. Si l'utilisateur ne s'enregistre pas avec ses codes d'accès de domaine Windows et que vous voulez qu'il s'enregistre uniquement avec un nom utilisateur, définissez le paramètre **Register** dans le modèle de configuration de l'agent sur **No Password** afin qu'il corresponde au paramètre d'enregistrement **Never**.



Avertissement : si le paramètre **Use Computer Logon** n'est **pas** sélectionné, le paramètre d'enregistrement **Never** permet l'accès au réseau sans authentification de l'utilisateur.

Mode d'enregistrement de l'agent

Utilisez la zone **Manage > Agent Configuration Templates** du Compliance Manager pour spécifier le mode d'enregistrement de l'agent. Les paramètres disponibles d'enregistrement de l'agent sont :

- **Always Prompt:** l'agent invite à saisir un nom utilisateur et un mot de passe et effectue l'enregistrement à chaque lancement de l'agent.
- **Prompt on Demand:** l'agent invite à saisir un nom utilisateur et un mot de passe seulement lorsque l'enregistrement a expiré. Sinon, il invite à saisir un nom utilisateur uniquement.

- **No Password:** l'agent n'invite pas à saisir de mot de passe pendant l'enregistrement sauf s'il est requis par le serveur d'applications de conformité.
- **Use Computer Logon:** l'agent n'invite pas à saisir de nom utilisateur ou de mot de passe. L'enregistrement a lieu lorsque l'utilisateur saisit ses codes d'accès de domaine Windows au moment où il ouvre une session sur son système d'extrémité.

Remarque : le paramètre Use Computer Logon peut uniquement être utilisé lorsque l'utilisateur ouvre une session sur son système d'extrémité avec ses codes d'accès de domaine Windows. Ce paramètre ne peut pas être utilisé avec l'agent temporaire. L'agent n'invite pas l'utilisateur qui se connecte pour la première fois à saisir son nom utilisateur et son mot de passe sauf si le paramètre Use Computer Logon a été sélectionné au cours de l'installation. Pour configurer l'installation de l'agent sur le paramètre Use Computer Logon, utilisez la commande suivante **msiexec /i "<chemin complet du fichier d'installation de l'agent>" AGENT_SETTINGS="Register=UseComputerLogon"**.

Enregistrement de l'agent temporaire de conformité

Paramètre d'enregistrement du Compliance Manager

Utilisez la zone **Configure System > Agent Registration** du Compliance Manager pour spécifier le paramètre d'enregistrement du Compliance Manager. Les paramètres d'enregistrement disponibles dans le Compliance Manager sont :

- **On:** l'agent demande à l'utilisateur de s'enregistrer avec un nom utilisateur et un mot de passe.
- **Off:** l'agent ne demande pas d'effectuer l'enregistrement.

Important : lorsque l'enregistrement n'est pas nécessaire, l'agent temporaire utilise la stratégie par défaut pour vérifier l'état de conformité d'un ordinateur d'extrémité. Assurez-vous que la stratégie par défaut est sélectionnée lorsque l'agent n'invite pas à s'enregistrer.

Paramètre d'enregistrement d'agent

Au cours de l'installation du serveur Web de l'agent temporaire, vous pouvez définir le paramètre d'enregistrement de l'agent de la manière suivante :

- Si la case "Always register agent with server" est sélectionnée, l'agent demande aux utilisateurs de s'enregistrer à l'aide de leur nom utilisateur et de leur mot de passe.
- Si la case "Always register agent with server" n'est **pas** sélectionnée, l'agent ne demande pas à effectuer l'enregistrement.

7.1 Synchronisation du paramètre d'enregistrement du Compliance Manager avec le mode d'enregistrement d'agent

Enregistrement de l'agent de conformité

Paramètre d'enregistrement du Compliance Manager	Mode d'enregistrement de l'agent	Exemple
Every (spécifie un intervalle temporel en minutes, heures, jours, semaines ou mois)	Always Prompt	Si le paramètre d'enregistrement du Compliance Manager est Every 1 day ou moins, définissez le mode d'enregistrement de l'agent sur Always Prompt. Ces paramètres fonctionnent ensemble pour demander à l'utilisateur de s'enregistrer tous les jours.
Every (spécifie un intervalle temporel en minutes, heures, jours, semaines ou mois)	Prompt on Demand	Si le paramètre d'enregistrement du Compliance Manager est Every 7 days ou plus, définissez le mode d'enregistrement de l'agent sur Prompt on Demand. Ces paramètres fonctionnent ensemble pour demander que l'utilisateur s'enregistre tous les sept jours.
Once	Prompt on Demand	Si le paramètre d'enregistrement du Compliance Manager est Once, définissez le mode d'enregistrement de l'agent sur Prompt on Demand. Ces paramètres fonctionnent ensemble pour demander à l'utilisateur de s'enregistrer seulement une fois.
Never	No Password	Si le paramètre d'enregistrement du Compliance Manager est Never, définissez le mode d'enregistrement de l'agent sur No Password. Ces paramètres fonctionnent ensemble pour que l'utilisateur n'ait jamais à s'enregistrer. Ces paramètres ne procèdent pas à l'authentification de l'utilisateur.

Paramètre d'enregistrement du Compliance Manager	Mode d'enregistrement de l'agent	Exemple
Never	Use Computer Logon	<p>Si le paramètre d'enregistrement du Compliance Manager est Never, définissez le mode d'enregistrement de l'agent sur Use Computer Logon. Le mode Use Computer Logon peut uniquement être utilisée lorsque l'utilisateur ouvre une session sur son système d'extrémité avec ses codes d'accès de domaine Windows.</p> <p>Ces paramètres fonctionnent ensemble pour demander l'utilisation de codes de connexion de l'ordinateur de l'utilisateur. L'avantage de ces paramètres pour l'utilisateur est qu'il doit uniquement saisir ces codes d'accès de domaine Windows lorsqu'il ouvre une session sur son système d'extrémité.</p>

Enregistrement de l'agent temporaire de conformité

Paramètre d'enregistrement du Compliance Manager	Paramètre d'enregistrement d'agent	Exemple
On	La case "Always register agent with server" est sélectionnée	<p>Si le paramètre d'enregistrement du Compliance Manager est sur On, sélectionnez le paramètre d'enregistrement de l'agent au cours de l'installation du serveur Web de l'agent temporaire.</p> <p>Ces paramètres fonctionnent ensemble pour demander à l'utilisateur de s'enregistrer lors de l'exécution de l'agent temporaire.</p>
Off	La case "Always register agent with server" n'est pas sélectionnée	<p>Si le paramètre d'enregistrement du Compliance Manager est sur Off, ne sélectionnez pas le paramètre d'enregistrement de l'agent au cours de l'installation du serveur Web de l'agent temporaire.</p>

Paramètre d'enregistrement du Compliance Manager	Paramètre d'enregistrement d'agent	Exemple
		<p>Ces paramètres fonctionnent ensemble afin que l'utilisateur n'ait pas à s'enregistrer lors de l'exécution de l'agent temporaire. Ces paramètres ne procèdent pas à l'authentification de l'utilisateur.</p> <p>Important : lorsque l'enregistrement n'est pas nécessaire, l'agent temporaire utilise la stratégie par défaut pour vérifier l'état de conformité d'un ordinateur d'extrémité. Assurez-vous que la stratégie par défaut est sélectionnée lorsque l'agent n'invite pas à s'enregistrer. Notez que la mise en application de RADIUS ne peut pas être utilisée lorsque l'enregistrement n'est pas nécessaire. En effet, l'accès à RADIUS est un accès utilisateur.</p>

7.2 Bon usage de l'enregistrement pour des scénarios spécifiques

Les scénarios suivants sont utilisés pour l'agent de conformité lorsque le paramètre d'enregistrement du Compliance Manager n'est **pas** défini sur Never et que le paramètre d'enregistrement de l'agent n'est **pas** défini sur No Password, et pour l'agent temporaire de conformité lorsque le paramètre d'enregistrement du Compliance Manager est défini sur On et que la case "Always register agent with server" est sélectionnée.

Scénario	Enregistrement du Compliance Manager
Une violation de sécurité par utilisateur ou plus	Expiration de l'enregistrement de chaque utilisateur. Cette action oblige chaque utilisateur à s'enregistrer de nouveau et à s'authentifier avec un nom utilisateur et un mot de passe valides.
Un ou plusieurs utilisateurs ont été déplacés d'un groupe vers un autre	Expiration de l'enregistrement de chaque utilisateur. Lorsque chaque utilisateur s'enregistre de nouveau avec un nom utilisateur et un mot de passe valides, la stratégie associée au nouveau groupe est appliquée sur le système d'extrémité de chaque utilisateur.

Scénario	Enregistrement du Compliance Manager
Un nom de groupe dans la banque d'utilisateurs de l'entreprise a été changé	<p>Expiration de l'enregistrement de chaque utilisateur dans le groupe. Cette action oblige chaque utilisateur du groupe à s'enregistrer de nouveau.</p> <p>Remarque : en outre, vérifiez que le groupe a été ajouté et classé par ordre de priorité de manière appropriée dans la zone Manage > Groups du Compliance Manager.</p>
Un utilisateur n'est plus employé	<p>Suppression de l'enregistrement de l'utilisateur.</p> <p>Remarque : en outre, supprimez l'utilisateur de la banque d'utilisateurs de l'entreprise.</p>

8 Annexe : cas de figure de mise en application

Utilisez ces définitions dans les cas de figure suivants :

- **User:** indique le type d'utilisateur dans ce cas de figure. Les utilisateurs sont soit distants soit des utilisateurs d'un réseau local. Les utilisateurs distants utilisent un réseau privé virtuel (VPN) pour se connecter aux ressources de l'entreprise.
- **Agent Type:** indique quel agent est installé sur l'ordinateur d'extrémité. Les configurations d'agent disponibles sont l'agent de quarantaine ou l'agent temporaire.
- **Enforcement Type:** indique la mise en application utilisée pour déterminer l'accès de l'ordinateur d'extrémité aux ressources de l'entreprise : mise en application de l'agent, mise en application de RADIUS ou mise en application de DHCP.
- **Network Hardware:** indique si du matériel réseau spécifique est nécessaire pour que ce cas de figure fonctionne correctement.

8.1 Création d'une stratégie pour les utilisateurs du réseau local avec application de l'agent

Dans ce cas de figure, les utilisateurs du réseau local sont continuellement évalués et l'application est assurée. Il n'y a pas d'utilisateurs distants dans ce cas de figure.

Utilisateur	Type d'agent	Mise en application	Matériel réseau
Utilisateurs du réseau local	agent de quarantaine	Mise en application de l'agent	Aucun

Stratégie en mode Enforce

Les profils suivants figurent dans la stratégie :

- **Windows XP operating system profile:** nécessite que Windows XP et les service packs appropriés soient installés.
- **Sophos Anti-Virus 9.x profile:** nécessite que Sophos Anti-Virus 9.x soit installé, que la protection en temps réel soit activée, que le fichier signature soit mis à jour dans les 5 jours et que la version du logiciel soit supérieure ou égale à 9.
- **Sophos Client Firewall 2.x profile:** nécessite que Sophos Client Firewall soit installé, activé et que la version du logiciel soit supérieure ou égale à 2.

Remarque : comme ce scénario utilise l'application de l'agent et n'affecte que les utilisateurs du réseau local, les modèles d'accès RADIUS et DHCP associés à la stratégie ne sont pas considérés.

État de conformité	Modèle d'accès Agent Enforcer	Action
<p>Conforme</p> <ul style="list-style-type: none"> ■ Windows XP et les services packs sont installés. ■ Sophos Anti-Virus 9.x est installé, la protection en temps réel est activée et le fichier signature est mis à jour tous les 5 jours. ■ Sophos Client Firewall 2.x est installé et activé. 	<p>Autorise l'accès réseau.</p>	<p>Aucune action n'est nécessaire.</p>
<p>Partiellement conforme</p> <ul style="list-style-type: none"> ■ Windows XP et les services packs sont installés. ■ Sophos Anti-Virus 9.x est installé, la protection en temps réel est activée, mais le fichier signature est obsolète. ■ Sophos Client Firewall 2.x est installé et activé. 	<p>Autorise l'accès réseau.</p>	<p>Un message indique aux utilisateurs que le logiciel va mettre à jour le fichier signature de Sophos Anti-Virus. Le logiciel met automatiquement à jour le fichier signature de Sophos Anti-Virus.</p>
<p>Non conforme</p> <ul style="list-style-type: none"> ■ Windows XP et les services packs sont installés. 	<p>Place les utilisateurs en quarantaine et autorise seulement l'accès à Internet</p>	<ul style="list-style-type: none"> ■ Un message indique aux utilisateurs que le logiciel va

État de conformité	Modèle d'accès Agent Enforcer	Action
<ul style="list-style-type: none"> ■ Sophos Anti-Virus 9.x est installé, mais la protection en temps réel est désactivée et le fichier signature n'est pas à jour. ■ Sophos Client Firewall 2.x est installé, mais n'est pas activé. 	<p>pour que la signature antivirus soit mise à jour.</p>	<p>mettre à jour le fichier signature de Sophos Anti-Virus. Le logiciel met automatiquement à jour le fichier signature de Sophos Anti-Virus.</p> <ul style="list-style-type: none"> ■ Un message indique aux utilisateurs que le logiciel va activer la protection en temps réel de Sophos Anti-Virus. Le logiciel active automatiquement la protection en temps réel de Sophos Anti-Virus. ■ Un message indique aux utilisateurs que le logiciel va activer Sophos Client Firewall. Le logiciel active automatiquement Sophos Client Firewall.

8.2 Création d'une stratégie pour utiliser l'application de l'agent et RADIUS

Dans ce cas de figure, les utilisateurs distants et du réseau local sont continuellement évalués, et l'application est fournie à la fois aux utilisateurs distants et à ceux du réseau local.

Remarque: ce cas de figure aide à déterminer les utilisateurs qui n'exécutent pas l'agent. Étant donné que tous les utilisateurs exécutent l'agent de quarantaine, les utilisateurs sans agent sont détectés par le concentrateur à accès distant.

Utilisateur	Type d'agent	Application	Matériel réseau
Utilisateurs distants avec agent	Agent de quarantaine	Application de l'agent et application RADIUS	Concentrateur à accès distant
Utilisateurs distants sans agent	Aucun	Application RADIUS	Concentrateur à accès distant
Utilisateurs du réseau local	Agent de quarantaine	Application de l'agent	Aucun

Stratégie en mode Enforce

Les profils suivants figurent dans la stratégie :

- **Windows XP operating system profile:** nécessite que Windows XP et les service packs appropriés soient installés.
- **Internet Explorer 8.x patch profile:** nécessite que tous les correctifs de sécurité Internet Explorer 8.x soient installés.
- **Sophos Anti-Virus 9.x profile:** nécessite que Sophos Anti-Virus 9.x soit installé, que la protection en temps réel soit activée, que le fichier signature soit mis à jour dans les 5 jours et que la version du logiciel soit supérieure ou égale à 9.
- **Sophos Client Firewall 2.x profile:** nécessite que Sophos Client Firewall soit installé, activé et que la version du logiciel soit supérieure ou égale à 2.

État de conformité	Modèle d'accès	Action
<p>Conforme</p> <ul style="list-style-type: none"> ■ Windows XP et les services packs sont installés. ■ Les correctifs de sécurité Internet Explorer 8.x sont installés. ■ Sophos Anti-Virus 9.x est installé, la protection en temps réel est activée et le fichier signature est mis à jour tous les 5 jours. ■ Sophos Client Firewall 2.x est installé et activé. 	<p>Utilisateurs distants avec agent</p> <ul style="list-style-type: none"> ■ Le modèle d'accès Agent Enforcer autorise l'accès réseau. ■ Le modèle d'accès RADIUS Enforcer autorise l'accès réseau. <p>Utilisateurs du réseau local avec agent</p> <ul style="list-style-type: none"> ■ Le modèle d'accès Agent Enforcer autorise l'accès réseau. 	Aucune action n'est nécessaire.
<p>Partiellement conforme</p> <ul style="list-style-type: none"> ■ Windows XP et les services packs sont installés. ■ Les correctifs de sécurité Internet Explorer 8.x sont installés. ■ Sophos Anti-Virus 9.x est installé, la protection en temps réel est activée, mais le fichier signature est obsolète. ■ Sophos Client Firewall 2.x est installé et activé. 	<p>Utilisateurs distants avec agent</p> <ul style="list-style-type: none"> ■ Le modèle d'accès Agent Enforcer autorise l'accès réseau. ■ Le modèle d'accès RADIUS Enforcer autorise l'accès réseau. <p>Utilisateurs du réseau local avec agent</p> <ul style="list-style-type: none"> ■ Le modèle d'accès Agent Enforcer autorise l'accès réseau. 	Un message indique aux utilisateurs que le logiciel va mettre à jour le fichier signature Sophos Anti-Virus. Le logiciel met automatiquement à jour le fichier signature Sophos Anti-Virus.
<p>Non conforme</p> <ul style="list-style-type: none"> ■ Windows XP et les services packs sont installés. 	<p>Utilisateurs distants avec agent</p> <ul style="list-style-type: none"> ■ Le modèle d'accès Agent Enforcer place les 	<p>Utilisateurs avec agent</p> <ul style="list-style-type: none"> ■ Un message indique aux utilisateurs qu'il leur

État de conformité	Modèle d'accès	Action
<ul style="list-style-type: none"> ■ Certains des correctifs de sécurité Internet Explorer 8.x sont installés et d'autres ne le sont pas. ■ Sophos Anti-Virus 9.x est installé, mais la protection en temps réel est désactivée et le fichier signature n'est pas à jour. ■ Sophos Client Firewall 2.x est installé, mais n'est pas activé. 	<p>utilisateurs en quarantaine et autorise seulement l'accès à Internet et au serveur de correction de l'entreprise. L'accès Internet permet la mise à jour de la signature antivirus. L'accès au serveur de correction permet de télécharger les correctifs Internet Explorer.</p> <ul style="list-style-type: none"> ■ Le modèle d'accès RADIUS Enforcer autorise l'accès réseau <p>Utilisateurs du réseau local avec agent</p> <ul style="list-style-type: none"> ■ Le modèle d'accès Agent Enforcer place les utilisateurs en quarantaine et autorise seulement l'accès à Internet et au serveur de correction de l'entreprise. L'accès Internet permet la mise à jour de la signature antivirus. L'accès au serveur de correction permet de télécharger les correctifs Internet Explorer. 	<p>manque des correctifs Internet Explorer nécessaires et propose un lien vers le serveur de correction de l'entreprise.</p> <ul style="list-style-type: none"> ■ Un message indique aux utilisateurs que le logiciel va mettre à jour le fichier signature Sophos Anti-Virus. Le logiciel met automatiquement à jour le fichier signature Sophos Anti-Virus. ■ Un message indique aux utilisateurs que le logiciel va activer la protection en temps réel Sophos Anti-Virus. Le logiciel active automatiquement la protection en temps réel Sophos Anti-Virus. ■ Un message indique aux utilisateurs que le logiciel va activer Sophos Client Firewall. Le logiciel active automatiquement Sophos Client Firewall.
<p>Inconnu</p> <p>La conformité est inconnue car l'agent n'est pas installé et aucune évaluation n'a été exécutée.</p>	<p>Utilisateurs distants sans agent</p> <ul style="list-style-type: none"> ■ Le modèle d'accès RADIUS Enforcer spécifie que le concentrateur à accès distant refuse l'accès réseau. 	<p>Utilisateurs distants sans agent</p> <ul style="list-style-type: none"> ■ Aucune action n'est exécutée car l'agent n'est pas installé.

8.3 Création d'une stratégie pour utiliser la mise en application de l'agent, de RADIUS et de DHCP

Dans ce cas de figure, les utilisateurs distants et du réseau local sont continuellement évalués, et la mise en application est fournie à la fois aux utilisateurs distants et à ceux du réseau local.

Remarque : ce cas de figure aide à déterminer les utilisateurs non autorisés. Étant donné que tous les utilisateurs exécutent l'agent de quarantaine, les utilisateurs non autorisés sont détectés par le serveur DHCP. Ce cas de figure nécessite l'utilisation d'un DHCP Enforcer.

Utilisateur	Type d'agent	Type de mise en application	Matériel réseau
Utilisateurs distants avec agent	Agent de quarantaine	Mise en application de l'agent et de RADIUS	Concentrateur à accès distant
Utilisateurs distants sans agent	Aucun	Mise en application de RADIUS	Concentrateur à accès distant
Utilisateurs du réseau local avec agent	Agent de quarantaine	Mise en application de l'agent et du protocole DHCP	Serveur DHCP
Utilisateurs du réseau local sans agent	Aucun	Mise en application du protocole DHCP	Serveur DHCP

Stratégie en mode Enforce

Les profils suivants figurent dans la stratégie :

- **Windows XP operating system profile:** nécessite que Windows XP et les service packs appropriés soient installés.
- **Sophos Anti-Virus 9.x profile:** nécessite que Sophos Anti-Virus 9.x soit installé, que la protection en temps réel soit activée, que le fichier signature soit mis à jour dans les 5 jours et que la version du logiciel soit supérieure ou égale à 9.
- **Sophos Client Firewall 2.x profile:** nécessite que Sophos Client Firewall soit installé, activé et que la version du logiciel soit supérieure ou égale à 2.

État de conformité	Modèle d'accès	Action
<p>Conforme</p> <ul style="list-style-type: none"> ■ Windows XP et les services packs sont installés. ■ Sophos Anti-Virus 9.x est installé, la protection en temps réel est activée et le fichier signature est mis à jour tous les 5 jours. ■ Sophos Client Firewall 2.x est installé et activé. 	<p>Utilisateurs distants avec agent</p> <ul style="list-style-type: none"> ■ Le modèle d'accès Agent Enforcer autorise l'accès réseau. ■ Le modèle d'accès RADIUS Enforcer autorise l'accès réseau. <p>Utilisateurs du réseau local avec agent</p> <ul style="list-style-type: none"> ■ Le modèle d'accès Agent Enforcer autorise l'accès réseau. ■ Le modèle d'accès DHCP Enforcer autorise l'accès réseau. 	Aucune action n'est nécessaire.

État de conformité	Modèle d'accès	Action
<p>Partiellement conforme</p> <ul style="list-style-type: none"> ■ Windows XP et les services packs sont installés. ■ Sophos Anti-Virus 9.x est installé, la protection en temps réel est activée, mais le fichier signature est obsolète. ■ Sophos Client Firewall 2.x est installé et activé. 	<p>Utilisateurs distants avec agent</p> <ul style="list-style-type: none"> ■ Le modèle d'accès Agent Enforcer autorise l'accès réseau. ■ Le modèle d'accès RADIUS Enforcer autorise l'accès réseau. <p>Utilisateurs du réseau local avec agent</p> <ul style="list-style-type: none"> ■ Le modèle d'accès Agent Enforcer autorise l'accès réseau. ■ Le modèle d'accès DHCP Enforcer autorise l'accès réseau. 	<ul style="list-style-type: none"> ■ Un message indique aux utilisateurs que le logiciel va mettre à jour le fichier signature de Sophos Anti-Virus. Le logiciel met automatiquement à jour le fichier signature de Sophos Anti-Virus.
<p>Non conforme</p> <ul style="list-style-type: none"> ■ Windows XP et les services packs sont installés. ■ Sophos Anti-Virus 9.x est installé, mais la protection en temps réel est désactivée et le fichier signature n'est pas à jour. ■ Sophos Client Firewall 2.x est installé, mais n'est pas activé. 	<p>Utilisateurs distants avec agent</p> <ul style="list-style-type: none"> ■ Le modèle d'accès Agent Enforcer place les utilisateurs en quarantaine et autorise seulement l'accès à Internet et au serveur de correction de l'entreprise. L'accès Internet permet la mise à jour de la signature antivirus. ■ Le modèle d'accès RADIUS Enforcer autorise l'accès réseau. <p>Utilisateurs du réseau local avec agent</p> <ul style="list-style-type: none"> ■ Le modèle d'accès Agent Enforcer place les utilisateurs en quarantaine et autorise seulement l'accès à Internet et au serveur de correction de l'entreprise. L'accès Internet permet la mise à jour de la signature antivirus. 	<ul style="list-style-type: none"> ■ Un message indique aux utilisateurs que le logiciel va mettre à jour le fichier signature de Sophos Anti-Virus. Le logiciel met automatiquement à jour le fichier signature de Sophos Anti-Virus. ■ Un message indique aux utilisateurs que le logiciel va activer la protection en temps réel de Sophos Anti-Virus. Le logiciel active automatiquement la protection en temps réel de Sophos Anti-Virus. ■ Un message indique aux utilisateurs que le logiciel va activer Sophos Client Firewall. Le logiciel active automatiquement Sophos Client Firewall.

État de conformité	Modèle d'accès	Action
	<ul style="list-style-type: none">■ Le modèle d'accès DHCP Enforcer autorise l'accès réseau.	
<p>Inconnu</p> <p>La conformité est inconnue car l'agent n'est pas installé et aucune évaluation n'a été exécutée.</p>	<p>Utilisateurs distants sans agent</p> <ul style="list-style-type: none">■ Le modèle d'accès RADIUS Enforcer spécifie que le concentrateur à accès distant refuse l'accès réseau. <p>Utilisateurs du réseau local sans agent</p> <ul style="list-style-type: none">■ Le modèle d'accès DHCP Enforcer spécifie que le serveur DHCP refuse l'accès réseau.	<p>Utilisateurs distants ou du réseau local sans agent</p> <ul style="list-style-type: none">■ Aucune action n'est exécutée car l'agent n'est pas installé.

9 Support technique

Vous pouvez obtenir du support technique pour les produits Sophos de l'une des manières suivantes :

- Rendez-vous sur le forum de la communauté SophosTalk en anglais sur <http://community.sophos.com/> et recherchez d'autres utilisateurs rencontrant le même problème que le vôtre.
- Rendez-vous sur la base de connaissances du support de Sophos sur <http://www.sophos.fr/support/>.
- Téléchargez la documentation des produits sur <http://www.sophos.fr/support/docs/>.
- Envoyez un courriel à support@sophos.fr, y compris le ou les numéros de version du logiciel Sophos, le ou les systèmes d'exploitation et le ou les niveaux de correctif ainsi que le texte du ou des messages d'erreur.

10 Mentions légales

Copyright © 2011 Sophos Limited. 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.

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