

**SOPHOS**

---

simple + secure

# Sophos Enterprise Manager Aide

Version du produit : 4.7

Date du document : juillet 2011



## Table des matières

1	À propos de Sophos Enterprise Manager.....	3
2	Guide de l'interface d'Enterprise Manager.....	4
3	Introduction.....	13
4	Configuration d'Enterprise Manager.....	15
5	Protection des ordinateurs.....	32
6	Mise à jour des ordinateurs.....	47
7	Configuration des stratégies.....	63
8	Paramétrage des alertes et des messages.....	121
9	Génération de rapports.....	131
10	Copie ou impression des données depuis Enterprise Manager.....	143
11	Résolution des problèmes.....	145
12	Glossaire.....	152
13	Support technique.....	155
14	Mentions légales.....	156

# 1 À propos de Sophos Enterprise Manager

Sophos Enterprise Manager, version 4.7, est une console automatisée qui déploie et gère de manière centralisée les logiciels de sécurité Sophos sur les ordinateurs Windows, Mac et Linux. Enterprise Manager vous permet de :

- Protéger votre réseau contre les virus, chevaux de Troie, vers, spywares, sites Web malveillants et autres menaces inconnues, et contre les adwares et autres applications potentiellement indésirables.
- Administrer la protection du pare-feu client sur les ordinateurs d'extrémité.
- Empêcher l'utilisation de périphériques de stockage externes non autorisés et de technologies de connexion sans fil sur des ordinateurs d'extrémité.
- Empêcher l'utilisateur de reconfigurer, désactiver ou désinstaller les logiciels de sécurité Sophos.

Pour en savoir plus sur ce qui fait la différence entre l'Enterprise Manager et ses licences et les autres produits Sophos et leurs licences, consultez l'article 113711 de la base de connaissances du support de Sophos (<http://www.sophos.fr/support/knowledgebase/article/113711.html>).

## 2 Guide de l'interface d'Enterprise Manager

### 2.1 Agencement de l'interface utilisateur

L'interface utilisateur d'Enterprise Manager comporte les zones suivantes :

#### Barre d'outils

La barre d'outils contient des raccourcis vers les commandes les plus utilisées pour l'utilisation et la configuration de votre logiciel de sécurité Sophos.

Pour plus d'informations, reportez-vous à la section [Boutons de la barre d'outils](#) à la page 5.

#### Tableau de bord

Le **Tableau de bord** donne un aperçu rapide de l'état de la sécurité du réseau.

Pour plus d'informations, consultez [Volets du Tableau de bord](#) à la page 7.

#### Liste des ordinateurs

La liste des ordinateurs apparaît en bas à droite. Elle comporte deux vues :

- La vue **Ordinateurs d'extrémité** affiche les ordinateurs du groupe sélectionné dans le volet **Groupes** en bas à gauche. Pour plus d'informations, consultez [Navigation dans la vue Ordinateurs d'extrémité](#) à la page 9.
- La vue **Gestionnaires de mise à jour** affiche l'ordinateur sur lequel Sophos Update Manager est installé. Pour plus d'informations, consultez [Navigation dans la vue Gestionnaires de mise à jour](#) à la page 11.

La capture d'écran ci-dessous montre la liste des ordinateurs dans la vue **Ordinateurs d'extrémité**.

The screenshot shows the Sophos Enterprise Manager interface. At the top, there's a menu bar with options like 'Fichier', 'Edition', 'Affichage', 'Actions', 'Groupes', 'Stratégies', 'Abonnements', 'Outils', and 'Aide'. Below the menu is a toolbar with icons for 'Rechercher de nouveaux ordinateurs', 'Créer un groupe', 'Voir/modifier une stratégie', 'Protéger', 'Gestionnaires de mise à jour', and 'Tableau de bord'. The main area is divided into several sections:

- Tableau de bord:** A summary of system health with four main cards:
  - Ordinateurs:** Shows counts for Administrés (302), Non administrés (0), Connectés (242), and Tous (302).
  - Ordinateurs avec alertes:** Shows counts for Virus/spywares (100, 33%), Comportements/richiers suspects (80, 26%), and Adwares et PUA (50, 17%).
  - Stratégies:** Shows 'Ordinateurs qui diffèrent de la stratégie' (26, 9%).
  - Protection:** Shows 'Ordinateurs non à jour' (52, 17%).
  - Erreurs:** Shows 'Ordinateurs avec des erreurs' (48, 16%).
- Mises à jour:** A card indicating the last update was on Monday, July 4, 2011, at 09:06.
- Ordinateurs dépassant le seuil d'un événement:** Shows 'Contrôle des périphériques' (1) and 'Pare-feu' (1).
- Groupes:** A tree view on the left showing a hierarchy: VPC-WIN2K3-REX > Non affectés > Boston, Oxford, Sydney.
- Stratégies:** A tree view on the left showing: Mise à jour > Antivirus et HIPS > Par défaut > SAV-1 > Pare-feu > Contrôle des périphériques > Protection anti-télération.
- Main Table:** A table listing individual computers with columns for 'Nom de l'ordinateur', 'Conformité à la stratégie', 'À jour', 'Alertes et erreurs', 'Sur accès', 'Pare-feu activé', and 'Contrôle de...'. It lists various computer names and their current status regarding updates, alerts, and security.

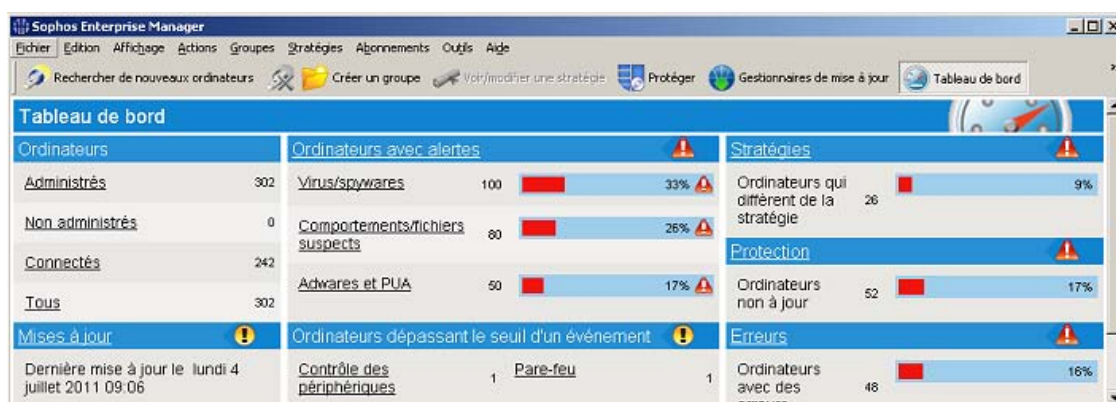
## 2.2 Boutons de la barre d'outils

Le tableau suivant décrit les boutons de la barre d'outils. Certains boutons de la barre d'outils sont disponibles seulement dans des circonstances spécifiques. Par exemple, le bouton **Protéger** pour installer les logiciels antivirus et de pare-feu est seulement disponible si un groupe d'ordinateurs est sélectionné dans le volet **Groupes** de la vue **Ordinateurs d'extrémité**.

Bouton de la barre d'outils	Description
<b>Rechercher de nouveaux ordinateurs</b>	Recherche des ordinateurs sur le réseau et les ajoute à la console. Pour plus d'informations, reportez-vous à la section <a href="#">Sélection de la méthode de recherche des ordinateurs</a> à la page 28 et aux autres rubriques de la section <i>Paramétrage d'Enterprise Manager &gt; Recherche d'ordinateurs sur le réseau</i> .
<b>Créer un groupe</b>	Crée un nouveau groupe pour les ordinateurs. Pour plus d'informations, reportez-vous à la section <a href="#">Création d'un groupe</a> à la page 20.

Bouton de la barre d'outils	Description
<b>Voir/Modifier une stratégie</b>	<p>Ouvre la stratégie sélectionnée dans le volet <b>Stratégies</b> en vue d'une modification.</p> <p>Pour plus d'informations, reportez-vous à la section <a href="#">Modification d'une stratégie</a> à la page 26.</p>
<b>Protéger</b>	<p>Installe les logiciels antivirus et de pare-feu sur les ordinateurs sélectionnés dans la liste des ordinateurs.</p> <p>Pour plus d'informations, reportez-vous à la section <a href="#">Protection des ordinateurs</a> à la page 34.</p>
<b>Ordinateurs d'extrémité</b>	<p>Change pour la vue <b>Ordinateurs d'extrémité</b> dans la liste des ordinateurs.</p> <p>La vue <b>Ordinateurs d'extrémité</b> affiche les ordinateurs du groupe qui est sélectionné dans le volet <b>Groupes</b>.</p> <p>Pour plus d'informations, reportez-vous à la section <a href="#">Navigation dans la vue Ordinateurs d'extrémité</a> à la page 9.</p>
<b>Gestionnaires de mise à jour</b>	<p>Passes à la vue <b>Gestionnaires de mise à jour</b> dans la liste des ordinateurs.</p> <p>La vue <b>Gestionnaires de mise à jour</b> affiche l'ordinateur sur lequel Sophos Update Manager est installé.</p> <p>Pour plus d'informations, reportez-vous à la section <a href="#">Navigation dans la vue Gestionnaires de mise à jour</a> à la page 11.</p>
<b>Tableau de bord</b>	<p>Affiche ou masque le <b>Tableau de bord</b>.</p> <p>Le <b>Tableau de bord</b> donne un aperçu rapide de l'état de la sécurité de votre réseau.</p> <p>Pour plus d'informations, reportez-vous à la section <a href="#">Volets du Tableau de bord</a> à la page 7.</p>
<b>Rapports</b>	<p>Démarre le <b>Gestionnaire des rapports</b> de manière à ce que vous puissiez générer des rapports sur les alertes et sur les événements sur votre réseau.</p> <p>Pour plus d'informations, reportez-vous à la section <a href="#">À propos des rapports</a> à la page 131 et aux autres rubriques de la section <i>Génération de rapports</i>.</p>

## 2.3 Volets du Tableau de bord






Le **Tableau de bord** contient les volets suivants :

Volet du Tableau de bord	Description
<b>Ordinateurs</b>	Indique le nombre total d'ordinateurs sur le réseau ainsi que le nombre d'ordinateurs connectés, administrés et non administrés.  Pour voir une liste des ordinateurs administrés, non administrés, connectés ou de tous les ordinateurs, cliquez sur l'un des liens de la zone <b>Ordinateurs</b> .
<b>Mises à jour</b>	Indique l'état du gestionnaire de mise à jour.
<b>Ordinateurs avec alertes</b>	Indique le nombre et le pourcentage d'ordinateurs administrés avec des alertes concernant : <ul style="list-style-type: none"> <li>■ Des virus et des spywares connus et inconnus</li> <li>■ Des comportements et fichiers suspects</li> <li>■ Des adwares et autres applications potentiellement indésirables</li> </ul> Pour voir une liste des ordinateurs administrés avec des alertes à traiter, cliquez sur le titre du volet <b>Ordinateurs avec alertes</b> .
<b>Ordinateurs au-dessus du seuil</b>	Indique le nombre d'ordinateurs avec des événements au-dessus du seuil au cours des sept derniers jours.  Pour consulter une liste des ordinateurs avec des événements de contrôle des périphériques ou de pare-feu, cliquez sur un lien dans le volet <b>Ordinateurs dépassant le seuil d'un événement</b> .
<b>Stratégies</b>	Indique le nombre et le pourcentage d'ordinateurs administrés avec violations de leur stratégie de groupe ou erreurs de comparaison de stratégie. Il inclut aussi les ordinateurs qui n'ont pas encore répondu à la stratégie modifiée que leur a transmis la console.  Pour voir une liste des ordinateurs administrés qui diffèrent de la stratégie, cliquez sur le titre du volet <b>Stratégies</b> .

Volet du Tableau de bord	Description
<b>Protection</b>	Indique le nombre et le pourcentage d'ordinateurs administrés et connectés sur lesquels Sophos Endpoint Security and Control ou Sophos Anti-Virus est obsolète ou utilise des données de détection inconnues.  Pour voir une liste des ordinateurs administrés connectés et non à jour, cliquez sur le titre du volet <b>Protection</b> .
<b>Erreurs</b>	Indique le nombre et le pourcentage d'ordinateurs administrés ayant des erreurs de contrôle, de mise à jour ou de pare-feu à traiter.  Pour voir une liste des ordinateurs administrés avec des erreurs de produits Sophos à traiter, cliquez sur le titre du volet <b>Erreurs</b> .

## 2.4 Icônes d'état de la sécurité

Le tableau ci-dessous vous indique la signification des icônes d'état de la sécurité qui apparaissent dans le **Tableau de bord** et dans la barre d'état d'Enterprise Manager.

Icônes d'état de la sécurité	Description
	<b>Normal</b> Le nombre d'ordinateurs affectés est en dessous du niveau d'alerte.
	<b>Warning</b> Le niveau d'alerte a été dépassé.
	<b>Critique</b> Le niveau critique a été dépassé.

### Icônes d'état de fonctionnement d'un volet du Tableau de bord

Une icône d'état de fonctionnement d'un volet du **Tableau de bord** s'affiche dans le coin supérieur droit d'un volet du Tableau de bord. Elle affiche l'état d'une zone de sécurité spécifique représentée par le volet.

Une icône d'état de fonctionnement d'un volet du **Tableau de bord** affiche l'état d'une icône du volet ayant l'état le plus sérieux, c'est-à-dire :

- Une icône d'état de fonctionnement d'un volet passe de l'état **Normal** à l'état **Alerte** lorsque le niveau d'alerte est dépassé pour au moins une icône du volet.
- Une icône d'état d'un volet passe de l'état "Alerte" à l'état "Critique" lorsque le seuil critique est dépassé pour au moins une icône du volet.

## L'icône d'état de fonctionnement du réseau

L'icône d'état de fonctionnement du réseau apparaît sur le côté droit de la barre d'état d'Enterprise Manager. Elle affiche l'état de sécurité général de votre réseau.

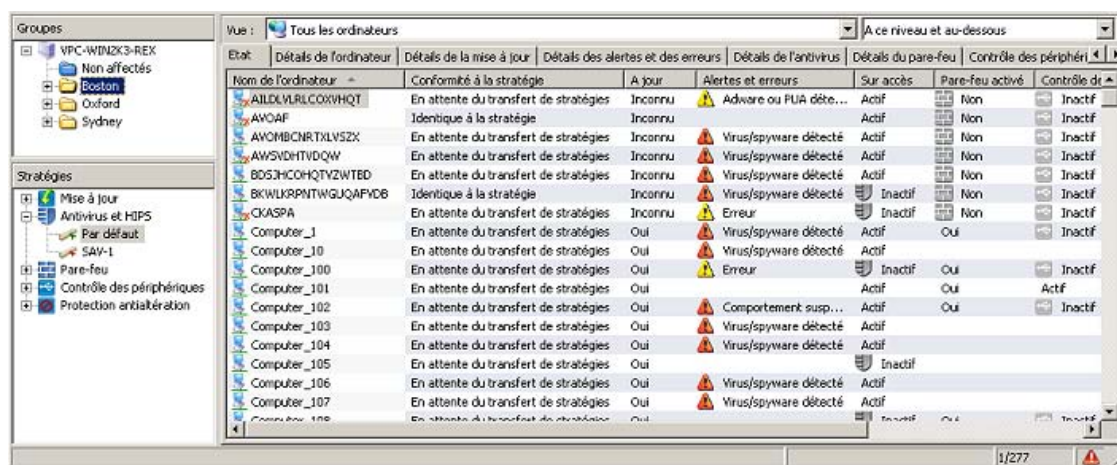
L'icône d'état de fonctionnement du réseau affiche l'état du volet du **Tableau de bord** ayant l'état le plus sérieux, c'est-à-dire :

- L'icône d'état de fonctionnement du réseau passe de l'état **Normal** à l'état **Alerte** lorsque le niveau d'alerte est dépassé pour au moins une icône du **Tableau de bord**.
- L'icône d'état de fonctionnement du réseau passe de l'état **Alerte** à l'état **Critique** lorsque le niveau critique est dépassé pour au moins une icône du **Tableau de bord**.

À la première installation ou mise à niveau d'Enterprise Manager, le **Tableau de bord** utilise les niveaux d'alerte et critique par défaut. Pour configurer vos propres niveaux d'alerte ou critique, reportez-vous à la section [Configuration du Tableau de bord](#) à la page 36.

Vous pouvez aussi configurer l'envoi des alertes par courriel aux destinataires de votre choix lorsqu'un niveau d'alerte ou critique a été dépassé pour un volet du **Tableau de bord**. Pour plus d'instructions, reportez-vous à la section [Configuration des alertes par courriel sur l'état du réseau](#) à la page 125.

## 2.5 Navigation dans la vue Ordinateurs d'extrémité



### Liste des ordinateurs

Dans la vue **Ordinateurs d'extrémité**, la liste des ordinateurs affiche les ordinateurs d'extrémité du groupe sélectionné dans le volet **Groupes**.


Cette vue comporte un certain nombre d'onglets. L'onglet **Etat** indique si les ordinateurs sont protégés par le contrôle sur accès, s'ils sont conformes aux stratégies de leur groupe, quelles fonctions sont activées et si les logiciels sont à jour. Cet onglet indique aussi la présence d'alertes. Les autres onglets fournissent des informations plus détaillées sur chacun de ces sujets.

Pour plus d'explications concernant les icônes affichées dans la liste des ordinateurs, reportez-vous à la section [Icônes de la liste des ordinateurs](#) à la page 10.


Vous pouvez copier ou imprimer les données affichées dans la liste des ordinateurs. Pour plus d'informations, reportez-vous à la section [Copie de données depuis la liste des ordinateurs](#) à

la page 143 et aux autres rubriques de la section *Copie ou impression des données depuis Enterprise Manager*.

### Volet Groupes

Dans le volet **Groupes**, créez des groupes  et placez-y les ordinateurs en réseau. Vous pouvez créer des groupes vous-même ou importer des conteneurs Active Directory, avec ou sans ordinateurs, et les utiliser comme groupes d'ordinateurs d' Enterprise Manager.

Pour plus d'informations, reportez-vous à la section [À quoi servent les groupes ?](#) à la page 19 et autres rubriques de la section *Paramétrage d'Enterprise Manager > Création et utilisation de groupes*.

Le groupe **Non affectés**  est destiné aux ordinateurs qui n'appartiennent pas encore à un groupe que vous avez créé.



### Volet Stratégies

Dans le volet **Stratégies**, vous créez et configurez les stratégies appliquées aux groupes d'ordinateurs. Pour de plus amples informations, reportez-vous aux éléments suivants :

- [À propos des stratégies](#) à la page 23 et autres rubriques de la section *Paramétrage d'Enterprise Manager > Création et utilisation de stratégies*
- La section *Configuration des stratégies*

## 2.6 Icônes de la liste des ordinateurs




### Alertes

Icône	Explication
	L'apparition d'un signal d'avertissement rouge dans la colonne <b>Alertes et erreurs</b> de l'onglet <b>Etat</b> signifie qu'un virus, un ver, un cheval de Troie, un spyware ou un comportement suspect a été détecté.
	<p>L'apparition d'un signal d'avertissement jaune dans la colonne <b>Alertes et erreurs</b> de l'onglet <b>Etat</b> indique l'un des problèmes suivants :</p> <ul style="list-style-type: none"> <li>■ Un fichier suspect a été détecté.</li> <li>■ Un adware ou toute autre application potentiellement indésirable a été détecté.</li> <li>■ Une erreur s'est produite.</li> </ul> <p>L'apparition d'un signal d'avertissement jaune dans la colonne <b>Conforme à la stratégie</b> indique que l'ordinateur n'utilise pas la même stratégie ou les mêmes stratégies que les autres ordinateurs de son groupe.</p>







S'il y a plusieurs alertes ou erreurs sur un ordinateur, l'icône de l'alerte ayant la priorité la plus haute apparaît dans la colonne **Alertes et erreurs**. Les types d'alertes sont répertoriés ci-dessous par ordre de priorité décroissant.

1. Alertes de virus et spyware
2. Alertes de comportement suspect
3. Alertes de fichier suspect
4. Alertes d'adware et PUA
5. Erreurs d'applications logicielles (par exemple, erreurs d'installation)

### Protection désactivée ou non à jour

Icône	Explication
	Un bouclier gris signifie que le contrôle sur accès est inactif.
	Un symbole affichant un pare-feu gris signifie que le pare-feu est désactivé.
	Une icône d'horloge signifie que le logiciel n'est pas à jour.

### État de l'ordinateur

Icône	Explication
	Un ordinateur bleu signifie que l'ordinateur est administré par Enterprise Manager.
	Un ordinateur surmonté d'une flèche jaune signifie que l'installation des logiciels antivirus et de pare-feu est en attente.
	Un ordinateur surmonté d'une flèche verte signifie que l'installation est en cours.
	Un ordinateur surmonté d'un sablier signifie que le composant de mise à jour automatique du logiciel de sécurité pour postes d'extrémité a été installé et qu'il est désormais en train de télécharger la version la plus récente du produit.
	Un ordinateur gris signifie que l'ordinateur n'est pas administré par Enterprise Manager.
	Un ordinateur près duquel se trouve une croix rouge signifie que l'ordinateur habituellement administré par Enterprise Manager est déconnecté du réseau (les ordinateurs non connectés et non administrés ne sont pas affichés).

## 2.7 Navigation dans la vue Gestionnaires de mise à jour

Abonnements logiciels		Gestionnaires de mise à jour							
Ajouter		Nom de l'ordinateur	Alertes	Erreurs	Dernière mise à jour	Etat du téléchargement	Configuration	Version	N
Recommandée		VPC-WIN2K3-REX		Echec de la mise à jour ...	04/07/2011 09:06:31	Dernière vérification à : 06/07/...	Correspondante	1.2.1.160	1
SUB-1									

### **Liste des ordinateurs**

Dans la vue **Gestionnaires de mise à jour**, paramétrez la mise à jour automatique des logiciels de sécurité Sophos depuis le site Web Sophos et consultez l'état et les détails du gestionnaire de mise à jour.

La liste des ordinateurs affiche l'ordinateur sur lequel Sophos Update Manager est installé.

### **Abonnements logiciels**

Utilisez le volet **Abonnements logiciels** pour créer ou modifier les abonnements aux logiciels qui spécifient quelles versions des logiciels pour ordinateurs d'extrémité sont téléchargées depuis Sophos pour chaque plate-forme.

## 3 Introduction

Voici un aperçu des tâches à exécuter pour protéger votre réseau suite à l'installation de l'Enterprise Manager et après avoir effectué toutes les étapes de l'**Assistant de téléchargement des logiciels de sécurité**. Pour plus d'informations sur l'utilisation de l'Enterprise Manager, reportez-vous aux documents et sections mentionnés.

Nous vous conseillons de consulter le *Guide de configuration des stratégies de Sophos Enterprise Manager* pour obtenir des conseils sur l'utilisation et l'administration des logiciels de sécurité Sophos. La documentation Sophos est disponible sur <http://www.sophos.fr/support/docs/>.

Si vous n'avez pas terminé l'**Assistant de téléchargement des logiciels de sécurité**, reportez-vous à la section [Exécution de l'Assistant de téléchargement des logiciels de sécurité](#) à la page 55.

Pour protéger votre réseau, suivez les étapes suivantes :

### 1. Création de groupes.

Vous pouvez créer des groupes vous-même, un par un, ou importer des conteneurs Active Directory, avec ou sans ordinateurs, et les utiliser comme groupes d'ordinateurs de l'Enterprise Manager.

Si vous voulez importer des conteneurs Active Directory, reportez-vous à la section [Importation de conteneurs et d'ordinateurs depuis Active Directory](#) à la page 28. Nous vous conseillons de commencer par importer des conteneurs à partir d'Active Directory sans ordinateurs, puis d'affecter des stratégies de groupe aux groupes, et enfin d'ajouter des ordinateurs aux groupes.

Pour plus d'informations sur la création manuelle de groupes, reportez-vous à la section [À quoi servent les groupes ?](#) à la page 19 et aux autres rubriques de la sous-section *Création et utilisation de groupes* sous la section *Configuration de l'Enterprise Manager*.

### 2. Configuration des stratégies.

L'Enterprise Manager dispose d'une série de stratégies par défaut qui sont essentielles au maintien de la protection du réseau. Les stratégies de **Mise à jour** et les stratégies **Antivirus et HIPS** sont prêtes à l'emploi. Pour configurer la stratégie de pare-feu, lancez l'assistant de **Stratégie de pare-feu**. Reportez-vous à la section [Configuration d'une stratégie de pare-feu](#) à la page 80.

### 3. Recherche de nouveaux ordinateurs sur le réseau et ajout à la console.

Si vous avez importé des conteneurs et des ordinateurs depuis Active Directory à l'étape 1, aucune autre opération n'est nécessaire. Autrement, reportez-vous à la section [Sélection de la méthode de recherche des ordinateurs](#) à la page 28 et aux autres rubriques de la sous-section *Recherche d'ordinateurs sur le réseau* sous la section *Configuration de l'Enterprise Manager*.

### 4. Protection des ordinateurs.

Lorsque vous faites glisser un ordinateur depuis le groupe **Non affectés** et le déposez dans un autre groupe, un assistant se lance pour vous aider à protéger les ordinateurs. Reportez-vous à la section [Protection des ordinateurs](#) à la page 34 et aux autres rubriques de la section *Protection des ordinateurs*.

5. Vérification de la protection des ordinateurs.

Une fois l'installation terminée, consultez de nouveau la liste des ordinateurs dans le nouveau groupe. Dans la colonne **Sur accès**, vous devriez voir apparaître le mot *Actif* : ceci signifie que l'ordinateur est protégé par le contrôle sur accès et qu'il est désormais géré par l'Enterprise Manager. Pour plus d'informations, reportez-vous à la section [Comment m'assurer que mon réseau est protégé ?](#) à la page 36.

6. Nettoyage des ordinateurs.

En cas de détection d'un virus, d'une application indésirable ou de tout autre problème sur votre réseau, procédez au nettoyage des ordinateurs affectés comme le décrit la section [Nettoyage immédiat des ordinateurs](#) à la page 43.

### Options de protection et d'administration supplémentaires

Par défaut, Sophos Endpoint Security and Control détecte virus, chevaux de Troie, vers et spywares et analyse le comportement des programmes fonctionnant sur le système. Vous pouvez ajouter une protection supplémentaire, par exemple contre les adwares, contre les applications potentiellement indésirables (PUA), les comportements suspects ou indésirables ou encore la perte accidentelle de données depuis les stations de travail. Pour plus de détails, reportez-vous aux sections suivantes :

- [Contrôle à la recherche des fichiers suspects](#) à la page 65
- [Recherche d'adwares et de PUA](#) à la page 68
- [À propos du contrôle des périphériques](#) à la page 111
- [À propos de la protection antialtération](#) à la page 118

Vous pouvez paramétrer l'accès délégué à Enterprise Manager en affectant les utilisateurs et les groupes Windows aux quatre rôles préconfigurés - Administrateur système, Administrateur, Service d'assistance et Invité. Le rôle de l'administrateur système qui inclut le groupe Windows Sophos Full Administrators dispose des droits complets et ne nécessite aucun paramétrage. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

## 4 Configuration d'Enterprise Manager

### 4.1 Gestion des rôles

#### 4.1.1 À propos des rôles

**Important :** si vous avez déjà utilisé l'administration déléguée, vous devez disposer du droit **Administration déléguée** pour configurer les rôles. Le rôle de l'administrateur système qui inclut le groupe Windows Sophos Full Administrators dispose des droits complets et ne nécessite aucun paramétrage. Pour plus d'informations, reportez-vous aux sections [Que sont les rôles préconfigurés ?](#) à la page 15 et [Quelles tâches les droits autorisent-ils ?](#) à la page 16.

Vous pouvez paramétrer l'accès délégué à la console en affectant des utilisateurs et des groupes Windows aux rôles de la console. Par exemple, un ingénieur du support technique peut mettre à jour ou nettoyer des ordinateurs, mais ne peut pas configurer des stratégies, car il s'agit d'une opération relevant de la responsabilité d'un administrateur.

Pour ouvrir Enterprise Manager, un utilisateur doit être membre du groupe Sophos Console Administrators et être affecté au moins à un rôle Enterprise Manager. Les membres du groupe Sophos Full Administrators ont un accès complet à Enterprise Manager.

**Remarque :** si vous voulez autoriser un utilisateur à utiliser un Enterprise Manager à distance ou supplémentaire, reportez-vous à la section [Comment un autre utilisateur peut-il utiliser Enterprise Manager ?](#) à la page 19.

Vous pouvez modifier et utiliser des rôles préconfigurés, mais vous ne pouvez pas créer vos propres rôles.

Vous pouvez affecter à un utilisateur autant de rôles que vous le souhaitez, en ajoutant aux rôles l'utilisateur individuel ou un groupe Windows auquel l'utilisateur appartient.

Si un utilisateur ne dispose pas du droit d'effectuer une certaine tâche dans la console, il peut toutefois visualiser les paramètres de configuration appartenant à cette tâche. Un utilisateur à qui aucun rôle n'est affecté ne peut pas ouvrir Enterprise Manager.

#### 4.1.2 Que sont les rôles préconfigurés ?

Il existe quatre rôles préconfigurés dans Enterprise Manager. Les rôles peuvent être modifiés, mais ils ne peuvent pas être renommés ou supprimés.

Rôle	Description
Administrateur système	Rôle préconfiguré disposant des droits complets d'administration des logiciels de sécurité Sophos sur le réseau et des rôles dans Enterprise Manager.
Administrateur	Rôle préconfiguré disposant des droits d'administration des logiciels de sécurité Sophos sur le réseau mais ne pouvant pas administrer les rôles dans Enterprise Manager.

Rôle	Description
Service d'assistance	Rôle préconfiguré disposant uniquement des droits d'actualisation, par exemple, pour nettoyer ou mettre à jour les ordinateurs.
Invité	Rôle préconfiguré avec un accès en lecture seule à Enterprise Manager.

### 4.1.3 Modification d'un rôle

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Administration déléguée** pour réaliser cette tâche. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

1. Dans le menu **Outils**, cliquez sur **Gérer les rôles**.
2. Dans la boîte de dialogue **Gestion des rôles**, dans l'onglet **Gestion des rôles**, sélectionnez le rôle que vous voulez modifier et cliquez sur **Modifier**.

La boîte de dialogue **Modification du rôle** apparaît.

3. Dans le volet **Utilisateurs et groupes**, ajoutez les utilisateurs ou les groupes Windows au rôle ou supprimez les utilisateurs ou les groupes existants selon le cas.

### 4.1.4 Affichage des rôles d'utilisateur ou de groupe

Pour voir les rôles auxquels un utilisateur ou un groupe Windows a été attribué :

1. Dans le menu **Outils**, cliquez sur **Gérer les rôles**.
2. Dans la boîte de dialogue **Gestion des rôles**, choisissez l'onglet **Vue utilisateur et groupe** et cliquez sur le bouton **Utilisateur ou groupe**.
3. Dans la boîte de dialogue **Sélection d'un utilisateur ou d'un groupe**, sélectionnez un utilisateur ou un groupe dont vous voulez visualiser les rôles et cliquez sur **OK**.

### 4.1.5 Quelles tâches les droits autorisent-ils ?

Droit	Tâches
Recherche des ordinateurs, protection et groupes	Démarrage de la recherche, arrêt de la recherche et découverte de domaines pour la recherche sur réseau, la recherche par plage d'adresses IP et la recherche Active Directory
	Importation d'ordinateurs et de groupes depuis Active Directory ; importation de groupes depuis Active Directory
	Importation d'ordinateurs depuis un fichier
	Suppression d'un ordinateur

Droit	Tâches
	Protection d'un ordinateur Déplacement d'un ordinateur Création d'un groupe Attribution d'un nouveau nom à un groupe Déplacement d'un groupe Suppression d'un groupe Affectation d'une stratégie à un groupe
Paramétrage de stratégie - antivirus et HIPS	Création d'une stratégie antivirus et HIPS Duplication d'une stratégie antivirus et HIPS Attribution d'un nouveau nom à une stratégie antivirus et HIPS Modification d'une stratégie antivirus et HIPS Rétablissement des paramètres antivirus et HIPS par défaut Suppression d'une stratégie antivirus et HIPS Ajout ou suppression d'une entrée de la liste principale des menaces
Paramétrage de stratégie - contrôle des périphériques	Création d'une stratégie de contrôle des périphériques Duplication d'une stratégie de contrôle des périphériques Attribution d'un nouveau nom à une stratégie de contrôle des périphériques Modification d'une stratégie de contrôle des périphériques Rétablissement des paramètres de contrôle des périphériques par défaut Suppression d'une stratégie de contrôle des périphériques
Paramétrage de stratégie - pare-feu	Création d'une stratégie de pare-feu Duplication d'une stratégie de pare-feu Attribution d'un nouveau nom à une stratégie de pare-feu Modification d'une stratégie de pare-feu Rétablissement des paramètres de pare-feu par défaut Suppression d'une stratégie de pare-feu

Droit	Tâches
Paramétrage de stratégie - protection antialtération	Création d'une stratégie de protection antialtération
	Duplication d'une stratégie de protection antialtération
	Attribution d'un nouveau nom à une stratégie de protection antialtération
	Modification d'une stratégie de protection antialtération
	Rétablissement des paramètres de protection antialtération par défaut
	Suppression d'une stratégie de protection antialtération
Paramétrage de stratégie - mise à jour	Création d'une stratégie de mise à jour
	Duplication d'un stratégie de mise à jour
	Attribution d'un nouveau nom à une stratégie de mise à jour
	Modification d'une stratégie de mise à jour
	Rétablissement des paramètres de mise à jour par défaut
	Suppression d'une stratégie de mise à jour
	Création d'un abonnement
	Modification d'un abonnement
	Attribution d'un nouveau nom à un abonnement
	Duplication d'un abonnement
	Suppression d'un abonnement
	Configuration du gestionnaire de mise à jour
Actualisation - nettoyage	Nettoyage des éléments détectés
	Reconnaissance des alertes
	Reconnaissance des erreurs
Actualisation - mise à jour et contrôle	Mise à jour immédiate des ordinateurs
	Exécution d'un contrôle intégral du système d'un ordinateur
	Application de la stratégie de groupe par les ordinateurs
Configuration du rapport	Création, modification ou suppression d'un rapport
Administration déléguée	Ajout d'un utilisateur ou d'un groupe à un rôle
	Suppression d'un utilisateur ou d'un groupe depuis un rôle

Droit	Tâches
Configuration du système	Modification des paramètres du serveur SMTP ; test des paramètres du serveur SMTP ; modification des destinataires des alertes par courriel
	Configuration des seuils du tableau de bord
	Configuration des rapports : configuration de la purge des alertes de la base de données ; définition du nom de l'entreprise affiché dans les rapports

### 4.1.6 Comment un autre utilisateur peut-il utiliser Enterprise Manager ?

Les membres du groupe Sophos Full Administrators ont un accès complet à Enterprise Manager.

Vous pouvez autoriser l'utilisation d'Enterprise Manager à d'autres utilisateurs. Pour ouvrir Enterprise Manager, un utilisateur doit être :

- Membre du groupe Sophos Console Administrators.
- Affecté à au moins un rôle Enterprise Manager.

Si vous voulez affecter un utilisateur au groupe Sophos Console Administrators, utilisez les outils Windows pour ajouter cet utilisateur au groupe.

Pour affecter un utilisateur à un rôle Enterprise Manager, dans le menu **Outils**, cliquez sur **Gérer les rôles**. Pour plus d'informations sur les rôles, reportez-vous à la section [À propos des rôles](#) à la page 15.

Pour utiliser un Enterprise Manager à distance ou supplémentaire, l'utilisateur doit :

- Être membre du groupe Sophos Console Administrators sur le serveur où le serveur d'administration Enterprise Manager est installé.
- Être membre du groupe Distributed COM Users sur le serveur où le serveur d'administration Enterprise Manager est installé. (le groupe Distributed COM Users est placé dans le conteneur Builtin de l'outil Utilisateurs et ordinateurs Active Directory).
- Affecté à au moins un rôle Enterprise Manager.

## 4.2 Création et utilisation de groupes

### 4.2.1 À quoi servent les groupes ?

Créez des groupes et placez-y des ordinateurs avant de commencer à les protéger et à les gérer.

Grâce aux groupes, vous pouvez :

- Mettre à jour les ordinateurs présents dans différents groupes depuis des sources différentes ou selon des planifications différentes.

- Utiliser différentes stratégies antivirus et HIPS, de pare-feu et d'autres stratégies pour différents groupes.
- Gérer les ordinateurs plus facilement.

**Astuce :** vous pouvez créer des groupes à l'intérieur de groupes et appliquer un ensemble de règles spécifiques à chaque groupe et sous-groupe.

## 4.2.2 Qu'est-ce qu'un groupe ?

Un groupe  est un dossier contenant un certain nombre d'ordinateurs.

Vous pouvez créer des groupes vous-même ou importer des conteneurs Active Directory, avec ou sans ordinateurs, et les utiliser comme groupes d'ordinateurs dans Enterprise Manager.

Chaque groupe dispose de paramètres pour la mise à jour, la protection antivirus et HIPS, la protection pare-feu, etc. Tous les ordinateurs d'un groupe doivent généralement utiliser ces paramètres aussi appelés une "stratégie".

Un groupe peut contenir des sous-groupes.

## 4.2.3 Qu'est-ce que le groupe Non affectés ?

Le groupe **Non affectés** est un groupe dans lequel Enterprise Manager conserve les ordinateurs avant de les placer dans des groupes.

Vous ne pouvez pas :

- Appliquer des stratégies au groupe **Non affectés**.
- Créer des sous-groupes dans le groupe **Non affectés**.
- Déplacer ou supprimer le groupe **Non affectés**.

## 4.2.4 Création d'un groupe

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Recherche des ordinateurs, protection et groupes** pour réaliser cette tâche. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Pour créer un groupe pour les ordinateurs :

1. Dans la vue **Ordinateurs d'extrémité**, dans le volet **Groupes** (sur le côté gauche de la console), sélectionnez l'endroit où vous souhaitez créer le groupe.  
Cliquez sur le nom de l'ordinateur en haut de la liste si vous souhaitez créer un nouveau groupe principal. Cliquez sur un groupe déjà existant si vous souhaitez créer un sous-groupe.
2. Dans la barre d'outils, cliquez sur l'icône **Créer un groupe**.  
Un "Nouveau groupe" est ajouté à la liste et son nom est mis en surbrillance.
3. Saisissez un nouveau nom pour le groupe.

Les stratégies de mise à jour, antivirus et HIPS, de pare-feu, des contrôle des périphériques et de protection antialtération sont automatiquement appliquées au nouveau groupe. Vous

pouvez modifier ces stratégies ou appliquer des stratégies différentes. Reportez-vous aux sections [Modification d'une stratégie](#) à la page 26 ou [Affectation d'une stratégie à un groupe](#) à la page 26.

**Remarque :** si le nouveau groupe est un sous-groupe, il utilisera en premier lieu les mêmes paramètres que le groupe auquel il appartient.

## 4.2.5 Ajout d'ordinateurs dans un groupe

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Recherche des ordinateurs, protection et groupes** pour réaliser cette tâche. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

1. Sélectionnez les ordinateurs que vous souhaitez ajouter à un groupe. Par exemple, cliquez sur le groupe **Non affectés** et sélectionnez les ordinateurs à partir de là.
2. Faites glisser et déposer les ordinateurs dans le nouveau groupe.

Si vous déplacez des ordinateurs non protégés du groupe **Non affectés** dans un groupe dans lequel la mise à jour automatique est paramétrée, un assistant se lance pour vous aider à les protéger.

Si vous déplacez les ordinateurs d'un groupe à un autre, ils utiliseront les mêmes stratégies que les ordinateurs qui sont déjà présents dans leur groupe de destination.

## 4.2.6 Suppression d'ordinateurs d'un groupe

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Recherche des ordinateurs, protection et groupes** pour réaliser cette tâche. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Vous pouvez supprimer des ordinateurs d'un groupe si, par exemple, vous souhaitez supprimer des entrées pour des ordinateurs n'étant plus connectés au réseau.

**Important :** si vous supprimez des ordinateurs qui sont encore connectés au réseau, ceux-ci ne seront plus du tout répertoriés ou administrés par la console.

Pour supprimer des ordinateurs :

1. Sélectionnez les ordinateurs que vous souhaitez supprimer.
2. Cliquez dessus avec le bouton droit de la souris et sélectionnez **Supprimer**.

Si vous désirez visualiser de nouveau les ordinateurs, cliquez sur l'icône **Rechercher de nouveaux ordinateurs** de la barre d'outils. Tant qu'ils n'ont pas été redémarrés, ces ordinateurs ne s'affichent pas comme administrés.

### 4.2.7 Opération de couper-coller d'un groupe

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Recherche des ordinateurs, protection et groupes** pour réaliser cette tâche. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

1. Sélectionnez le groupe que vous désirez couper et coller. Dans le menu **Edition**, cliquez sur **Couper**.
2. Sélectionnez le groupe dans lequel vous souhaitez placer le groupe. Dans le menu **Edition**, cliquez sur **Coller**.

### 4.2.8 Suppression d'un groupe

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Recherche des ordinateurs, protection et groupes** pour réaliser cette tâche. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Tout ordinateur qui était dans le groupe supprimé sera placé dans le groupe **Non affectés**.

1. Sélectionnez le groupe que vous souhaitez supprimer.
2. Cliquez dessus avec le bouton droit de la souris et sélectionnez **Supprimer**. Lorsqu'on vous le demande, confirmez que vous voulez supprimer le groupe ainsi que ses sous-groupes si le groupe en possède.

### 4.2.9 Attribution d'un nouveau nom à un groupe

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Recherche des ordinateurs, protection et groupes** pour réaliser cette tâche. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

1. Sélectionnez le groupe que vous souhaitez renommer.
2. Cliquez dessus avec le bouton droit de la souris et sélectionnez **Renommer**.

### 4.2.10 Affectation d'une stratégie à un groupe

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Recherche des ordinateurs, protection et groupes** pour réaliser cette tâche. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

1. Dans le volet **Stratégies**, sélectionnez la stratégie.
2. Cliquez sur la stratégie et faites-la glisser sur le groupe sur lequel vous souhaitez que la stratégie s'applique. Lorsque vous y êtes invité, confirmez si vous désirez continuer.

**Remarque :** autrement, cliquez avec le bouton droit de la souris sur un groupe et sélectionnez **Voir/Modifier les détails de la stratégie du groupe**. Sélectionnez ensuite les stratégies de ce groupe dans les menus déroulants.

### 4.2.11 Vérification des stratégies utilisées par un groupe

Pour voir quelles stratégies ont été affectées à un groupe :

- Dans le volet **Groupes**, cliquez avec le bouton droit de la souris sur le groupe. Sélectionnez **Voir/Modifier les détails de la stratégie du groupe**.

Dans la boîte de dialogue des détails du groupe apparaissent les stratégies en cours d'utilisation.

## 4.3 Création et utilisation de stratégies

### 4.3.1 À propos des stratégies

Une stratégie est un ensemble de paramètres appliqués à tous les ordinateurs d'un groupe.

Lorsque vous installez Enterprise Manager, des stratégies par défaut offrant un niveau de sécurité de base sont créées pour vous. Ces stratégies sont appliquées à tous les groupes que vous avez créés. Vous pouvez modifier les stratégies par défaut.

Vous pouvez aussi créer jusqu'à quatre nouvelles stratégies de chaque type. Une fois que vous avez atteint cette limite, les options **Créer une stratégie** et **Dupliquer une stratégie** sont désactivées.

Vous pouvez appliquer la même stratégie à plusieurs groupes.

Les types de stratégies suivantes sont disponibles dans Enterprise Manager :

- La stratégie de **Mise à jour** définit la manière dont les ordinateurs sont mis à jour avec les nouveaux logiciels de sécurité.
- La stratégie **antivirus et HIPS** définit la manière dont le logiciel de sécurité effectue le contrôle des ordinateurs à la recherche de virus, chevaux de Troie, vers, spywares, adwares, applications potentiellement indésirables, comportements et fichiers suspects et la manière dont il les nettoie.
- La stratégie de **Pare-feu** définit la manière dont le pare-feu assure la protection des ordinateurs.
- La stratégie de **Contrôle des périphériques** spécifie les périphériques de stockage et de réseau qui ne sont pas autorisés d'utilisation sur les stations de travail.
- La stratégie de **Protection antialtération** définit le mot de passe permettant aux utilisateurs autorisés de reconfigurer, désactiver ou désinstaller les logiciels de sécurité Sophos.

### 4.3.2 Quelles sont les stratégies par défaut ?

Lorsque vous installez Enterprise Manager, les stratégies par défaut sont créées pour vous.

### Stratégie de mise à jour

La stratégie de mise à jour par défaut assure :

- La mise à jour automatique des ordinateurs toutes les 10 minutes depuis l'emplacement par défaut. L'emplacement par défaut est un partage UNC \\<NomOrdinateur>\SophosUpdate, où NomOrdinateur correspond au nom de l'ordinateur sur lequel le gestionnaire de mise à jour est installé.

### Stratégie antivirus et HIPS

La stratégie antivirus et HIPS par défaut assure :

- Le contrôle sur accès des virus et des spywares (mais pas des fichiers suspects, des adwares et autres applications potentiellement indésirables).
- L'analyse de l'exécution des programmes fonctionnant sur le système (Sophos Anti-Virus et Sophos Endpoint Security and Control pour Windows 2000 et supérieur).
- L'affichage d'alertes de sécurité sur le bureau de l'ordinateur affecté et leur ajout au journal des événements.

### Stratégie de pare-feu

Par défaut, Sophos Client Firewall est activé et bloque tout le trafic non indispensable. Avant de l'utiliser sur votre réseau, configurez-le pour autoriser les applications que vous désirez utiliser. Reportez-vous à la section [Configuration d'une stratégie de pare-feu](#) à la page 80.

Pour une liste complète des paramètres du pare-feu par défaut, reportez-vous à l'article 57757 de la base de connaissances du support technique (<http://www.sophos.fr/support/knowledgebase/article/57757.html>).

### Stratégie de contrôle des périphériques

Par défaut, le contrôle des périphériques est désactivé et tous les périphériques sont autorisés.

### Stratégie de protection antialtération

Par défaut, la protection antialtération est désactivée et aucun mot de passe n'est spécifié pour permettre aux utilisateurs des ordinateurs d'extrémité autorisés à reconfigurer, désactiver ou désinstaller les logiciels de sécurité Sophos.

## 4.3.3 Dois-je créer mes propres stratégies ?

Lorsque vous installez Enterprise Manager, les stratégies par défaut sont créées pour vous. Ces stratégies s'appliquent à tous les groupes que vous créez.

Les stratégies par défaut offrent un niveau de base de sécurité, mais pour utiliser des fonctions comme le contrôle des périphériques, vous devez créer de nouvelles stratégies ou changer les stratégies par défaut.

**Remarque :** lorsque vous modifiez la stratégie par défaut, cette modification s'applique à toutes les nouvelles stratégies que vous créez.

**Remarque :** si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie** pour créer ou modifier une stratégie. Par exemple, le droit **Paramétrage de stratégie**

- **antivirus et HIPS** vous permet de créer ou de modifier une stratégie antivirus et HIPS. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

### Stratégie de mise à jour

La stratégie de mise à jour par défaut est paramétrée pour que les ordinateurs d'extrémité vérifient la présence de mises à jour pour l'abonnement recommandé toutes les 10 minutes depuis le partage UNC de distribution du logiciel par défaut. Pour changer les abonnements, mettre à jour les emplacements et pour tout autre paramétrage, configurez les stratégies de mise à jour comme le décrit la section [À propos de la stratégie de mise à jour](#) à la page 56.

### Antivirus et HIPS

La stratégie antivirus et HIPS par défaut protège les ordinateurs contre les virus et autres programmes malveillants. Toutefois, pour activer la détection d'autres applications ou comportements indésirables ou suspects, vous pouvez créer de nouvelles stratégies ou changer la stratégie par défaut. Reportez-vous à la section [À propos de la stratégie antivirus et HIPS](#) à la page 63.

### Stratégie de pare-feu

Pour autoriser l'accès au réseau aux applications fiables, configurez les stratégies de pare-feu comme le décrit la section [Configuration d'une stratégie de pare-feu](#) à la page 80.

### Contrôle des périphériques

Par défaut, le contrôle des périphériques est désactivé. Pour limiter l'utilisation de périphériques autorisés, configurez les stratégies de contrôle des périphériques comme le décrit la section [À propos du contrôle des périphériques](#) à la page 111.

### Protection antialtération

Par défaut, la protection antialtération est désactivée. Pour activer la protection antialtération, configurez les stratégies antialtération comme le décrit la section [À propos de la protection antialtération](#) à la page 118.

## 4.3.4 Création d'une stratégie

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie** pour réaliser cette tâche. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Vous pouvez créer jusqu'à quatre nouvelles stratégies de chaque type. Une fois que vous avez atteint cette limite, les options **Créer une stratégie** et **Dupliquer une stratégie** sont désactivées.

Pour créer une stratégie :

1. Dans la vue **Ordinateurs d'extrémité**, dans le volet **Stratégies**, cliquez avec le bouton droit de la souris sur le type de stratégie que vous désirez créer, par exemple "Mise à jour" et sélectionnez **Créer une stratégie**.

Une "Nouvelle stratégie" est ajoutée à la liste et son nom est mis en surbrillance.

2. Saisissez un nouveau nom pour cette stratégie.

3. Cliquez deux fois sur la nouvelle stratégie. Saisissez les paramètres de votre choix.

Pour obtenir des instructions sur la manière de choisir les paramètres, reportez-vous à la section sur la configuration de la stratégie appropriée.

Vous avez créé une stratégie qui peut à présent être appliquée aux groupes.

### 4.3.5 Affectation d'une stratégie à un groupe

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Recherche des ordinateurs, protection et groupes** pour réaliser cette tâche. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

1. Dans le volet **Stratégies**, sélectionnez la stratégie.
2. Cliquez sur la stratégie et faites-la glisser sur le groupe sur lequel vous souhaitez que la stratégie s'applique. Lorsque vous y êtes invité, confirmez si vous désirez continuer.

**Remarque :** autrement, cliquez avec le bouton droit de la souris sur un groupe et sélectionnez **Voir/Modifier les détails de la stratégie du groupe**. Sélectionnez ensuite les stratégies de ce groupe dans les menus déroulants.

### 4.3.6 Modification d'une stratégie

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie** pour réaliser cette tâche. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Pour modifier la stratégie d'un groupe ou de groupes d'ordinateurs :

1. Dans le volet **Stratégies**, cliquez deux fois sur la stratégie que vous désirez modifier.
2. Modifiez les paramètres.

Pour plus d'informations sur la manière de configurer différentes stratégies, reportez-vous aux sections respectives.

### 4.3.7 Attribution d'un nouveau nom à une stratégie

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie** pour réaliser cette tâche. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

**Remarque :** il est impossible de renommer une stratégie "Par défaut".

Pour renommer une stratégie :

1. Dans le volet **Stratégies**, sélectionnez la stratégie que vous désirez renommer.
2. Cliquez dessus avec le bouton droit de la souris et sélectionnez **Renommer une stratégie**.

### 4.3.8 Suppression d'une stratégie

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie** pour réaliser cette tâche. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

**Remarque :** il est impossible de supprimer une stratégie "Par défaut".

Pour supprimer une stratégie :

1. Dans le volet **Stratégies**, cliquez avec le bouton droit de la souris sur la stratégie que vous désirez supprimer et sélectionnez **Supprimer une stratégie**.
2. Tout groupe utilisant la stratégie supprimée utilisera dorénavant la stratégie par défaut.

### 4.3.9 Affichage des groupes utilisant une stratégie

Pour voir à quels groupes a été appliquée une stratégie spécifique :

- Dans le volet **Stratégies**, cliquez avec le bouton droit de la souris sur la stratégie et sélectionnez **Voir les groupes utilisant la stratégie**.

Une liste des groupes qui utilisent la stratégie apparaît.

### 4.3.10 Vérification de l'utilisation de la stratégie de groupe par les ordinateurs

Vous pouvez vérifier si tous les ordinateurs d'un groupe sont conformes aux stratégies de ce groupe.

1. Sélectionnez le groupe que vous désirez vérifier.
2. Dans la liste des ordinateurs de la vue **Ordinateurs d'extrémité**, sur l'onglet **Etat**, observez la colonne **Conformité aux stratégies**.
  - Si vous voyez "Identique à la stratégie", l'ordinateur est conforme aux stratégies de son groupe.
  - Si vous voyez un avertissement jaune et "Diffère de la stratégie", l'ordinateur n'utilise pas la même stratégie ou les mêmes stratégies que les autres ordinateurs de son groupe.

Pour plus d'informations détaillées sur l'état des fonctions de sécurité sur l'ordinateur et des stratégies appliquées à l'ordinateur, reportez-vous à l'onglet respectif dans la vue **Ordinateurs d'extrémité**, par exemple, l'onglet **Détails de l'antivirus**.

Si vous souhaitez que vos ordinateurs soient conformes aux stratégies de leurs groupes, reportez-vous à la section [Application de la stratégie de groupe par les ordinateurs](#) à la page 27.

### 4.3.11 Application de la stratégie de groupe par les ordinateurs

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Actualisation - mise à jour et contrôle** pour effectuer cette tâche. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Si vous découvrez que des ordinateurs ne sont pas conformes aux stratégies de leur groupe, vous pouvez appliquer les stratégies de groupe à cet ordinateur.

1. Sélectionnez le ou les ordinateurs non conformes à la stratégie de groupe.
2. Cliquez avec le bouton droit de la souris et sélectionnez **Mettre en conformité avec**. Puis sélectionnez le type de stratégie approprié, par exemple **Stratégie antivirus et HIPS du groupe**.

## 4.4 Recherche d'ordinateurs sur le réseau

### 4.4.1 Sélection de la méthode de recherche des ordinateurs

Vous pouvez utiliser la fonction “Rechercher de nouveaux ordinateurs” et choisir parmi les différentes options qui vous permettent de retrouver les ordinateurs en réseau et de les ajouter à Enterprise Manager. Voici les différentes options :

- [Importation de conteneurs et d'ordinateurs depuis Active Directory](#) à la page 28
- [Recherche des ordinateurs avec Active Directory](#) à la page 29
- [Recherche des ordinateurs sur le réseau](#) à la page 29
- [Recherche d'ordinateurs par plage IP](#) à la page 30
- [Importation d'ordinateurs depuis un fichier](#) à la page 31

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Recherche des ordinateurs, protection et groupes** pour ajouter des ordinateurs dans la console. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

### 4.4.2 Importation de conteneurs et d'ordinateurs depuis Active Directory

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Recherche des ordinateurs, protection et groupes** pour réaliser cette tâche. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

L'importation de groupes depuis Active Directory récupère la structure du conteneur Active Directory et la copie dans Enterprise Manager sous la forme d'une structure de groupe d'ordinateurs. Vous pouvez importer la structure du groupe uniquement ou les groupes et les ordinateurs. Si vous optez pour la dernière solution, les ordinateurs trouvés dans Active Directory sont placés dans leurs groupes respectifs et pas dans le groupe **Non affectés**.

Vous pouvez avoir à la fois des groupes “normaux” que vous créez et gérez vous-même et des groupes importés depuis Active Directory.

Pour importer des groupes depuis Active Directory :

1. Dans la barre d'outils, cliquez sur l'icône **Rechercher de nouveaux ordinateurs**.

2. Dans la boîte de dialogue **Recherche de nouveaux ordinateurs**, dans le volet **Importation depuis Active Directory**, sélectionnez **Importer** et cliquez sur **OK**.  
Sinon, sélectionnez un groupe dans lequel vous voulez importer votre ou vos conteneurs Active Directory, cliquez avec le bouton droit de la souris et sélectionnez **Importer depuis Active Directory**.  
L'**Assistant d'importation depuis Active Directory** démarre.
3. Suivez les instructions de l'assistant. Lorsqu'on vous demande de choisir quoi importer, sélectionnez **Ordinateurs et groupes** ou **Groupes uniquement**, en fonction de ce que vous voulez importer.

Dès que vous avez importé les conteneurs depuis Active Directory, appliquez les stratégies aux groupes. Reportez-vous à la section [À propos des stratégies](#) à la page 23.

### 4.4.3 Recherche des ordinateurs avec Active Directory

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Recherche des ordinateurs, protection et groupes** pour réaliser cette tâche. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Vous pouvez utiliser Active Directory pour rechercher les ordinateurs en réseau et les ajouter dans le groupe **Non affectés**.

1. Dans la barre d'outils, cliquez sur l'icône **Rechercher de nouveaux ordinateurs**.
2. Dans la boîte de dialogue **Recherche de nouveaux ordinateurs**, sélectionnez **Rechercher avec Active Directory** et cliquez sur **OK**.
3. Vous êtes invité à saisir un nom utilisateur et un mot de passe. Ceci est indispensable si vous avez des ordinateurs (par exemple, Windows XP Service Pack 2) dont l'accès est impossible sans les détails d'un compte.  
Le compte doit être un compte d'administrateur de domaine ou disposer des pleins droits administratifs sur les ordinateurs XP cibles.  
Si vous utilisez un compte de domaine, vous *devez* saisir le nom utilisateur sous la forme domaine\utilisateur.
4. Dans la boîte de dialogue **Recherche des ordinateurs**, sélectionnez les domaines dans lesquels vous souhaitez effectuer la recherche. Cliquez sur **OK**.
5. Cliquez sur le groupe **Non affectés** pour visualiser les ordinateurs qui ont été trouvés.

Pour commencer à gérer les ordinateurs, sélectionnez-les et glissez-les dans un groupe.

### 4.4.4 Recherche des ordinateurs sur le réseau

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Recherche des ordinateurs, protection et groupes** pour réaliser cette tâche. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Pour ajouter une liste d'ordinateurs trouvés dans les domaines et les groupes de travail Windows dans le groupe **Non affectés** :

1. Dans la barre d'outils, cliquez sur l'icône **Rechercher de nouveaux ordinateurs**.

2. Dans la boîte de dialogue **Recherche de nouveaux ordinateurs**, sélectionnez **Rechercher sur le réseau** et cliquez sur **OK**.
3. Dans la boîte de dialogue **Codes d'accès**, saisissez le nom utilisateur et le mot de passe d'un compte qui dispose des droits suffisants pour récupérer les informations relatives à l'ordinateur.  
Le compte doit être un compte d'administrateur de domaine ou disposer des pleins droits administratifs sur les ordinateurs cibles. Si vous utilisez un compte de domaine, saisissez le nom utilisateur au format domaine\utilisateur.  
Vous pouvez ignorer cette étape si vos ordinateurs cibles sont accessibles sans les détails d'un compte.
4. Dans la boîte de dialogue **Recherche des ordinateurs**, sélectionnez les domaines ou groupes de travail dans lesquels vous souhaitez rechercher. Cliquez sur **OK**.
5. Cliquez sur le groupe **Non affectés** pour visualiser les ordinateurs qui ont été trouvés.

Pour commencer à gérer les ordinateurs, sélectionnez-les et glissez-les dans un groupe.

#### 4.4.5 Recherche d'ordinateurs par plage IP

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Recherche des ordinateurs, protection et groupes** pour réaliser cette tâche. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Vous pouvez utiliser une plage d'adresses IP pour rechercher les ordinateurs en réseau et les ajouter dans le groupe **Non affectés**.

**Remarque :** vous ne pouvez pas utiliser les adresses IPV6.

1. Dans la barre d'outils, cliquez sur l'icône **Rechercher de nouveaux ordinateurs**.
2. Dans la boîte de dialogue **Recherche de nouveaux ordinateurs**, sélectionnez **Rechercher par plage IP** et cliquez sur **OK**.
3. Dans la boîte de dialogue **Codes d'accès**, vous êtes invité à saisir un nom utilisateur et un mot de passe. Ceci est indispensable si vous avez des ordinateurs (par exemple, Windows XP Service Pack 2) dont l'accès est impossible sans les détails d'un compte.  
Le compte doit être un compte d'administrateur de domaine ou disposer des pleins droits administratifs sur les machines XP cibles.  
Si vous utilisez un compte de domaine, vous *devez* saisir le nom utilisateur sous la forme domaine\utilisateur.  
Dans le volet **SNMP**, saisissez le nom de la communauté SNMP.
4. Dans la boîte de dialogue **Recherche d'ordinateurs**, saisissez le **Début de plage IP** et la **Fin de plage IP**. Cliquez sur **OK**.
5. Cliquez sur le groupe **Non affectés** pour visualiser les ordinateurs qui ont été trouvés.

Pour commencer à gérer les ordinateurs, sélectionnez-les et glissez-les dans un groupe.

## 4.4.6 Importation d'ordinateurs depuis un fichier

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Recherche des ordinateurs, protection et groupes** pour réaliser cette tâche. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Pour que Enterprise Manager puisse répertorier vos ordinateurs, vous pouvez importer les noms des ordinateurs depuis un fichier.

Le fichier contenant les noms des ordinateurs doit impérativement être l'un des suivants :

- Un fichier utilisant les conventions répertoriées ci-dessous.
- Un fichier SGR exporté depuis Sophos SAVAdmin.

Vous pouvez créer un fichier en utilisant des entrées semblables à celles-ci :

```
[NomGroupe1 ]
Domaine1 |Windows7 |NomOrdinateur1
Domaine1 |WindowsServer2008R2 |NomOrdinateur2
```

**Remarque :** il n'est pas nécessaire de spécifier dans quel groupe seront placés les ordinateurs. Si vous saisissez [] (sans espace entre les crochets) pour le nom du groupe, les ordinateurs seront placés dans le dossier **Non affectés**.

**Remarque :** les noms des systèmes d'exploitation valides sont les suivants : Windows2000, Windows2000Server, WindowsXP, Windows2003, WindowsVista, Windows7, WindowsServer2008, WindowsServer2008R2, MACOSX et Linux.

Le nom de domaine et le système d'exploitation sont tous les deux facultatifs. Une entrée peut ainsi apparaître sous la forme suivante :

```
[NomGroupe1 ]
NomOrdinateur1
```

Importez les noms des ordinateurs comme suit :

1. Dans le menu **Fichier**, cliquez sur **Importer les ordinateurs depuis un fichier**.
2. Dans la fenêtre du navigateur, sélectionnez le fichier.
3. Cliquez sur le groupe **Non affectés** pour voir les ordinateurs qui ont été trouvés.
4. Pour commencer à gérer les ordinateurs, sélectionnez-les et glissez-les dans un groupe.

## 5 Protection des ordinateurs

### 5.1 Préparation de l'installation du logiciel antivirus

En plus de vous assurer que les ordinateurs sont conformes à la configuration système générale, des étapes supplémentaires sont à exécuter avant de pouvoir y installer automatiquement le logiciel.

Pour préparer l'installation du logiciel antivirus :

1. Sur les ordinateurs Windows 7/Vista :
  - a) Sous Windows 7, dans le Panneau de configuration, ouvrez le Centre Réseau et partage. Pour l'emplacement **Réseau professionnel**, assurez-vous que les options sont configurées ci-dessous :
    - Recherche du réseau : activé
    - Partage de fichiers et d'imprimantes : activé
    - Connexions de partage de fichiers : activer le partage de fichiers pour les périphériques qui utilisent le chiffrement 40 ou 56 bits
    - Partage protégé par mot de passe : désactivé
  - b) Sous Windows Vista, dans le Panneau de configuration, ouvrez le Centre Réseau et partage. Assurez-vous que les options sont configurées comme ci-dessous :
    - Recherche du réseau : activé
    - Partage de fichiers : activé
    - Partage d'imprimantes : activé
    - Partage protégé par mot de passe : désactivé
  - c) Assurez-vous que le service Registre à distance est lancé et que son type de démarrage est défini sur Automatique. Ce service n'est pas actif par défaut sous Windows 7/Vista.
  - d) Sous Windows 7, paramétrez le Contrôle de compte d'utilisateur sur **Ne jamais notifier**. Une fois l'installation terminée, rétablissez cette option sur **Par défaut**.
  - e) Sous Windows Vista, désactivez le Contrôle de compte d'utilisateur. Une fois l'installation terminée, activez de nouveau cette option.
  - f) Désactivez l'Assistant Partage.
  - g) Ouvrez le Pare-feu Windows avec fonctions avancées de sécurité en allant dans le Panneau de configuration et en cliquant sur **Outils d'administration**. Assurez-vous que les **Connexions entrantes** sont autorisées.
  - h) Changez les **Règles de trafic entrant** pour activer les processus ci-dessous. Une fois l'installation terminée, désactivez de nouveau ces processus.
    - Administration à distance (NP-Entrée) Domaine
    - Administration à distance (NP-Entrée) Privé

Administration à distance (RPC) Domaine

Administration à distance (RPC) Privé

Administration à distance (RPC-EPMAP) Domaine

Administration à distance (RPC-EPMAP) Privé

2. Sur les ordinateurs Windows 2003/XP Pro/2000 :
  - a) Assurez-vous que les services Registre à distance, Serveur, Explorateur d'ordinateur et Planificateur de tâches sont démarrés.
  - b) Assurez-vous que le partage admin C\$ est activé.
  - c) Assurez-vous que Partage de fichiers simple est désactivé (XP uniquement).
3. Sur les ordinateurs Windows XP SP2 ou supérieur :
  - a) Assurez-vous que les services Registre à distance, Serveur, Explorateur d'ordinateur et Planificateur de tâches sont démarrés.
  - b) Assurez-vous que le partage admin C\$ est activé.
  - c) Assurez-vous que Partage de fichiers simple est désactivé.
  - d) Activez le Partage de fichiers et d'imprimantes pour les réseaux Microsoft.
  - e) Assurez-vous que les ports TCP 8192, 8193 et 8194 sont ouverts.
  - f) Redémarrez l'ordinateur pour appliquer les changements.

## 5.2 Suppression des logiciels de sécurité tiers

Si vous souhaitez supprimer les logiciels de sécurité tiers précédemment installés, procédez de la manière suivante AVANT de sélectionner **Détection des logiciels de sécurité tiers** dans l'**Assistant de protection des ordinateurs** et de l'installer :

- Si les ordinateurs utilisent le logiciel antivirus d'un autre éditeur, veillez à ce que son interface utilisateur soit fermée.
- Si les ordinateurs utilisent le pare-feu ou le produit HIPS d'un autre éditeur, veillez à ce qu'il soit désactivé ou configuré pour permettre au programme d'installation Sophos de s'exécuter.
- Si vous désirez supprimer le logiciel d'un autre éditeur ainsi que son outil de mise à jour (pour l'empêcher de réinstaller automatiquement le logiciel), suivez les étapes ci-dessous. Si aucun outil de mise à jour n'est installé sur les ordinateurs, vous pouvez ignorer les étapes ci-dessous.

**Remarque:** vous devez redémarrer localement tous les ordinateurs sur lesquels vous supprimez le logiciel antivirus tiers.

Si l'outil de mise à jour d'un autre éditeur est installé sur les ordinateurs et si vous souhaitez le supprimer, vous allez devoir modifier le fichier de configuration avant d'exécuter l'option **Détection des logiciels de sécurité tiers** de l'**Assistant de protection des ordinateurs**.

**Remarque :** si des ordinateurs utilisent le pare-feu ou le produit HIPS d'un autre éditeur, il est possible que vous soyez obligé de conserver l'outil de mise à jour de cet éditeur. Pour plus de précisions, reportez-vous à la documentation de l'éditeur.

Pour modifier le fichier de configuration :

1. Depuis le répertoire d'installation centralisée, recherchez le fichier data.zip.
2. Extrayez le fichier de configuration crt.cfg de data.zip.
3. Modifiez le fichier crt.cfg pour changer la ligne "RemoveUpdateTools=0" en "RemoveUpdateTools=1".
4. Enregistrez vos changements ainsi que le fichier crt.cfg dans le même répertoire que celui qui contient data.zip. Ne remplacez pas crt.cfg dans data.zip, sinon il sera remplacé à la mise à jour suivante du fichier data.zip.

Lorsque vous exécutez l'**Assistant de Protection des ordinateurs** et sélectionnez **Détection des logiciels de sécurité tiers**, le fichier de configuration modifié supprime alors tout outil de mise à jour tiers ainsi que tout logiciel de sécurité tiers.

## 5.3 Protection des ordinateurs

Avant de protéger les ordinateurs depuis la console :

- Appliquez la stratégie de mise à jour au groupe avant de pouvoir protéger les ordinateurs dans ce groupe.
- Si vous souhaitez protéger automatiquement les ordinateurs Windows XP depuis la console, assurez-vous que le "Partage de fichiers simple" est désactivé.
- Si vous utilisez l'administration déléguée, vous devez disposer du droit **Recherche des ordinateurs, protection et groupes** pour protéger les ordinateurs. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

L'installation automatique avec Enterprise Manager n'est pas possible sur les ordinateurs Mac et Linux. Pour plus d'informations sur comment protéger ces systèmes d'exploitation, reportez-vous au *Guide de démarrage de Sophos Enterprise Manager*. La documentation Sophos est disponible sur <http://www.sophos.fr/support/docs/>.

Pour protéger les ordinateurs :

1. En fonction de la situation des groupes que vous voulez protéger (déjà dans un groupe ou dans aucun groupe), effectuez l'une des opérations suivantes :
  - Si les ordinateurs que vous voulez protéger sont dans le groupe **Non affectés**, faites-les glisser dans un groupe.
  - Si les ordinateurs que vous voulez protéger sont déjà dans un groupe, sélectionnez-les, cliquez avec le bouton droit de la souris et cliquez sur **Protéger les ordinateurs**.

L'**Assistant de protection des ordinateurs** se lance.

2. Suivez les instructions de l'assistant. Sur la page **Sélection des fonctionnalités**, sélectionnez les fonctionnalités que vous désirez.

La protection antivirus est toujours sélectionnée et doit être installée. Vous pouvez également choisir d'installer les fonctions suivantes :

■ **Sophos Client Firewall**

Le pare-feu client est uniquement disponible s'il est inclus dans votre licence et seulement pour Windows 2000 ou supérieur.

Vous ne pouvez pas installer le pare-feu sur des ordinateurs exécutant des systèmes d'exploitation serveur ou Windows Vista Starter.

■ **Détection des logiciels de sécurité tiers**

Laissez la case **Détection des logiciels de sécurité tiers** sélectionnée si vous voulez que le logiciel d'un autre éditeur soit supprimé automatiquement. La détection des logiciels de sécurité tiers consiste à désinstaller uniquement les produits ayant les mêmes fonctionnalités que ceux que vous installez.

3. Sur la page **Récapitulatif de la protection**, tout problème rencontré avec l'installation figure dans la colonne **Problèmes de protection**. Résolvez les problèmes relatifs à l'installation (reportez-vous à la section [L'installation de Sophos Endpoint Security and Control a échoué](#) à la page 147) ou exécutez une installation manuelle sur ces ordinateurs (reportez-vous au *Guide de démarrage de Sophos Enterprise Manager* ). Cliquez sur **Suivant**.
4. Sur la page **Codes d'accès**, saisissez les détails d'un compte qui peut être utilisé pour installer le logiciel.

Généralement, il s'agit d'un compte d'administrateur de domaine. Il doit impérativement :

- Posséder les droits d'administrateur local sur les ordinateurs que vous souhaitez protéger.
- Pouvoir se connecter à l'ordinateur sur lequel vous avez installé le serveur d'administration.
- Avoir un accès en lecture à l'emplacement Serveur principal spécifié dans la stratégie de **Mise à jour**. Reportez-vous à la section [À propos des emplacements du serveur de mise à jour](#) à la page 57 et aux autres rubriques de la section *Configuration des emplacements du serveur de mise à jour*.

**Remarque :** si vous utilisez un compte de domaine, vous *devez* saisir le nom utilisateur au format **domaine\utilisateur**.

Si les ordinateurs sont dans des domaines différents couverts par le même schéma Active Directory, utilisez plutôt le compte Administrateur Enterprise dans Active Directory.

## 5.4 Affichage des emplacements des fichiers d'amorce

Si Enterprise Manager ne parvient pas à installer l'antivirus ou le pare-feu sur certains ordinateurs, effectuez l'installation manuellement.

Pour rechercher les programmes d'installation :

1. Dans le menu **Affichage**, cliquez sur **Emplacements des fichiers d'amorce**.

2. Dans la boîte de dialogue **Emplacements des fichiers d'amorce**, pour chaque abonnement logiciels, vous verrez les emplacements contenant les programmes d'installation des logiciels, ainsi que les plates-formes sur lesquelles les logiciels sont pris en charge et leurs versions. Notez l'emplacement du programme d'installation dont vous avez besoin.  
Si votre licence inclut le pare-feu, vous pouvez l'installer en même temps que l'antivirus sur des ordinateurs Windows 2000 ou supérieur.

Pour plus d'informations sur l'installation manuelle des logiciels de sécurité sur différents systèmes d'exploitation, reportez-vous au *Guide de démarrage de Sophos Enterprise Manager*.

## 5.5 Vérification de la protection de votre réseau

### 5.5.1 Comment m'assurer que mon réseau est protégé ?

Pour avoir un aperçu de l'état de sécurité du réseau, utilisez le Tableau de bord. Pour plus d'informations, reportez-vous aux sections [Volets du Tableau de bord](#) à la page 7 et [Configuration du Tableau de bord](#) à la page 36.

Vous pouvez identifier les ordinateurs à problèmes en utilisant la liste des ordinateurs et les filtres de cette liste. Par exemple, vous pouvez voir les ordinateurs sur lesquels le pare-feu n'est pas installé ou ceux ayant des alertes nécessitant votre attention. Pour plus d'informations, reportez-vous aux sections [Vérification de la protection des ordinateurs](#) à la page 37, [Vérification de l'état de mise à jour des ordinateurs](#) à la page 38, et [Recherche d'ordinateurs avec problèmes](#) à la page 38.

Vous pouvez vérifier si tous les ordinateurs d'un groupe sont conformes aux stratégies de ce groupe, comme le décrit la section [Vérification de l'utilisation de la stratégie de groupe par les ordinateurs](#) à la page 27.

### 5.5.2 Configuration du Tableau de bord

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Configuration système** pour configurer le Tableau de bord. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Le Tableau de bord affiche des indicateurs d'alerte ou critique en fonction du pourcentage d'ordinateurs administrés avec des alertes ou des erreurs à traiter ou du temps écoulé depuis la dernière mise à jour depuis Sophos.

Vous pouvez configurer les niveaux d'alerte ou critique que vous souhaitez utiliser.

1. Dans le menu **Outils**, cliquez sur **Configurer le tableau de bord**.
2. Dans la boîte de dialogue **Configuration du Tableau de bord**, changez les valeurs de seuil dans les zones de texte **Niveau d'alerte** et **Niveau critique** comme décrit ci-dessous.
  - a) Sous **Ordinateurs avec des alertes à traiter**, **Ordinateurs avec des erreurs de produits Sophos** et **Stratégie et protection**, saisissez un pourcentage d'ordinateurs administrés

affectés par un problème particulier et qui déclenchera le passage de l'indicateur respectif de l'état "alerte" à l'état "critique".

- b) Sous **Ordinateurs avec événements**, saisissez le nombre d'événements ayant eu lieu dans une période de sept jours qui déclenchent une alerte affichée sur le Tableau de bord.
- c) Sous **Dernière protection depuis Sophos**, saisissez l'heure de la dernière mise à jour réussie depuis Sophos qui déclenchera la passage de l'indicateur "Mises à jour" à l'état "alerte" ou "critique". Cliquez sur **OK**.

Si vous réglez un niveau sur zéro, les avertissements se déclencheront dès la réception de la première alerte.

Vous pouvez aussi configurer l'envoi des alertes par courriel aux destinataires de votre choix lorsqu'un seuil d'alerte ou critique a été dépassé. Pour plus d'instructions, reportez-vous à la section [Configuration des alertes par courriel sur l'état du réseau](#) à la page 125.

### 5.5.3 Vérification de la protection des ordinateurs

Les ordinateurs sont protégés s'ils exécutent le contrôle sur accès et le pare-feu (si vous l'avez installé). Pour une protection intégrale, le logiciel doit aussi être mis à jour.

**Remarque :** vous avez peut-être choisi de ne pas utiliser le contrôle sur accès sur certains types d'ordinateurs comme, par exemple, les serveurs de fichiers. Dans ce cas, assurez-vous que les ordinateurs utilisent les contrôles planifiés et qu'ils sont à jour.

Pour vérifier que les ordinateurs sont protégés :

1. Sélectionnez le groupe d'ordinateurs que vous désirez vérifier.
2. Si vous désirez vérifier les ordinateurs dans les sous-groupes du groupe, sélectionnez **À ce niveau et au-dessous** dans la liste déroulante.
3. Dans la liste des ordinateurs, sur l'onglet **État**, observez la colonne **Sur accès**.

Si vous voyez "Actif", l'ordinateur exécute le contrôle sur accès. Si vous voyez un bouclier gris, il ne l'exécute pas.

4. Si vous avez installé le pare-feu, observez la colonne **Pare-feu activé**.

Si vous voyez "Oui", le pare-feu est activé. Si vous voyez une icône du pare-feu grisée et le mot "Non", le pare-feu est désactivé.

5. Si vous utilisez d'autres fonctionnalités comme le contrôle des périphériques, vérifiez l'état dans la colonne respective.

Pour plus d'informations sur la procédure de vérification de mise à jour des ordinateurs, reportez-vous à la section [Vérification de l'état de mise à jour des ordinateurs](#) à la page 38.

Pour plus d'informations sur la recherche des ordinateurs à problèmes à l'aide de filtres de listes d'ordinateurs, reportez-vous à la section [Recherche d'ordinateurs avec problèmes](#) à la page 38.

## 5.5.4 Vérification de l'état de mise à jour des ordinateurs

Si vous avez configuré Enterprise Manager comme recommandé, les ordinateurs recevront automatiquement les mises à jour.

Pour vérifier que les ordinateurs sont à jour :

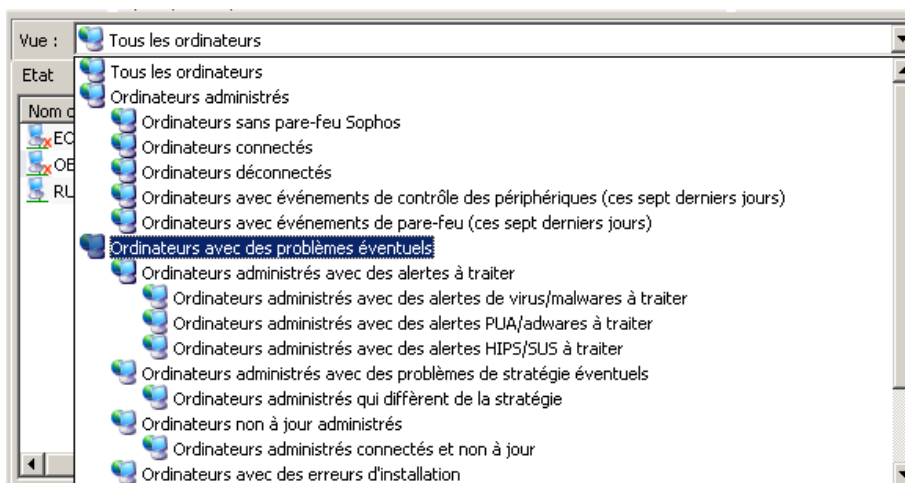
1. Sélectionnez le groupe d'ordinateurs que vous désirez vérifier.
2. Si vous désirez vérifier les ordinateurs dans un des sous-groupes, sélectionnez **A ce niveau et au-dessous** dans la liste déroulante.
3. Sur l'onglet **Etat**, observez la colonne **A jour** ou allez sur l'onglet **Détails de la mise à jour**.
  - Si vous voyez “Oui” dans la colonne **A jour**, l'ordinateur est à jour.
  - Si l'icône d'une horloge apparaît, l'ordinateur n'est pas à jour. Le texte indique depuis combien de temps l'ordinateur n'est pas à jour.

Pour plus d'informations sur la mise à jour de ces ordinateurs obsolètes, reportez-vous à la section [Mise à jour des ordinateurs non à jour](#) à la page 61.

## 5.5.5 Recherche d'ordinateurs avec problèmes

Pour afficher une liste des ordinateurs qui ne sont pas correctement protégés ou qui ont d'autres problèmes liés à la protection :

1. Sélectionnez le groupe d'ordinateurs que vous désirez vérifier.
2. Dans la liste déroulante **Vue**, sélectionnez les ordinateurs que vous voulez rechercher, par exemple, les **Ordinateurs avec des problèmes éventuels**.



Vous pouvez aussi sélectionner une sous-entrée de cette entrée pour afficher les ordinateurs affectés par un problème spécifique (par exemple, les ordinateurs qui diffèrent de la stratégie de groupe ou lorsqu'une erreur sur un produit Sophos a lieu).

3. Si le groupe contient des sous-groupes, sélectionnez également si vous souhaitez rechercher les ordinateurs **A ce niveau seulement** ou **A ce niveau et au-dessous**.

Tout ordinateur ayant des problèmes de protection sera répertorié.

Pour plus d'informations sur le traitement des problèmes de protection, reportez-vous à la section [Les ordinateurs n'utilisent pas le contrôle sur accès](#) à la page 145 et aux autres rubriques de la section *Résolution des problèmes*.

## 5.6 Traitement des alertes et des erreurs



### 5.6.1 Que signifient les icônes d'alertes ?

Si un virus ou un spyware, un élément suspect, un adware ou toute autre application potentiellement indésirable est détecté, des icônes d'alerte apparaissent sur l'onglet **Etat** dans la vue **Ordinateurs d'extrémité**.

Les icônes d'alertes sont représentées ci-dessous. Les autres rubriques de cette section contiennent des conseils sur le traitement des alertes.

**Remarque :** des avertissements apparaissent aussi dans la console si le logiciel est désactivé ou non à jour. Pour plus d'informations, reportez-vous à la section [Comment m'assurer que mon réseau est protégé ?](#) à la page 36.

#### Icônes d'alertes

Icône	Explication
	L'apparition d'un signal d'avertissement rouge dans la colonne <b>Alertes et erreurs</b> signifie qu'un virus, un ver, un cheval de Troie, un spyware ou un comportement suspect a été détecté.
	L'apparition d'un signal d'avertissement jaune dans la colonne <b>Alertes et erreurs</b> indique l'un des problèmes suivants : <ul style="list-style-type: none"> <li>■ Un fichier suspect a été détecté.</li> <li>■ Un adware ou toute autre application potentiellement indésirable a été détecté.</li> <li>■ Une erreur s'est produite.</li> </ul> L'apparition d'un signal d'avertissement jaune dans la colonne <b>Conforme à la stratégie</b> indique que l'ordinateur n'utilise pas la même stratégie ou les mêmes stratégies que les autres ordinateurs de son groupe.

S'il y a plusieurs alertes ou erreurs sur un ordinateur, l'icône de l'alerte ayant la priorité la plus haute apparaît dans la colonne **Alertes et erreurs**. Les types d'alertes sont répertoriés ci-dessous par ordre de priorité décroissant.

1. Alertes de virus et spyware

2. Alertes de comportement suspect
3. Alertes de fichier suspect
4. Alertes d'adware et PUA
5. Erreurs d'applications logicielles (par exemple, erreurs d'installation)

Pour plus de détails sur une alerte, par exemple, le nom de l'élément détecté, cliquez sur l'onglet **Détails des alertes et des erreurs**.

## 5.6.2 Traitement des alertes sur les éléments détectés

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Actualisation - nettoyage** pour nettoyer les éléments détectés ou effacer les alertes depuis la console. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Pour prendre des mesures contre les alertes affichées dans la console :

1. Dans la vue **Ordinateurs d'extrémité**, sélectionnez le ou les ordinateurs dont vous souhaitez voir les alertes. Cliquez avec le bouton droit de la souris et sélectionnez **Résoudre les alertes et les erreurs**.

La boîte de dialogue **Résolution des alertes et des erreurs** apparaît.

2. Les mesures que vous pouvez prendre contre une alerte dépendent de l'état du nettoyage de l'alerte. Observez la colonne **État du nettoyage** et décidez des mesures à prendre.

**Astuce :** vous pouvez trier les alertes en cliquant sur un en-tête de colonne. Par exemple, pour trier les alertes par statut de nettoyage, cliquez sur l'en-tête de colonne **État du nettoyage**.

Etat du nettoyage	Description et mesures à prendre
Nettoyable	Vous pouvez supprimer l'élément. Pour cela, sélectionnez l'alerte ou les alertes et cliquez sur <b>Nettoyage</b> .
Type de menace non nettoyable	Ce type d'élément détecté, par exemple, un fichier ou un comportement suspect, ne peut pas être nettoyé de la console. Vous devez décider si vous voulez autoriser ou bloquer l'élément. Si vous ne faites pas confiance à cet élément, vous pouvez l'envoyer à Sophos en vue d'une analyse. Pour plus d'informations, reportez-vous à la section <a href="#">Recherche d'informations sur les éléments détectés</a> à la page 41.
Non nettoyable	Cet élément ne peut pas être nettoyé de la console. Pour plus d'informations sur l'élément et sur les actions que vous pouvez prendre, reportez-vous à la section <a href="#">Recherche d'informations sur les éléments détectés</a> à la page 41.
Contrôle intégral requis	Cet élément est nettoyable, mais un contrôle intégral de l'ordinateur d'extrémité est nécessaire avant que le nettoyage puisse être exécuté. Retrouvez plus d'instructions à la section <a href="#">Contrôle immédiat des ordinateurs</a> à la page 43.

Etat du nettoyage	Description et mesures à prendre
Redémarrage requis	L'élément a été partiellement supprimé, mais l'ordinateur d'extrémité n'a pas besoin d'être redémarré pour terminer le nettoyage. <b>Remarque :</b> les ordinateurs d'extrémité doivent être redémarrés localement et non pas depuis Enterprise Manager.
Échec du nettoyage	L'élément n'a pas pu être supprimé. Un nettoyage manuel peut être nécessaire. Pour plus d'informations, reportez-vous à la section <a href="#">Gestion des éléments détectés en cas d'échec du nettoyage</a> à la page 44.
Nettoyage en cours (démarré à <heure>)	Le nettoyage est en cours.
Délai d'attente dépassé pour le nettoyage (démarré à <heure>)	Le délai d'attente est dépassé pour le nettoyage. L'élément n'a peut-être pas été nettoyé. Ceci peut se produire, par exemple, lorsque l'ordinateur d'extrémité est déconnecté du réseau ou lorsque le réseau est occupé. Vous pouvez essayer de nettoyer une nouvelle fois l'élément ultérieurement.

Si vous avez décidé d'autoriser un élément, reportez-vous à la section [Autorisation des adwares et des PUA](#) à la page 69 ou [Autorisation d'éléments suspects](#) à la page 66.

### 5.6.3 Recherche d'informations sur les éléments détectés

Si vous voulez en savoir plus sur une menace ou sur un autre élément détecté sur un ordinateur d'extrémité et signalé dans la console ou si vous avez besoin de conseils sur les mesures à prendre contre l'élément, suivez les étapes suivantes :

1. Dans la vue **Ordinateurs d'extrémité**, dans la liste des ordinateurs, cliquez deux fois sur l'ordinateur affecté.
2. Dans la boîte de dialogue **Détails de l'ordinateur**, défilez jusqu'à la section **Alertes et erreurs à traiter**. Dans la liste des éléments détectés, cliquez sur le nom de l'élément qui vous intéresse.

Ceci vous connecte directement au site Web de Sophos où vous pouvez lire une description de l'élément et des conseils sur les mesures à prendre.

**Remarque :** vous pouvez aussi vous rendre sur la page des **Analyses de sécurité** sur le site Web de Sophos (<http://www.sophos.fr/security/analyses/>), cliquez sur l'onglet correspondant au type d'élément que vous recherchez, puis saisissez le nom de l'élément dans la boîte de recherche ou recherchez-le dans la liste des éléments.

### 5.6.4 Effacement des alertes ou des erreurs depuis la console

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Actualisation - nettoyage** pour effacer les alertes ou les erreurs depuis la console. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Si vous prenez des mesures pour traiter les alertes ou si vous êtes certain que l'ordinateur est sain, vous pouvez effacer l'alerte affichée dans la console.

**Remarque:** vous ne pouvez pas effacer les alertes concernant les erreurs d'installation. Celles-ci sont effacées uniquement lorsque l'installation de Sophos Endpoint Security and Control est installée avec succès sur l'ordinateur.

1. Dans la vue **Ordinateurs d'extrémité**, sélectionnez le ou les ordinateurs pour lesquels vous souhaitez effacer les alertes. Cliquez avec le bouton droit de la souris et sélectionnez **Résoudre les alertes et les erreurs**.

La boîte de dialogue **Résolution des alertes et des erreurs** apparaît.

2. Pour effacer les alertes ou les erreurs des produits Sophos depuis la console, allez respectivement sur l'onglet Alertes ou Erreurs, sélectionnez les alertes ou les erreurs que vous voulez effacer et cliquez sur **Approuver**.

Les alertes approuvées (supprimées) n'apparaissent plus dans la console.

Pour plus d'informations sur la manière d'effacer les alertes du gestionnaire de mise à jour depuis la console, reportez-vous à la section [Effacement des alertes du gestionnaire de mise à jour depuis la console](#) à la page 42.

## 5.6.5 Effacement des alertes du gestionnaire de mise à jour depuis la console

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Actualisation - nettoyage** pour effacer les alertes depuis la console. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Pour effacer les alertes du gestionnaire de mise à jour depuis la console :

1. Dans la vue **Gestionnaires de mise à jour**, sélectionnez le gestionnaire de mise à jour. Cliquez avec le bouton droit de la souris et sélectionnez **Approuver les alertes**.

La boîte de dialogue **Alertes du gestionnaire de mise à jour** apparaît.

2. Pour effacer les alertes depuis la console, sélectionnez les alertes que vous souhaitez effacer et cliquez sur **Approuver**.

Les alertes approuvées (supprimées) n'apparaissent plus dans la console.

## 5.7 Contrôle des ordinateurs

### 5.7.1 À propos du contrôle

Par défaut, Sophos Endpoint Security and Control détecte automatiquement les virus, les chevaux de Troie, les vers et les spywares connus et inconnus présents dans les fichiers auxquels un utilisateur tente d'accéder. Il analyse également le comportement des programmes s'exécutant sur le système.

Vous pouvez également configurer Sophos Endpoint Security and Control pour effectuer les tâches suivantes :

- Contrôler les ordinateurs à la recherche des fichiers suspects. Reportez-vous à la section [Contrôle à la recherche des fichiers suspects](#) à la page 65.
- Contrôler les ordinateurs à la recherche des adwares et autres applications potentiellement indésirables. Reportez-vous à la section [Recherche d'adwares et de PUA](#) à la page 68.
- Contrôler les ordinateurs à des heures définies. Reportez-vous à la section [Contrôle des ordinateurs à des heures définies](#) à la page 73.

Pour plus d'informations sur la configuration du contrôle, reportez-vous à la section [À propos de la stratégie antivirus et HIPS](#) à la page 63.

Cette section décrit comment effectuer immédiatement un contrôle intégral du système des ordinateurs sélectionnés.

## 5.7.2 Contrôle immédiat des ordinateurs

Vous pouvez contrôler un ou plusieurs ordinateurs immédiatement sans attendre le prochain contrôle planifié.

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Correction - mise à jour et contrôle** pour contrôler les ordinateurs. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

**Remarque :** seuls les ordinateurs Windows 2000 ou supérieur peuvent faire l'objet d'un contrôle intégral du système demandé depuis la console.

Pour contrôler les ordinateurs immédiatement :

1. Sélectionnez les ordinateurs dans la liste des ordinateurs ou un groupe depuis le volet **Groupes**. Cliquez avec le bouton droit de la souris et sélectionnez **Contrôle intégral du système**.  
Autrement, dans le menu **Actions**, sélectionnez **Contrôle intégral du système**.
2. Dans la boîte de dialogue **Contrôle intégral du système**, vérifiez les détails des ordinateurs à contrôler et cliquez sur **OK** pour lancer le contrôle.

**Remarque :** si le contrôle détecte les composants d'une menace dans la mémoire, il s'arrête et une alerte est envoyée à Enterprise Manager. En effet, la poursuite du contrôle pourrait permettre à la menace de se propager. Nettoyez l'ordinateur de la menace avant d'exécuter de nouveau le contrôle.

## 5.8 Nettoyage des ordinateurs

### 5.8.1 Nettoyage immédiat des ordinateurs

Vous pouvez procéder à un nettoyage immédiat des ordinateurs Windows 2000 et supérieur infectés par un virus ou ayant des applications indésirables.

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Actualisation - nettoyage** pour nettoyer les ordinateurs. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

**Remarque :** pour nettoyer les ordinateurs Mac ou Linux, vous pouvez soit configurer un nettoyage automatique depuis la console (reportez-vous à la section [Configuration du nettoyage automatique](#) à la page 45), soit nettoyer les ordinateurs individuellement comme le décrit la section [Gestion des éléments détectés en cas d'échec du nettoyage](#) à la page 44.

Si un élément (par exemple, un cheval de Troie ou une application potentiellement indésirable) a été “partiellement détecté”, avant de nettoyer l'ordinateur affecté, exécutez un contrôle intégral de l'ordinateur pour trouver tous les composants de l'élément partiellement détecté. Dans la liste des ordinateurs, vue **Ordinateurs d'extrémité**, cliquez avec le bouton droit de la souris sur l'ordinateur affecté et cliquez sur **Contrôle intégral du système**. Pour plus d'informations, reportez-vous à la section [Élément partiellement détecté](#) à la page 149.

Pour nettoyer les ordinateurs immédiatement :

1. Dans la liste des ordinateurs, vue **Ordinateurs d'extrémité**, cliquez avec le bouton droit de la souris sur le ou les ordinateurs que vous voulez nettoyer, puis cliquez sur **Résoudre les alertes et les erreurs**.
2. Dans la boîte de dialogue **Résolution des alertes et des erreurs**, sur l'onglet **Alertes**, sélectionnez la case à cocher de chaque élément que vous voulez nettoyer, ou cliquez sur **Sélectionner tout**. Cliquez sur **Nettoyage**.

En cas de nettoyage réussi, la liste des ordinateurs n'affiche plus les alertes.

Si une quelconque alerte demeure répertoriée, procédez à un nettoyage manuel des ordinateurs. Reportez-vous à la section [Gestion des éléments détectés en cas d'échec du nettoyage](#) à la page 44.

**Remarque :** le nettoyage de certains virus nécessite l'exécution d'un contrôle intégral du système qui essaye de nettoyer *tous* les virus. Cette opération peut prendre du temps. Les alertes sont mises à jour à la fin du contrôle.

## 5.8.2 Gestion des éléments détectés en cas d'échec du nettoyage

Si vous ne parvenez pas à nettoyer les ordinateurs depuis la console, procédez à un nettoyage manuel.

1. Dans la liste des ordinateurs, cliquez deux fois sur l'ordinateur infecté.
2. Dans la boîte de dialogue **Détails de l'ordinateur**, défilez jusqu'à la section **Alertes et erreurs à traiter**. Dans la liste des éléments détectés, cliquez sur le nom de l'élément que vous voulez supprimer de l'ordinateur.

Cette opération vous connecte au site Web de Sophos sur lequel vous pouvez lire des conseils sur le nettoyage de votre ordinateur.

3. Rendez-vous sur l'ordinateur et effectuez le nettoyage manuellement.

**Remarque :** le site Web de Sophos vous permet de télécharger des outils de désinfection spéciaux pour certains virus et vers.

### 5.8.3 Configuration du nettoyage automatique

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - antivirus et HIPS** pour effectuer cette tâche. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Vous pouvez nettoyer les ordinateurs automatiquement dès la découverte d'un virus ou de tout autre élément. Pour cela, modifiez les paramètres du contrôle sur accès et du contrôle planifié comme décrit ci-dessous :

**Remarque :** le contrôle sur accès ne peut pas nettoyer les adwares et les autres applications potentiellement indésirables (PUA). Traitez ceux-ci comme le décrit la section [Nettoyage immédiat des ordinateurs](#) à la page 43 ou activez le nettoyage automatique des adwares et des PUA pour les contrôles planifiés.

1. Vérifiez quelle stratégie antivirus et HIPS est utilisée par le ou les groupes d'ordinateurs que vous voulez configurer.  
Reportez-vous à la section [Vérification des stratégies utilisées par un groupe](#) à la page 23.
2. Dans le volet **Stratégies**, cliquez deux fois sur **Antivirus et HIPS**. Puis cliquez deux fois sur la stratégie que vous désirez changer.

La boîte de dialogue **Stratégie antivirus et HIPS** apparaît.

3. Configurez un nettoyage automatique pour le *contrôle sur accès*.
  - a) Dans le volet **Configurer l'antivirus et HIPS**, cliquez sur le bouton **Contrôle sur accès**.
  - b) Dans la boîte de dialogue **Paramètres de contrôle sur accès**, cliquez sur l'onglet **Nettoyage**.
  - c) Paramétrez les options comme décrit ci-dessous.

#### Virus/spywares

Sélectionnez **Nettoyer automatiquement les éléments contenant un virus/spyware**. Vous pouvez aussi spécifier ce que vous souhaitez faire des éléments en cas d'échec du nettoyage :

- Refuser l'accès uniquement
- Supprimer
- Refuser l'accès et déplacer dans l'emplacement par défaut
- Refuser l'accès et déplacer dans <chemin UNC>

#### Remarques

- Si vous sélectionnez **Refuser l'accès et déplacer dans** et que vous définissez un emplacement, les ordinateurs Mac OS X déplaceront quand même les éléments infectés dans l'emplacement par défaut.
- Les paramètres **Refuser l'accès et déplacer dans l'emplacement par défaut** et **Refuser l'accès et déplacer dans** ne s'appliquent pas aux ordinateurs Linux et seront ignorés par ceux-ci.

#### Fichiers suspects

**Remarque :** ces paramètres s'appliquent seulement à Windows 2000 et supérieur.

Vous pouvez spécifier l'action à entreprendre lors de la détection de fichiers suspects :

- Refuser l'accès uniquement
- Supprimer
- Refuser l'accès et déplacer dans l'emplacement par défaut
- Refuser l'accès et déplacer dans <chemin UNC>

4. Paramétrez le nettoyage automatique pour le *contrôle planifié*.

- a) Dans la boîte de dialogue **Stratégie antivirus et HIPS**, dans la zone **Contrôle planifié**, sélectionnez le contrôle et cliquez sur **Modifier**.
- b) Dans la boîte de dialogue **Paramètres du contrôle planifié**, cliquez sur **Configurer**.
- c) Dans la boîte de dialogue **Paramètres de contrôle et de nettoyage**, cliquez sur l'onglet **Nettoyage**.
- d) Paramétrez les options comme décrit ci-dessous.

#### **Virus/spywares**

Sélectionnez **Nettoyer automatiquement les éléments contenant un virus/spyware**. Vous pouvez aussi spécifier ce que vous souhaitez faire des éléments en cas d'échec du nettoyage :

- Journaliser uniquement
- Supprimer
- Déplacer dans l'emplacement par défaut ou Déplacer dans <chemin UNC>

#### **Remarques**

- Le déplacement d'un fichier exécutable réduit la probabilité de son exécution.
- Vous ne pouvez pas automatiquement déplacer une infection à plusieurs composants.

#### **Adwares et PUA**

**Remarque :** ce paramètre s'applique uniquement à Windows 2000 et supérieur.

Sélectionnez **Nettoyer automatiquement les adwares et les PUA**, si vous le souhaitez.

#### **Fichiers suspects**

Vous pouvez spécifier l'action à entreprendre lors de la détection de fichiers suspects :

- Journaliser uniquement
- Supprimer
- Déplacer dans l'emplacement par défaut ou Déplacer dans <chemin UNC>

#### **Remarques**

- Ces paramètres s'appliquent seulement à Windows 2000 et supérieur.
- Le déplacement d'un fichier exécutable réduit la probabilité de son exécution.
- Vous ne pouvez pas automatiquement déplacer une infection à plusieurs composants.

## 6 Mise à jour des ordinateurs

### 6.1 Configuration du gestionnaire de mise à jour

#### 6.1.1 Qu'est-ce que le gestionnaire de mise à jour ?

Le gestionnaire de mise à jour vous permet de configurer la mise à jour automatique des logiciels de sécurité Sophos depuis un site Web Sophos.

Enterprise Manager prend en charge un seul gestionnaire de mise à jour. Ce dernier est installé avec Enterprise Manager et administré depuis celui-ci.

Le gestionnaire de mise à jour est configuré lorsque vous exécutez l'**Assistant de téléchargement des logiciels de sécurité**, lequel démarre automatiquement lorsque vous ouvrez Enterprise Manager pour la première fois après l'installation.

Vous pouvez changer la configuration du gestionnaire de mise à jour ultérieurement, par exemple, si vous voulez distribuer les logiciels Sophos téléchargés sur des partages supplémentaires sur votre réseau.

#### 6.1.2 Comment fonctionne le gestionnaire de mise à jour ?

Une fois que vous avez configuré le gestionnaire de mise à jour, ce dernier :

- Se connecte, à une fréquence planifiée, à un magasin de distribution de données à Sophos ou sur votre réseau.
- Télécharge les mises à jour des données de détection des menaces et celles des logiciels de sécurité auxquels l'administrateur s'est abonné.
- Place les logiciels mis à jour dans un ou plusieurs partages réseau sous une forme adaptée à l'installation sur les ordinateurs d'extrémité.

Les ordinateurs se mettent à jour automatiquement depuis les partages, et ce, dans la mesure où les logiciels Sophos qui y sont installés ont été configurés pour cela, en appliquant, par exemple, une stratégie de mise à jour.

#### 6.1.3 Visualisation ou modification de la configuration du gestionnaire de mise à jour

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - mise à jour** pour configurer le gestionnaire de mise à jour. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

1. Si vous êtes dans la vue **Ordinateurs d'extrémité**, cliquez sur le bouton **Gestionnaires de mise à jour** sur la barre d'outils pour afficher la vue **Gestionnaires de mise à jour**.

2. Dans la liste des ordinateurs, sélectionnez le gestionnaire de mise à jour. Cliquez avec le bouton droit de la souris, puis cliquez sur **Voir/Modifier la configuration**.

**Remarque :** sinon, sélectionnez le gestionnaire de mise à jour, allez dans le menu **Actions**, choisissez **Gestionnaire de mise à jour**, puis cliquez sur **Voir/Modifier la configuration**.

La boîte de dialogue **Configuration du gestionnaire de mise à jour** apparaît.

3. Modifiez la configuration comme le décrivent les sections suivantes :
  - [Sélection d'une source de mise à jour pour le gestionnaire de mise à jour](#) à la page 48.
  - [Sélection des logiciels à télécharger](#) à la page 49.
  - [Détermination de l'emplacement des logiciels](#) à la page 49.
  - [Création ou modification d'une planification des mises à jour](#) à la page 51.
  - [Configuration du journal du gestionnaire de mise à jour](#) à la page 52.
  - [Configuration de la mise à jour automatique d'un gestionnaire de mise à jour](#) à la page 52.

Pour plus d'informations sur la manière d'effacer les alertes du gestionnaire de mise à jour depuis la console, reportez-vous à la section [Effacement des alertes du gestionnaire de mise à jour depuis la console](#) à la page 42.

Après avoir configuré le gestionnaire de mise à jour, vous pouvez configurer vos stratégies de mise à jour et les appliquer aux ordinateurs d'extrémité.

#### 6.1.4 Sélection d'une source de mise à jour pour le gestionnaire de mise à jour

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - mise à jour** pour configurer le gestionnaire de mise à jour. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Sélectionnez une source à partir de laquelle le gestionnaire de mise à jour téléchargera les logiciels de sécurité et les mises à jour en vue d'une distribution sur l'ensemble du réseau.

1. Si vous êtes dans la vue **Ordinateurs d'extrémité**, cliquez sur le bouton **Gestionnaires de mise à jour** sur la barre d'outils pour afficher la vue **Gestionnaires de mise à jour**.
2. Dans la liste des ordinateurs, sélectionnez le gestionnaire de mise à jour. Cliquez avec le bouton droit de la souris, puis cliquez sur **Voir/Modifier la configuration**.
3. Dans la boîte de dialogue **Configuration du gestionnaire de mise à jour**, sur l'onglet **Sources**, cliquez sur **Ajouter**.
4. Dans la boîte de dialogue **Détails de la source**, dans le champ **Adresse**, sélectionnez **Sophos** pour télécharger les logiciels et les mises à jour directement depuis Sophos.
5. Dans les champs **Nom utilisateur** et **Mot de passe**, saisissez les codes d'accès de téléchargement fournis par Sophos.

6. Si vous accédez à Internet via un serveur proxy, sélectionnez **Utiliser un serveur proxy pour se connecter**. Puis saisissez l'**Adresse** et le numéro du **Port** du serveur proxy. Saisissez un **Nom utilisateur** et un **Mot de passe** qui donnent accès au serveur proxy. Si le nom utilisateur doit avoir une qualification pour indiquer le domaine, utilisez la forme domaine\nomutilisateur. Cliquez sur OK.

La nouvelle source apparaît dans la liste de la boîte de dialogue **Configuration du gestionnaire de mise à jour**.

### 6.1.5 Sélection des logiciels à télécharger

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - mise à jour** pour configurer le gestionnaire de mise à jour. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Sélectionnez les abonnements que le gestionnaire de mise à jour va mettre à jour.

1. Si vous êtes dans la vue **Ordinateurs d'extrémité**, cliquez sur le bouton **Gestionnaires de mise à jour** sur la barre d'outils pour afficher la vue **Gestionnaires de mise à jour**.
2. Dans la liste des ordinateurs, sélectionnez le gestionnaire de mise à jour. Cliquez avec le bouton droit de la souris, puis cliquez sur **Voir/Modifier la configuration**.
3. Dans la boîte de dialogue **Configuration du gestionnaire de mise à jour**, sur l'onglet **Abonnements**, sélectionnez l'abonnement logiciels dans la liste des abonnements disponibles.  
Pour voir les détails d'un abonnement, par exemple, quels logiciels il inclut, cliquez sur **Voir les détails**.
4. Pour déplacer l'abonnement sélectionné dans la liste "Abonné à", cliquez sur le bouton "Ajouter".



Pour déplacer tous les abonnements dans la liste "Abonné à", cliquez sur le bouton "Ajouter tout".



Pour plus d'informations sur les abonnements, reportez-vous à la section [À propos des abonnements logiciels](#) à la page 54.

### 6.1.6 Détermination de l'emplacement des logiciels

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - mise à jour** pour configurer le gestionnaire de mise à jour. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Après avoir sélectionné les logiciels à télécharger, vous pouvez déterminer où ils doivent être placés sur le réseau. Par défaut, les logiciels sont placés dans un partage UNC

\\<NomOrdinateur>\SophosUpdate, où NomOrdinateur est le nom de l'ordinateur sur lequel le gestionnaire de mise à jour est installé.

Vous pouvez distribuer les logiciels téléchargés sur les partages supplémentaires de votre réseau. Pour cela, ajoutez un partage réseau existant dans la liste des partages disponibles, puis déplacez-le dans la liste des partages de mise à jour comme décrit ci-dessous. Autrement, assurez-vous que le compte **SophosUpdateMgr** dispose des droits en lecture sur ces partages.

Pour une liste des plates-formes sur lesquelles les partages réseau sont pris en charge, reportez-vous à la section [Sur quelles plates-formes les partages réseau sont-ils pris en charge ?](#) à la page 50

Pour déterminer où les logiciels sont placés :

1. Si vous êtes dans la vue **Ordinateurs d'extrémité**, cliquez sur le bouton **Gestionnaires de mise à jour** sur la barre d'outils pour afficher la vue **Gestionnaires de mise à jour**.
2. Dans la liste des ordinateurs, sélectionnez le gestionnaire de mise à jour. Cliquez avec le bouton droit de la souris, puis cliquez sur **Voir/Modifier la configuration**.
3. Dans la boîte de dialogue **Configuration du gestionnaire de mise à jour**, sur l'onglet **Distribution**, sélectionnez un abonnement logiciels dans la liste.
4. Sélectionnez un partage dans la liste des partages "Disponibles" et déplacez-le dans la liste "Mettre à jour dans" en cliquant sur le bouton "Ajouter" (>).

Le partage par défaut \\<NomOrdinateur>\SophosUpdate est toujours présent dans la liste "Mettre à jour dans". Vous ne pouvez pas supprimer ce partage de la liste.

La liste des partages "Disponibles" inclut tous les partages que Enterprise Manager connaît.

Vous pouvez ajouter un partage existant dans la liste des partages "Disponibles" ou enlever un à l'aide du bouton "Ajouter" (>) ou "Supprimer" (<).

5. Si vous voulez saisir une description de partage ou les codes d'accès nécessaires pour écrire dans le partage, sélectionnez ce dernier et cliquez sur **Configurer**. Dans la boîte de dialogue **Gestionnaire des partages**, saisissez la description et les codes d'accès.

Si vous voulez entrer les mêmes codes d'accès pour plusieurs partages, sélectionnez les partages dans la liste "Mettre à jour dans" et cliquez sur **Configurer**. Dans la boîte de dialogue **Configuration de plusieurs partages**, saisissez les codes d'accès qui seront utilisés pour écrire sur les partages.

### 6.1.7 Sur quelles plates-formes les partages réseau sont-ils pris en charge ?

Les partages réseau sur les plates-formes suivantes sont pris en charge :

- Partages sous Windows NT et supérieur.
- Partages Samba hébergés sur un serveur Linux, par exemple, SUSE Linux Enterprise 10 (SLES 10).
- Partages Samba hébergés sur Netware 5.1 SP3 et Netware 6.5 SP3 à SP7, noyau Netware.
- Partages Samba hébergés sur Mac OSX 10.2 ou supérieur.
- Partages Samba hébergés sur Unix.

- Partages Novell Storage Services (NSS) prenant en charge l'authentification NDS, hébergés sur Novell Open Enterprise Server 1 et 2, noyau Linux.
- Partages Netware File System (NFS) prenant en charge l'authentification NDS, hébergés sur Netware 5.1 SP3 et Netware 6.5 SP3 à SP7, noyau Netware.
- Systèmes de fichiers NetApp.
- Partages Samba hébergés sur Novell Open Enterprise Server 1 et 2.
- Partages Novell Storage Services (NSS) prenant en charge l'authentification NDS, hébergés sur Netware 5.1 SP3 et Netware 6.5 SP3 à SP7, noyau Netware.

### 6.1.8 Création ou modification d'une planification des mises à jour

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - mise à jour** pour configurer le gestionnaire de mise à jour. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Par défaut, le gestionnaire de mise à jour vérifie dans la banque de données Sophos les mises à jour des **données de détection des menaces** toutes les 10 minutes.

Vous pouvez changer cet intervalle de mise à jour. Le minimum est 5 minutes et le maximum 1 440 minutes (24 heures). Nous vous conseillons de choisir un intervalle de mise à jour de 10 minutes pour les données de détection des menaces pour que vous receviez une protection contre les nouvelles menaces immédiatement après la publication par Sophos de ces données de détection.

Par défaut, le gestionnaire de mise à jour vérifie dans la banque de données Sophos les mises à jour des **logiciels** toutes les 60 minutes.

Vous pouvez changer cet intervalle de mise à jour. Le minimum est 10 minutes et le maximum 1 440 minutes (24 heures).

Pour les mises à jour logicielles, vous pouvez soit spécifier un intervalle de mise à jour utilisé toutes les heures chaque jour, soit créer des planifications plus sophistiquées où chaque jour peut être défini indépendamment et divisé en périodes avec des intervalles de mise à jour différents.

**Remarque :** vous pouvez créer une planification différente pour chaque jour de la semaine. Seule une planification peut être associée à un jour de la semaine.

1. Si vous êtes dans la vue **Ordinateurs d'extrémité**, cliquez sur le bouton **Gestionnaires de mise à jour** sur la barre d'outils pour afficher la vue **Gestionnaires de mise à jour**.
2. Dans la liste des ordinateurs, sélectionnez le gestionnaire de mise à jour. Cliquez avec le bouton droit de la souris, puis cliquez sur **Voir/Modifier la configuration**.
3. Dans la boîte de dialogue **Configuration du gestionnaire de mise à jour**, sur l'onglet **Planification**, saisissez l'intervalle entre les mises à jour des données de détection des menaces.
4. Saisissez l'intervalle entre les mises à jour des logiciels.
  - Si vous voulez spécifier un intervalle de mise à jour qui est utilisé toutes les heures chaque jour, sélectionnez l'option **Vérifier les mises à jour toutes les n minutes** et saisissez l'intervalle en minutes.

- Si vous voulez créer une planification plus sophistiquée ou des planifications différentes suivant les jours de la semaine, sélectionnez l'option **Configurer et gérer les mises à jour planifiées** et cliquez sur **Ajouter**.

Dans la boîte de dialogue **Planification des mises à jour**, saisissez un nom de planification, sélectionnez les jours de la semaine et les intervalles de mise à jour.

### 6.1.9 Configuration du journal du gestionnaire de mise à jour

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - mise à jour** pour configurer le gestionnaire de mise à jour. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

1. Si vous êtes dans la vue **Ordinateurs d'extrémité**, cliquez sur le bouton **Gestionnaires de mise à jour** sur la barre d'outils pour afficher la vue **Gestionnaires de mise à jour**.
2. Dans la liste des ordinateurs, sélectionnez le gestionnaire de mise à jour. Cliquez avec le bouton droit de la souris, puis cliquez sur **Voir/Modifier la configuration**.
3. Dans la boîte de dialogue **Configuration du gestionnaire de mise à jour**, sur l'onglet **Journalisation**, sélectionnez pour combien de jours vous voulez conserver le journal et la taille maximale de ce dernier.

### 6.1.10 Configuration de la mise à jour automatique d'un gestionnaire de mise à jour

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - mise à jour** pour configurer le gestionnaire de mise à jour. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

1. Si vous êtes dans la vue **Ordinateurs d'extrémité**, cliquez sur le bouton **Gestionnaires de mise à jour** sur la barre d'outils pour afficher la vue **Gestionnaires de mise à jour**.
2. Dans la liste des ordinateurs, sélectionnez le gestionnaire de mise à jour. Cliquez avec le bouton droit de la souris, puis cliquez sur **Voir/Modifier la configuration**.
3. Dans la boîte de dialogue **Configuration du gestionnaire de mise à jour**, sur l'onglet **Avancés**, sélectionnez une version du gestionnaire de mise à jour avec laquelle vous voulez rester à jour.

Enterprise Manager prend seulement en charge la version "recommandée" du gestionnaire de mise à jour. Cela signifie que le gestionnaire de mise à jour sera toujours mis à niveau vers la version qui est identifiée comme telle pour Sophos. La version même du gestionnaire de mise à jour changera.

### 6.1.11 Demande de vérification immédiate des mises à jour au gestionnaire de mise à jour

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Actualisation - mise à jour et contrôle** pour effectuer cette tâche. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Après avoir configuré le gestionnaire de mise à jour, ce dernier vérifie les mises à jour et les télécharge depuis sa source de mise à jour dans les partages de mise à jour qu'il gère automatiquement en fonction de la planification donnée. Si vous voulez que le gestionnaire de mise à jour vérifie et télécharge immédiatement les mises à jour des données de détection des menaces, les mises à jour logicielles pour les systèmes d'extrémité et les mises à jour logicielles pour le gestionnaire de mise à jour lui-même, procédez aux étapes suivantes :

1. Si vous êtes dans la vue **Ordinateurs d'extrémité**, cliquez sur le bouton **Gestionnaires de mise à jour** sur la barre d'outils pour afficher la vue **Gestionnaires de mise à jour**.
2. Dans la liste des ordinateurs, sélectionnez le gestionnaire de mise à jour, cliquez avec le bouton droit de la souris et cliquez sur **Mettre à jour maintenant**.

### 6.1.12 Surveillance du gestionnaire de mise à jour

1. Si vous êtes dans la vue **Ordinateurs d'extrémité**, cliquez sur le bouton **Gestionnaires de mise à jour** sur la barre d'outils pour afficher la vue **Gestionnaires de mise à jour**.
2. Dans la liste des ordinateurs, vérifiez s'il y a d'éventuels problèmes dans les colonnes **Alertes** et **Erreurs**.
3. Si une alerte ou une erreur apparaît près du gestionnaire de mise à jour, cliquez avec le bouton droit de la souris sur ce dernier et cliquez sur **Voir les détails du gestionnaire de mise à jour**.

Dans la boîte de dialogue **Détails du gestionnaire de mise à jour**, vous pouvez voir l'heure des dernières mises à jour des données de détection des menaces et des logiciels, l'état de l'abonnement ou des abonnements que le gestionnaire de mise à jour maintient à jour ainsi que l'état de ce dernier.

4. Pour en savoir plus sur l'état d'un gestionnaire de mise à jour donné et pour avoir plus d'informations sur les moyens de l'exploiter, suivez le lien dans la colonne **Description**.

**Remarque :** la section **Mises à jour** du tableau de bord ne signale pas d'alerte ou d'erreur si le gestionnaire de mise à jour est temporairement incapable de mettre à jour. Des alertes et des erreurs sont générées seulement si la durée écoulée depuis la dernière mise à jour du gestionnaire de mise à jour dépasse le seuil d'alerte ou critique défini dans [Configuration du Tableau de bord](#) à la page 36.

### 6.1.13 Demande au gestionnaire de mise à jour de se mettre en conformité avec les paramètres de configuration

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Actualisation - mise à jour et contrôle** pour effectuer cette tâche. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

1. Si vous êtes dans la vue **Ordinateurs d'extrémité**, cliquez sur le bouton **Gestionnaires de mise à jour** sur la barre d'outils pour afficher la vue **Gestionnaires de mise à jour**.
2. Dans la liste des ordinateurs, sélectionnez le gestionnaire de mise à jour, cliquez avec le bouton droit de la souris et cliquez sur **Mettre en conformité avec la configuration**.

## 6.1.14 Publication des logiciels de sécurité sur un serveur Web

Vous pouvez, si vous le souhaitez, publier les logiciels de sécurité Sophos sur un serveur Web pour que les ordinateurs disposent d'un accès via HTTP.

Pour publier les logiciels de sécurité sur un serveur Web, procédez de la manière suivante :

1. Pour connaître le chemin du dossier partagé, connu sous le nom d'emplacement des fichiers d'amorce, dans lequel les logiciels de sécurité ont été téléchargés :

- a) Dans Enterprise Manager, dans le menu **Affichage**, cliquez sur **Emplacements des fichiers d'amorce**.

Dans la boîte de dialogue **Emplacements des fichiers d'amorce**, la colonne **Emplacement** affiche le chemin de l'emplacement des fichiers d'amorce pour chaque plate-forme.

- b) Notez le chemin jusqu'au dossier CID mais sans l'inclure. Par exemple :  
`\\nom_serveur\SophosUpdate`

2. Mettez l'emplacement des fichiers d'amorce, y compris les sous-dossiers, à disposition sur le serveur Web.

3. Spécifiez les noms utilisateur et mots de passe pour empêcher tout accès non autorisé à ce dossier sur le serveur Web.

**Remarque :** la documentation de votre serveur Web doit expliquer comment partager un dossier sur le Web et comment paramétrer les noms utilisateur et les mots de passe. Pour plus d'informations sur la manière de procéder, veuillez contacter le fabricant du serveur Web.

## 6.2 Configuration des abonnements logiciels

### 6.2.1 À propos des abonnements logiciels

Un abonnement logiciels permet de spécifier quelles versions des logiciels pour ordinateurs d'extrémité sont téléchargées depuis Sophos pour chaque plate-forme.

L'**Assistant de téléchargement des logiciels de sécurité** définit un abonnement par défaut appelé "Recommandé." Cet abonnement inclut les versions de tous les logiciels sélectionnés dont l'utilisation est recommandée et vous garantit la mise à jour automatique de votre logiciel.

Si vous avez sélectionné toutes les plates-formes que vous souhaitez protéger dans l'assistant, il n'est pas nécessaire de configurer les abonnements logiciels. Si vous souhaitez ajouter une protection pour une nouvelle plate-forme, configurez l'abonnement comme le décrit la section [Abonnement aux logiciels de sécurité](#) à la page 55.

Si vous n'avez pas effectué toutes les tâches de l'assistant après avoir installé Enterprise Manager, reportez-vous à la section [Exécution de l'Assistant de téléchargement des logiciels de sécurité](#) à la page 55.

## 6.2.2 Abonnement aux logiciels de sécurité

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - mise à jour** pour modifier un abonnement logiciels. Pour plus d'informations sur l'administration déléguée, reportez-vous à la section [À propos des rôles](#) à la page 15.

Pour vous abonner aux logiciels de sécurité :

1. Dans le menu **Affichage**, cliquez sur **Gestionnaire de mise à jour**.
2. Dans le volet **Abonnements logiciels**, cliquez deux fois sur l'abonnement que vous souhaitez modifier ou cliquez sur le bouton **Ajouter** en haut du volet pour créer un nouvel abonnement.

La boîte de dialogue **Abonnement logiciels** apparaît.

Sinon, si vous voulez créer une copie d'un abonnement existant, sélectionnez l'abonnement, cliquez dessus avec le bouton droit de la souris et cliquez sur **Dupliquer l'abonnement**.

Saisissez un nouveau nom d'abonnement, puis cliquez deux fois dessus pour ouvrir la boîte de dialogue **Abonnement logiciels**.

3. Dans la boîte de dialogue **Abonnement logiciels**, modifiez le nom de l'abonnement, si vous le souhaitez.
4. Sélectionnez les plates-formes pour lesquelles vous souhaitez télécharger les logiciels.
5. Pour chacune des plates-formes sélectionnées, cliquez dans le champ **Version** situé à côté de la plate-forme et cliquez une nouvelle fois. Dans la liste du menu déroulant des versions disponibles, sélectionnez la version que vous souhaitez télécharger, par exemple, *9.7 Recommandé(e)*.

**Important :** sélectionnez une version fixe (par exemple, *9.7.1*) uniquement si le support technique de Sophos vous a conseillé de le faire.

Si vous avez créé un nouvel abonnement logiciels, configurez le gestionnaire de mise à jour pour le maintenir à jour comme le décrit la section [Visualisation ou modification de la configuration du gestionnaire de mise à jour](#) à la page 47.

Vous pouvez aussi paramétrer les alertes par courriel d'abonnement logiciels. Pour plus d'informations sur ces alertes, reportez-vous à la section [Configuration des alertes d'abonnement logiciels](#) à la page 121.

## 6.2.3 Exécution de l'Assistant de téléchargement des logiciels de sécurité

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - mise à jour** pour exécuter l'**Assistant de téléchargement des logiciels de sécurité**. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Si vous n'avez pas terminé l'**Assistant de téléchargement des logiciels de sécurité** après avoir installé Enterprise Manager, procédez ainsi :

- Dans le menu **Actions**, cliquez sur **Exécuter l'Assistant de téléchargement des logiciels de sécurité**.

L'**Assistant d'abonnement aux mises à jour Sophos** vous guide tout au long des opérations de sélection et de téléchargement des logiciels.

## 6.2.4 Comment savoir quelles stratégies de mise à jour utilisent l'abonnement logiciels

Pour voir quelles stratégies de mise à jour utilisent un abonnement logiciels donné :

- Sélectionnez l'abonnement, cliquez avec le bouton droit de la souris, puis cliquez sur **Voir l'utilisation de l'abonnement**.

Dans la boîte de dialogue **Utilisation des abonnements logiciels**, une liste des stratégies de mise à jour qui utilisent l'abonnement apparaît.

## 6.3 Configuration de la stratégie de mise à jour

### 6.3.1 À propos de la stratégie de mise à jour

La mise à jour des stratégies vous permet de maintenir vos ordinateurs à jour avec vos logiciels de sécurité choisis. Enterprise Manager vérifie les mises à jour et met à jour les ordinateurs, si nécessaire, dans un intervalle donné.

La stratégie de mise à jour par défaut vous permet d'installer et de mettre à jour les logiciels spécifiés dans l'abonnement "Recommandé".

Si vous voulez changer la stratégie de mise à jour par défaut ou en créer une nouvelle, suivez les instructions dans les sections suivantes.

- [Sélection d'un abonnement](#) à la page 56
- [À propos des emplacements du serveur de mise à jour](#) à la page 57
- [Planification des mises à jour](#) à la page 60
- [Sélection d'une source différente pour l'installation initiale](#) à la page 60
- [Journalisation des mises à jour](#) à la page 61

**Remarque :** si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - mise à jour** pour configurer une stratégie de mise à jour. Pour plus d'informations sur l'administration déléguée, reportez-vous à la section [À propos des rôles](#) à la page 15.

### 6.3.2 Sélection d'un abonnement

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - mise à jour** pour configurer une stratégie de mise à jour. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Un abonnement permet de spécifier quelles versions des logiciels pour ordinateurs d'extrémité sont téléchargées depuis Sophos pour chaque plate-forme. L'abonnement par défaut inclut les derniers logiciels pour Windows 2000 et supérieur.

Pour sélectionner un abonnement :

1. Vérifiez quelle stratégie de mise à jour est utilisée par le ou les groupes d'ordinateurs que vous désirez configurer.  
Reportez-vous à la section [Vérification des stratégies utilisées par un groupe](#) à la page 23.
2. Dans le volet **Stratégies**, cliquez deux fois sur **Mise à jour**. Puis cliquez deux fois sur la stratégie que vous désirez changer.
3. Dans la boîte de dialogue **Stratégie de mise à jour**, cliquez sur l'onglet **Abonnement** et sélectionnez l'abonnement pour les logiciels que vous souhaitez maintenir à jour.

### 6.3.3 Configuration des emplacements du serveur de mise à jour

#### 6.3.3.1 À propos des emplacements du serveur de mise à jour

Par défaut, les ordinateurs se mettent à jour à partir d'une seule source principale de mise à jour dans un partage UNC, \\<NomOrdinateur>\SophosUpdate, où <NomOrdinateur> correspond au nom de l'ordinateur du gestionnaire de mise à jour. Vous pouvez spécifier une source secondaire pour les mises à jour et activer l'itinérance. Si les ordinateurs d'extrémité ne sont pas en mesure de contacter leur source principale, ils tentent de se mettre à jour depuis leur source secondaire (si elle a été spécifiée). Nous vous recommandons de toujours spécifier une source secondaire.

L'emplacement des serveurs de mise à jour principal et l'emplacement des serveurs de mise à jour secondaire peuvent soit être des partages UNC, soit des URL HTTP depuis tout gestionnaire de mise à jour sur votre réseau. L'emplacement des serveurs de mise à jour secondaire peut aussi être paramétré pour récupérer les mises à jour directement depuis Sophos sur Internet via HTTP.

**Remarque :** le gestionnaire de mise à jour peut avoir plusieurs partages de distribution à disposition selon la manière dont vous l'avez configuré.

#### 6.3.3.2 À propos de l'itinérance pour les ordinateurs portables

Certains utilisateurs d'ordinateurs portables effectuent de nombreux déplacements domestiques ou internationaux au sein d'une entreprise. Lorsque l'itinérance est activée (sur une stratégie de mise à jour pour les ordinateurs portables itinérants), les ordinateurs portables itinérants tentent de rechercher et de se mettre à jour à partir de l'emplacement de serveurs de mise à jour le plus proche en envoyant des requêtes aux autres ordinateurs d'extrémité (fixes) du réseau local auxquels ils sont connectés, réduisant ainsi les délais de mise à jour et les coûts de bande passante.

Un ordinateur portable itinérant récupère les emplacements des serveurs de mise à jour et les codes d'accès en envoyant des requêtes aux ordinateurs fixes du même réseau local. S'il reçoit plusieurs emplacements, l'ordinateur portable détermine lequel est le plus proche et l'utilise. Si aucun emplacement ne fonctionne, l'ordinateur portable utilise l'emplacement principal (puis l'emplacement secondaire) défini dans sa stratégie de mise à jour.

**Remarque :** lorsque les ordinateurs fixes envoient les emplacements de mise à jour et les codes d'accès à l'ordinateur portable, les mots de passe sont brouillés lors de la transmission et du stockage. En revanche, les comptes définis pour les ordinateurs d'extrémité pour pouvoir lire les emplacements des serveurs de mise à jour doivent toujours être aussi restrictifs que possible

et permettre uniquement un accès en lecture seule. Reportez-vous à la section [Détermination de l'emplacement des logiciels](#) à la page 49.

L'itinérance peut uniquement être utilisée lorsque :

- Il n'y a qu'un seul Enterprise Manager commun aux ordinateurs d'extrémité itinérants et fixes.
- Les ordinateurs d'extrémité fixes utilisent le même abonnement logiciels que les ordinateurs portables itinérants.
- Les ordinateurs d'extrémité fixes et itinérants utilisent la version 4.7 ou supérieure d'Enterprise Manager et la version 9.7 d'Endpoint Security and Control.
- Tous les pare-feu tiers sont configurés afin de permettre aux requêtes et aux réponses d'emplacements de mise à jour. Le port normalement utilisé est le port 51235 mais il peut être configuré. Pour plus de détails, consultez l'article <http://www.sophos.fr/support/knowledgebase/article/110371.html>.

Activez l'itinérance lors de la spécification des sources de mises à jour. Pour plus d'instructions sur la manière de procéder, reportez-vous à la section [Changement des codes d'accès du serveur principal](#) à la page 58.

### 6.3.3.3 Changement des codes d'accès du serveur principal

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - mise à jour** pour configurer une stratégie de mise à jour. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Pour changer les codes d'accès du serveur principal :

1. Dans le volet **Stratégies**, cliquez deux fois sur **Mise à jour**. Puis cliquez deux fois sur la stratégie de mise à jour que vous désirez changer.
2. Dans la boîte de dialogue **Stratégie de mise à jour**, sur l'onglet **Serveur principal**, entrez les nouveaux codes d'accès qui seront utilisés pour accéder au serveur. Changez les autres détails, si besoin est.
3. Dans le volet **Groupes**, sélectionnez un groupe qui utilise la stratégie de mise à jour que vous venez de changer. Cliquez avec le bouton droit de la souris et sélectionnez **Mettre en conformité avec, Stratégie de mise à jour du groupe**.

Répétez cette étape pour chaque groupe qui utilise cette stratégie de mise à jour.

### 6.3.3.4 Paramétrage de l'emplacement du serveur de mise à jour secondaire

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - mise à jour** pour configurer une stratégie de mise à jour. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Pour paramétrer l'emplacement du serveur de mise à jour secondaire :

1. Vérifiez quelle stratégie de mise à jour est utilisée par le ou les groupes d'ordinateurs que vous désirez configurer.  
Reportez-vous à la section [Vérification des stratégies utilisées par un groupe](#) à la page 23.
2. Dans le volet **Stratégies**, cliquez deux fois sur **Mise à jour** puis cliquez deux fois sur la stratégie que vous souhaitez modifier.

3. Dans la boîte de dialogue **Stratégie de mise à jour**, cliquez sur l'onglet **Serveur secondaire** et sélectionnez la case à cocher **Spécifier les détails du serveur secondaire**.
4. Dans le champ **Adresse (HTTP ou UNC)**, procédez de la manière suivante :
  - Saisissez l'URL HTTP ou le chemin du réseau UNC du partage du serveur de mise à jour.
  - Sélectionnez **Sophos**.

**Important :** si vous choisissez une URL HTTP ou un partage qui n'est pas maintenu par un Gestionnaire de mise à jour géré, Enterprise Manager ne pourra pas vérifier si l'abonnement logiciels spécifié est disponible. Assurez-vous que le partage contient l'abonnement logiciels spécifié sinon les ordinateurs ne seront pas mis à jour.

5. Si la stratégie inclut des ordinateurs Mac et si vous avez spécifié un chemin UNC dans le champ **Adresse**, sous **Sélectionner un protocole de partage de fichiers pour Mac OS X**, sélectionnez un protocole pour que les Macs puissent accéder au partage de mise à jour.
6. Si nécessaire, dans le champ **Nom utilisateur**, saisissez le nom utilisateur du compte qui sera utilisé pour accéder au serveur, puis saisissez et confirmez le mot de passe. Pour HTTP Sophos, il s'agit de vos codes d'accès d'abonnement.

Ce compte doit avoir les droits d'accès en lecture seule (navigation) sur le partage que vous avez saisi dans le champ de l'adresse ci-dessus.

**Remarque :** si le nom utilisateur doit avoir une qualification pour indiquer le domaine, utilisez la forme domaine\nomutilisateur. Pour plus d'informations sur la manière de vérifier un compte utilisateur Windows, reportez-vous à l'article 11637 de la base de connaissances (<http://www.sophos.fr/support/knowledgebase/article/11637.html>).

7. Pour réduire la bande passante, cliquez sur **Avancés**. Dans la boîte de dialogue **Paramètres avancés**, sélectionnez **Limiter la quantité de bande passante utilisée** et utilisez le curseur pour spécifier la bande passante maximum en Ko/seconde.
8. Si vous accédez à Internet via un serveur proxy, cliquez sur **Détails du proxy**. Dans la boîte de dialogue **Détails du proxy**, sélectionnez la case **Accéder au serveur via un proxy** et saisissez ensuite l'**Adresse** du serveur proxy et son numéro de **Port**. Saisissez un **Nom utilisateur** et un **Mot de passe** qui donnent accès au serveur proxy. Si le nom utilisateur doit avoir une qualification pour indiquer le domaine, utilisez la forme domaine\nomutilisateur.

**Remarque :** sachez que certains fournisseurs de service Internet exigent que les requêtes HTTP soient envoyées au serveur proxy.

9. Cliquez sur **OK** pour fermer la boîte de dialogue **Stratégie de mise à jour**.
10. Dans le volet **Groupes**, cliquez avec le bouton droit de la souris sur un groupe qui utilise la stratégie de mise à jour que vous venez de changer et cliquez sur **Mettre en conformité avec > Stratégie de mise à jour du groupe**.

Répétez cette étape pour chaque groupe qui utilise cette stratégie de mise à jour.

### 6.3.4 Planification des mises à jour

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - mise à jour** pour configurer une stratégie de mise à jour. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Par défaut, les ordinateurs d'extrémité vérifient les mises à jour dans le partage réseau toutes les 5 minutes.

**Remarque :** cet intervalle de mise à jour ne s'applique pas si les ordinateurs téléchargent les mises à jour directement depuis Sophos. Les ordinateurs utilisant Sophos PureMessage peuvent vérifier les mises à jour toutes les 15 minutes. Les ordinateurs n'utilisant pas Sophos PureMessage se mettront à jour toutes les 60 minutes.

Pour spécifier l'intervalle de mise à jour :

1. Vérifiez quelle stratégie de mise à jour est utilisée par le ou les groupes d'ordinateurs que vous désirez configurer.  
Reportez-vous à la section [Vérification des stratégies utilisées par un groupe](#) à la page 23.
2. Dans le volet **Stratégies**, cliquez deux fois sur **Mise à jour**. Puis cliquez deux fois sur la stratégie que vous désirez changer.
3. Dans la boîte de dialogue **Stratégie de mise à jour**, sur l'onglet **Planification**, laissez **Permettre l'utilisation automatique des mises à jour aux ordinateurs** sélectionné. Saisissez l'intervalle entre les mises à jour logicielles (en minutes).
4. Si les ordinateurs se mettent à jour via une connexion modem à Internet, sélectionnez **Vérifier les mises à jour à la connexion**.

Les ordinateurs tenteront alors d'effectuer la mise à jour chaque fois qu'ils se connecteront à Internet.

### 6.3.5 Sélection d'une source différente pour l'installation initiale

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - mise à jour** pour configurer une stratégie de mise à jour. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Par défaut, les logiciels de sécurité sont installés sur les ordinateurs, puis maintenus à jour depuis la source spécifiée sur l'onglet **Serveur principal**. Vous pouvez spécifier une source différente pour l'installation initiale

**Remarque :**

Ce paramètre s'applique uniquement aux ordinateurs Windows 2000 et supérieur.

Si votre serveur principal est une adresse HTTP (Web) et si vous souhaitez effectuer l'installation sur les ordinateurs depuis la console, vous devez spécifier une source d'installation initiale.

Pour effectuer l'installation initiale depuis une source différente :

1. Vérifiez quelle stratégie de mise à jour est utilisée par le ou les groupes d'ordinateurs que vous désirez configurer.  
Reportez-vous à la section [Vérification des stratégies utilisées par un groupe](#) à la page 23.

2. Dans le volet **Stratégies**, cliquez deux fois sur **Mise à jour**. Puis cliquez deux fois sur la stratégie que vous désirez changer.
3. Dans la boîte de dialogue **Stratégie de mise à jour**, sur l'onglet **Source d'installation initiale**, dessélectionnez la case à cocher **Utiliser l'adresse du serveur principal**. Puis saisissez l'adresse de la source que vous souhaitez utiliser.

### 6.3.6 Journalisation des mises à jour

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - mise à jour** pour configurer une stratégie de mise à jour. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Par défaut, les ordinateurs enregistrent leur activité de mise à jour. La taille maximale du journal par défaut est de 1 Mo. Le niveau du journal par défaut est normal.

Pour changer les paramètres de journalisation :

1. Vérifiez quelle stratégie de mise à jour est utilisée par le ou les groupes d'ordinateurs que vous désirez configurer.  
Reportez-vous à la section [Vérification des stratégies utilisées par un groupe](#) à la page 23.
2. Dans le volet **Stratégies**, cliquez deux fois sur **Mise à jour**. Puis cliquez deux fois sur la stratégie que vous désirez changer.
3. Dans la boîte de dialogue **Stratégie de mise à jour**, sur l'onglet **Journalisation**, laissez **Enregistrer l'activité de Sophos AutoUpdate** sélectionné. Dans le champ **Taille maximale du journal**, spécifiez une taille maximale du journal en Mo.
4. Dans le champ **Niveau du journal**, sélectionnez **Normal** ou **Détaillé**.  
La journalisation détaillée fournit des informations sur beaucoup plus d'activités que le journal normal c'est pourquoi il prend du volume plus rapidement. Utilisez ce paramétrage uniquement lorsqu'une journalisation détaillée est nécessaire pour la résolution des problèmes.

## 6.4 Mise à jour des ordinateurs non à jour

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Correction - mise à jour et contrôle** pour mettre à jour les ordinateurs. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Après avoir configuré les stratégies de mise à jour et les avoir appliqué à vos ordinateurs en réseau, les ordinateurs sont maintenus à jour automatiquement. Il n'est pas nécessaire de mettre les ordinateurs à jour manuellement sauf en cas de problème avec la mise à jour.

Si, dans la vue **Ordinateurs d'extrémité**, dans la liste des ordinateurs, vous voyez l'icône d'une horloge près d'un ordinateur dans la colonne **A jour** de l'onglet **Etat**, les logiciels de sécurité sur cet ordinateur ne sont pas à jour. Le texte indique depuis combien de temps l'ordinateur n'est pas à jour.

Un ordinateur peut ne pas être à jour pour l'une des deux raisons suivantes :

- L'ordinateur ne parvient pas à récupérer une mise à jour depuis le serveur.

- Le serveur ne dispose pas du logiciel Sophos le plus récent.

Pour diagnostiquer le problème et mettre à jour les ordinateurs :

1. Dans la vue **Ordinateurs d'extrémité**, sélectionnez le groupe qui contient les ordinateurs non à jour.
2. Sur l'onglet **Etat**, cliquez sur la colonne **A jour** pour trier les ordinateurs par leur état de mise à jour.
3. Cliquez sur l'onglet **Détails de la mise à jour** et observez la colonne **Serveur principal**.

Le répertoire à partir duquel chaque ordinateur se met à jour apparaît.

4. A présent, observez les ordinateurs qui se mettent à jour à partir d'un répertoire particulier.
  - *Si certains ne sont pas à jour alors que d'autres le sont*, le problème provient des ordinateurs individuels. Sélectionnez-les, cliquez dessus avec le bouton droit de la souris, puis cliquez sur **Mettre les ordinateurs à jour maintenant**.
  - *Si tous ne sont pas à jour*, le problème peut provenir du répertoire. Dans le menu **Affichage**, cliquez sur **Gestionnaire de mise à jour**. Sélectionnez le gestionnaire de mise à jour qui gère le répertoire que vous croyez non à jour, cliquez dessus avec le bouton droit de la souris, puis cliquez sur **Mettre à jour maintenant**. Dans le menu **Affichage**, cliquez sur **Ordinateurs d'extrémité**. Sélectionnez les ordinateurs non à jour, cliquez avec le bouton droit de la souris, puis cliquez sur **Mettre les ordinateurs à jour maintenant**.

## 7 Configuration des stratégies

### 7.1 Configuration de la stratégie antivirus et HIPS

#### 7.1.1 À propos de la stratégie antivirus et HIPS

Une stratégie antivirus et HIPS vous permet de détecter et de nettoyer les virus, chevaux de Troie, vers, spywares ainsi que les adwares et autres applications potentiellement indésirables. Elle vous permet aussi d'effectuer le contrôle de vos ordinateurs à la recherche de tout comportement suspect, des fichiers suspects et des rootkits. Vous pouvez utiliser différents paramètres pour chaque groupe d'ordinateurs.

Par défaut, Sophos Endpoint Security and Control détecte automatiquement les virus, les chevaux de Troie, les vers et les spywares connus et inconnus présents dans les fichiers auxquels un utilisateur tente d'accéder. Il analyse également le comportement des programmes s'exécutant sur le système.

Vous pouvez également configurer Sophos Endpoint Security and Control pour effectuer les tâches suivantes :

- [Contrôle à la recherche des fichiers suspects](#) à la page 65
- [Recherche d'adwares et de PUA](#) à la page 68
- [Contrôle des ordinateurs à des heures définies](#) à la page 73

Vous pouvez également faire nettoyer les ordinateurs automatiquement dès la découverte d'un virus ou de toute autre menace. Pour cela, modifiez les paramètres du contrôle sur accès comme le décrit la section [Configuration du nettoyage automatique](#) à la page 45.

**Remarque :** si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - antivirus et HIPS** pour modifier une stratégie antivirus et HIPS. Pour plus d'informations sur l'administration déléguée, reportez-vous à la section [À propos des rôles](#) à la page 15.

**Remarque :** Enterprise Manager 4.7 ne peut pas effectuer de contrôles planifiés sur les Mac. Utilisez une autre option de contrôle ou reportez-vous à l'*Aide de Sophos Anti-Virus pour Mac OS X* pour plus d'options de contrôle.

#### 7.1.2 Contrôle à la recherche des virus, chevaux de Troie, vers et spywares

Par défaut, Sophos Endpoint Security and Control détecte automatiquement les virus, les chevaux de Troie, les vers et les spywares connus et inconnus présents dans les fichiers auxquels un utilisateur tente d'accéder.

## 7.1.3 Détection des comportements et des fichiers suspects (HIPS)

### 7.1.3.1 Qu'est-ce que HIPS ?

Le système de prévention des intrusions sur l'hôte (HIPS) est une technologie de sécurité protégeant les ordinateurs des fichiers suspects, des virus non identifiés et de tout comportement suspect. Il existe deux méthodes HIPS : détection des comportements suspects et détection des fichiers suspects.

**Remarque :** les options HIPS s'appliquent seulement à Sophos Endpoint Security and Control pour Windows 2000 et supérieur.

#### Détection des comportements suspects

La détection des comportements suspects est l'analyse dynamique de tous les programmes fonctionnant sur l'ordinateur pour détecter et bloquer toute activité qui semble malveillante. Un comportement suspect peut inclure des changements apportés au registre qui pourrait entraîner l'exécution automatique d'un virus lors du redémarrage de l'ordinateur.

La détection des comportements suspects inclut la détection de la mémoire tampon qui procède à une analyse dynamique du comportement de tous les programmes s'exécutant sur le système afin de détecter les attaques par saturation de la mémoire tampon.

**Remarque :** la fonction de "détection du dépassement de la mémoire tampon" n'est pas disponible pour Windows Vista, Windows 2008, Windows 7 et pour les versions 64 bits de Windows. Ces systèmes d'exploitation sont protégés contre les dépassements de la mémoire tampon par la fonctionnalité de prévention de l'exécution des données (DEP, Data Execution Prevention) de Microsoft.

Pour plus d'informations sur la configuration de la détection des comportements suspects, reportez-vous à la section [Détection et blocage de tout comportement suspect](#) à la page 64.

#### Détection des fichiers suspects

Sophos Endpoint Security and Control peut effectuer un contrôle à la recherche des fichiers suspects. Ceux-ci peuvent contenir certaines caractéristiques communes aux malwares mais pas suffisantes pour que les fichiers soient identifiés comme nouveaux éléments d'un malware.

Pour plus d'informations sur la configuration de la détection des fichiers suspects, reportez-vous à la section [Contrôle à la recherche des fichiers suspects](#) à la page 65.

### 7.1.3.2 Détection et blocage de tout comportement suspect

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - antivirus et HIPS** pour effectuer cette tâche. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Par défaut, Sophos Endpoint Security and Control analyse le comportement des programmes sur le système, mais ne bloque pas les programmes affichant un comportement suspect.

Nous vous conseillons d'exécuter Sophos Endpoint Security and Control en mode Alerter uniquement pour un certain temps et d'autoriser les programmes dont vous avez besoin avant d'activer le blocage automatique des comportements suspects. Lorsqu'un comportement suspect ou un dépassement de la mémoire tampon est détecté, vous pouvez soit supprimer, soit autoriser l'élément suspect. Reportez-vous aux sections [Nettoyage immédiat des ordinateurs](#)

à la page 43 et [Autorisation d'éléments suspects](#) à la page 66. Après avoir autorisé tous les programmes dont vous avez besoin, activez le blocage des comportements suspects.

1. Vérifiez quelle stratégie antivirus et HIPS est utilisée par le ou les groupes d'ordinateurs que vous voulez configurer.  
Reportez-vous à la section [Vérification des stratégies utilisées par un groupe](#) à la page 23.
2. Dans le volet **Stratégies**, cliquez deux fois sur **Antivirus et HIPS**. Puis cliquez deux fois sur la stratégie que vous désirez changer.
3. Dans la boîte de dialogue **Stratégie antivirus et HIPS**, cliquez sur le bouton **Comportement suspect**.

La boîte de dialogue **Détection des comportements suspects** apparaît. Par défaut, les trois options (**Détecter les comportements suspects**, **Détecter les dépassements de la mémoire tampon** et **Alerter uniquement**) sont activées.

4. Dessélectionnez la case à cocher **Alerter uniquement**.

### 7.1.3.3 Contrôle à la recherche des fichiers suspects

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - antivirus et HIPS** pour effectuer cette tâche. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Un *fichier suspect* est un fichier qui contient certaines caractéristiques communes aux malwares mais pas en nombre suffisant pour identifier le fichier comme un nouvel élément de malware (par exemple, un fichier contenant du code de décompression dynamique fréquemment utilisé par les malwares).

**Remarque :** cette option s'applique uniquement à Sophos Endpoint Security and Control pour Windows 2000 et supérieur.

1. Vérifiez quelle stratégie antivirus et HIPS est utilisée par le ou les groupes d'ordinateurs que vous voulez configurer.  
Reportez-vous à la section [Vérification des stratégies utilisées par un groupe](#) à la page 23.
2. Dans le volet **Stratégies**, cliquez deux fois sur **Antivirus et HIPS**. Puis cliquez deux fois sur la stratégie que vous désirez changer.
3. Dans la boîte de dialogue **Stratégie antivirus et HIPS**, définissez les options comme suit :

#### ■ Contrôle sur accès

Pour configurer le contrôle sur accès, dans le volet **Configurer l'antivirus et HIPS**, assurez-vous que la case à cocher **Activer le contrôle sur accès** est sélectionnée. Cliquez sur le bouton **Configurer** près de la case à cocher.

Sur l'onglet **Contrôle**, dans le volet **Options de contrôle**, sélectionnez la case à cocher **Rechercher les fichiers suspects**. Cliquez sur **OK**.

### ■ Contrôle planifié

Pour configurer les contrôles planifiés, dans le volet **Contrôle planifié**, cliquez sur **Ajouter** (ou sélectionnez un contrôle existant et cliquez sur **Modifier**).

Dans la boîte de dialogue **Paramètres du contrôle planifié**, saisissez vos paramètres puis cliquez sur **Configurer**.

Dans la boîte de dialogue **Paramètres de contrôle et de nettoyage**, sur l'onglet **Contrôle**, dans le volet **Options de contrôle**, sélectionnez la case à cocher **Rechercher les fichiers suspects**. Cliquez sur **OK**.

Lorsqu'un fichier suspect est détecté, vous pouvez soit supprimer, soit autoriser le fichier. Reportez-vous aux sections [Nettoyage immédiat des ordinateurs](#) à la page 43 et [Autorisation d'éléments suspects](#) à la page 66.

#### 7.1.3.4 Autorisation d'éléments suspects

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - antivirus et HIPS** pour effectuer cette tâche. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Si vous avez activé une ou plusieurs options HIPS (par exemple, la détection des comportements suspects, la détection des dépassements de la mémoire tampon ou la détection des fichiers suspects), mais voulez utiliser certains des éléments détectés, vous pouvez les autoriser de la manière suivante :

1. Vérifiez quelle stratégie antivirus et HIPS est utilisée par le ou les groupes d'ordinateurs que vous voulez configurer.  
Reportez-vous à la section [Vérification des stratégies utilisées par un groupe](#) à la page 23.
2. Dans le volet **Stratégies**, cliquez deux fois sur **Antivirus et HIPS**. Puis cliquez deux fois sur la stratégie que vous désirez changer.
3. Dans la boîte de dialogue **Stratégie antivirus et HIPS**, cliquez sur le bouton **Autorisation**.
4. Dans la boîte de dialogue **Gestionnaire d'autorisation**, cliquez sur l'onglet correspondant au type de comportement ayant été détecté, par exemple, "Dépassement de la mémoire tampon".
  - Pour autoriser un programme qui a été détecté, recherchez le programme dans la liste **Connus** et déplacez-le de cette liste **Connus** dans la liste **Autorisés**.
  - Pour autoriser un élément que Sophos Endpoint Security and Control n'a *pas* encore classé comme suspect, cliquez sur **Nouveau**. Naviguez jusqu'à l'élément et sélectionnez-le pour l'ajouter à la liste **Autorisés**.

Si vous voulez supprimer un élément de la liste, sélectionnez-le et cliquez sur **Supprimer**. Si vous avez autorisé l'élément, sa suppression de la liste le bloque effectivement une nouvelle fois, utilisez donc cette option seulement si vous êtes sûr qu'il ne doit pas être autorisé. Cette option ne supprime pas l'élément du disque.

## 7.1.4 Protection Live Sophos

### 7.1.4.1 À propos de la protection Live Sophos

La protection Live Sophos utilise la technologie dans-le-nuage pour décider instantanément si un fichier suspect est une menace et prendre les mesures spécifiées dans la stratégie antivirus et HIPS.

La protection Live améliore la détection des nouveaux malwares sans aucun risque de détection indésirable. L'opération consiste à effectuer une recherche instantanée comparant les identités des fichiers malveillants connus les plus récents. Lorsque de nouveaux malwares sont identifiés, Sophos envoie des mises à jour en quelques secondes.

Pour bénéficier au maximum de la protection Live, assurez-vous que les options suivantes sont activées.

#### ■ Activer la protection Live

Si un contrôle antivirus sur un ordinateur d'extrémité a identifié un fichier comme suspect, mais ne peut pas l'identifier davantage comme sain ou malveillant d'après les fichiers d'identités des menaces (IDE) stockés sur l'ordinateur, certaines caractéristiques de ce fichier comme sa somme de contrôle sont envoyées à Sophos pour une analyse approfondie. La vérification dans-le-nuage (in-the-cloud) recherche instantanément un fichier suspect dans la base de données des SophosLabs. Si le fichier est identifié comme sain ou malveillant, la décision est renvoyée à l'ordinateur et l'état du fichier est automatiquement mis à jour.

#### ■ Envoyer automatiquement des fichiers échantillons à Sophos

Si un fichier est jugé potentiellement malveillant mais ne peut pas être identifié avec certitude comme malveillant d'après ses seules caractéristiques, la protection Live permet à Sophos de demander un échantillon du fichier. Si cette option est activée et si Sophos n'a pas déjà d'échantillon de ce fichier, ce dernier est soumis automatiquement.

La soumission de ces échantillons de fichiers aide Sophos à améliorer en permanence la détection des malwares sans aucun risque de faux positifs.

**Remarque :** la taille maximum de l'échantillon est 10 Mo. Le délai d'attente pour le chargement de l'échantillon est de 30 secondes. Il n'est pas recommandé d'envoyer automatiquement des échantillons par le biais d'une connexion lente (moins de 56 Kbps).

**Important :** vous devez vous assurer que le domaine Sophos auquel les données des fichiers sont envoyées est fiable dans votre solution de filtrage web. Pour plus de détails, consultez l'article 62637 de la base de connaissances du support (<http://www.sophos.fr/support/knowledgebase/article/62637.html>).

Si vous utilisez une solution Sophos de filtrage web, par exemple l'apppliance web WS1000, aucune opération de votre part n'est nécessaire car les domaines Sophos sont déjà fiables.

### 7.1.4.2 Activation ou désactivation de la protection Live Sophos

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - antivirus et HIPS** pour effectuer cette tâche. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Par défaut, Endpoint Security and Control envoie des données de fichiers telles que les sommes de contrôle à Sophos, mais n'envoie pas d'échantillons de fichiers. Pour bénéficier au maximum de la protection Live Sophos, activez les deux options de la protection Live Sophos.

Pour activer ou désactiver les options de la protection Live Sophos :

1. Vérifiez quelle stratégie antivirus et HIPS est utilisée par le ou les groupes d'ordinateurs que vous voulez configurer.  
Reportez-vous à la section [Vérification des stratégies utilisées par un groupe](#) à la page 23.
2. Dans le volet **Stratégies**, cliquez deux fois sur **Antivirus et HIPS**. Puis cliquez deux fois sur la stratégie que vous désirez changer.
3. Dans la boîte de dialogue **Stratégie antivirus et HIPS**, cliquez sur le bouton **Protection Live Sophos**.
4. Dans la boîte de dialogue **Protection Live Sophos** :
  - Pour activer ou désactiver l'envoi de données de fichiers à Sophos, sélectionnez ou désélectionnez la case à cocher **Activer la protection Live**.
  - Pour activer ou désactiver l'envoi d'échantillons de fichiers à Sophos, sélectionnez ou désélectionnez la case à cocher **Envoyer automatiquement les échantillons de fichiers à Sophos**.

**Remarque :** lorsqu'un échantillon de fichier est envoyé à Sophos en vue d'un contrôle en ligne, les données de fichiers sont toujours envoyées avec l'échantillon.

## 7.1.5 Adwares et PUA

### 7.1.5.1 Recherche d'adwares et de PUA

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - antivirus et HIPS** pour effectuer cette tâche. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

**Remarque :** cette option s'applique uniquement à Sophos Endpoint Security and Control pour Windows 2000 et supérieur.

Nous vous recommandons de commencer par utiliser un contrôle planifié pour détecter les applications potentiellement indésirables. Vous pouvez ainsi gérer en toute sécurité les applications qui sont *déjà* en cours d'exécution sur votre réseau. Vous pouvez ensuite activer la détection sur accès pour protéger vos ordinateurs à l'avenir.

1. Vérifiez quelle stratégie antivirus et HIPS est utilisée par le ou les groupes d'ordinateurs que vous voulez configurer.  
Reportez-vous à la section [Vérification des stratégies utilisées par un groupe](#) à la page 23.
2. Dans le volet **Stratégies**, cliquez deux fois sur **Antivirus et HIPS**. Puis cliquez deux fois sur la stratégie que vous désirez changer.  
La boîte de dialogue **Stratégie antivirus et HIPS** apparaît.
3. Dans le volet **Contrôle planifié**, cliquez sur **Ajouter** pour créer un nouveau contrôle ou cliquez deux fois sur un contrôle dans la liste pour le modifier.

4. Dans la boîte de dialogue **Paramètres du contrôle planifié**, cliquez sur **Configurer** (en bas de la page).
5. Dans la boîte de dialogue **Paramètres de contrôle et de nettoyage**, sur l'onglet **Contrôle**, sous **Options de contrôle**, sélectionnez **Rechercher les adwares et les PUA**. Cliquez sur **OK**.

Lorsque le contrôle s'exécute, il se peut que Sophos Endpoint Security and Control signale certains adwares ou autres applications potentiellement indésirables.

6. Si vous souhaitez que vos ordinateurs exécutent ces applications, vous devez les autoriser (reportez-vous à la section [Autorisation des adwares et des PUA](#) à la page 69). Sinon, supprimez-les (reportez-vous à la section [Nettoyage immédiat des ordinateurs](#) à la page 43).
7. Si vous désirez activer la détection sur accès, ouvrez de nouveau la boîte de dialogue **Stratégie antivirus et HIPS**. Dans le volet **Configurer l'antivirus et HIPS**, assurez-vous que la case à cocher **Activer le contrôle sur accès** est sélectionnée. Cliquez sur le bouton **Configurer** près de la case à cocher. Dans la boîte de dialogue **Paramètres de contrôle sur accès**, sélectionnez **Rechercher les adwares et les PUA**.

**Remarque :** certaines applications "surveillent" les fichiers et tentent d'y accéder régulièrement. Si le contrôle sur accès est activé, il détecte chaque accès et envoie plusieurs alertes. Reportez-vous à la section [Fréquentes alertes concernant les applications potentiellement indésirables](#) à la page 149.

### 7.1.5.2 Autorisation des adwares et des PUA

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - antivirus et HIPS** pour effectuer cette tâche. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Si vous avez activé Sophos Endpoint Security and Control pour détecter les adwares et autres applications potentiellement indésirables (PUA), il peut vous empêcher d'utiliser une application que vous souhaitez utiliser.

Pour autoriser ces applications :

1. Vérifiez quelle stratégie antivirus et HIPS est utilisée par le ou les groupes d'ordinateurs que vous voulez configurer.  
Reportez-vous à la section [Vérification des stratégies utilisées par un groupe](#) à la page 23.
2. Dans le volet **Stratégies**, cliquez deux fois sur **Antivirus et HIPS**. Puis cliquez deux fois sur la stratégie que vous désirez changer.
3. Dans la boîte de dialogue **Stratégie antivirus et HIPS**, cliquez sur le bouton **Autorisation**.
4. Dans la boîte de dialogue **Gestionnaire d'autorisation**, sur l'onglet **Adwares et PUA**, dans la liste des **Adwares et PUA connus**, sélectionnez l'application de votre choix. Cliquez sur **Ajouter** pour l'ajouter à la liste des **Adwares et PUA autorisés**.
5. Si vous ne voyez pas l'application que vous voulez autoriser, cliquez sur **Nouvelle entrée**.

La boîte de dialogue **Ajout d'un nouvel adware ou PUA** apparaît.

6. Allez sur la page web Sophos des analyses de sécurité, <http://www.sophos.fr/security/analyses/>. Sur l'onglet **Adwares et PUA**, recherchez l'application que vous voulez autoriser.
  7. Dans Enterprise Manager, dans la boîte de dialogue **Ajout d'un nouvel adware ou PUA**, saisissez le nom de l'application que vous voulez autoriser et cliquez sur **OK**.  
L'application est ajoutée à la liste des **Adwares et PUA connus**.
  8. Sélectionnez l'application et cliquez sur **Ajouter** pour l'ajouter à la liste des **Adwares et PUA autorisés**.
- Si vous voulez supprimer une application de la liste, sélectionnez-la et cliquez sur **Supprimer**.

## 7.1.6 Protection Web

### 7.1.6.1 À propos de la protection Web

La protection Web assure une protection étendue contre les menaces du web en empêchant l'accès aux emplacements connus pour héberger des malwares. Il bloque l'accès à ces sites par les ordinateurs d'extrémité en effectuant une recherche en temps réel dans la base de données en ligne Sophos répertoriant les sites Web malveillants.

Protection Web :

- Bloque l'accès réseau vers les sites Web malveillants.
- Contrôle les données et les fichiers téléchargés avec Internet Explorer.

Pour plus d'informations sur l'activation du contrôle du Web, reportez-vous à la section [Activation de la protection Web](#) à la page 70.

### 7.1.6.2 Activation de la protection Web

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - antivirus et HIPS** pour effectuer cette tâche. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Pour activer la protection Web :

1. Vérifiez quelle stratégie antivirus et HIPS est utilisée par le ou les groupes d'ordinateurs que vous voulez configurer.  
Reportez-vous à la section [Vérification des stratégies utilisées par un groupe](#) à la page 23.
2. Dans le volet **Stratégies**, cliquez deux fois sur **Antivirus et HIPS**. Puis cliquez deux fois sur la stratégie que vous désirez changer.
3. Dans la boîte de dialogue de la stratégie **Antivirus et HIPS**, à côté du champ **Bloquer l'accès aux sites Web malveillants**, sélectionnez **Activé**. Cette option est activée par défaut.

Pour plus d'informations sur l'autorisation de sites Web spécifiques, reportez-vous à la section [Autorisation de sites Web](#) à la page 71.

4. Pour contrôler des données et des fichiers téléchargés via Internet Explorer, à côté de **Contrôle des téléchargements**, sélectionnez **Activé**.

Vous pouvez aussi sélectionner **Identique à celui sur accès**, si vous voulez désactiver et activer les contrôles sur accès et de téléchargement simultanément.

### 7.1.6.3 Autorisation de sites Web

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - antivirus et HIPS** pour effectuer cette tâche. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.



**Avertissement :** l'autorisation d'un site Web classé comme malveillant peut vous exposer à des menaces, veillez à ce que l'accès du site Web soit sûr avant de l'autoriser.

Si vous voulez débloquer un site Web que Sophos a classé comme malveillant, vous pouvez l'ajouter dans la liste des sites autorisés. L'autorisation d'un site Web empêche la vérification des URL de ce site par le service de filtrage web en ligne Sophos.

**Remarque :** si le contrôle des téléchargements est activé pendant que vous utilisez Internet Explorer pour vous rendre sur un site Web contenant une menace, l'accès à ce site sera bloqué même s'il est répertorié en tant que site Web autorisé.

Pour autoriser un site Web :

1. Vérifiez quelle stratégie antivirus et HIPS est utilisée par le ou les groupes d'ordinateurs que vous voulez configurer.  
Reportez-vous à la section [Vérification des stratégies utilisées par un groupe](#) à la page 23.
2. Dans le volet **Stratégies**, cliquez deux fois sur **Antivirus et HIPS**. Puis cliquez deux fois sur la stratégie que vous désirez changer.
3. Dans la boîte de dialogue **Stratégie antivirus et HIPS**, cliquez sur le bouton **Autorisation**.
4. Dans la boîte de dialogue **Gestionnaire d'autorisation**, sur l'onglet **Sites Web**, cliquez sur **Ajouter** pour ajouter un site Web à l'aide d'une des options disponibles.

Vous pouvez ajouter un site Web en entrant son nom de domaine, son adresse IP ou son adresse IP accompagnée du masque de sous-réseau.

Si vous voulez modifier ou supprimer un site Web de la liste, sélectionnez ce site Web et cliquez soit sur **Modifier**, soit sur **Supprimer**.

Pour voir une liste des sites Web bloqués récemment sur un ordinateur d'extrémité, reportez-vous à la section [Affichage des sites Web bloqués](#) à la page 129.

## 7.1.7 Contrôle sur accès

### 7.1.7.1 Modification de la fréquence du contrôle sur accès

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - antivirus et HIPS** pour effectuer cette tâche. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Vous pouvez spécifier si les fichiers doivent être contrôlés lorsque vous les ouvrez (“à la lecture”), les sauvegardez (“à l'écriture”) ou les renommez.

**Remarque :**

Le contrôle des fichiers “à l'écriture” ou “au moment de renommer” peut avoir un impact sur les performances des ordinateurs. L'utilisation de ces options n'est généralement pas recommandée.

Ces options s'appliquent aux ordinateurs Windows seulement.

1. Vérifiez quelle stratégie antivirus et HIPS est utilisée par le ou les groupes d'ordinateurs que vous voulez configurer.  
Reportez-vous à la section [Vérification des stratégies utilisées par un groupe](#) à la page 23.
2. Dans le volet **Stratégies**, cliquez deux fois sur **Antivirus et HIPS**. Puis cliquez deux fois sur la stratégie que vous désirez changer.
3. Dans la boîte de dialogue **Stratégie antivirus et HIPS**, dans le volet **Contrôle sur accès**, cliquez sur le bouton **Configurer**.
4. Dans la boîte de dialogue **Paramètres de contrôle sur accès**, dans l'onglet **Contrôle**, sous **Vérifier les fichiers**, sélectionnez les options que vous désirez.

#### 7.1.7.2 Exclusion des éléments du contrôle sur accès

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - antivirus et HIPS** pour effectuer cette tâche. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Vous pouvez exclure des éléments du contrôle sur accès.

1. Vérifiez quelle stratégie antivirus et HIPS est utilisée par le ou les groupes d'ordinateurs que vous voulez configurer.  
Reportez-vous à la section [Vérification des stratégies utilisées par un groupe](#) à la page 23.
2. Dans le volet **Stratégies**, cliquez deux fois sur **Antivirus et HIPS**. Puis cliquez deux fois sur la stratégie que vous désirez changer.  
La boîte de dialogue **Stratégie antivirus et HIPS** apparaît.
3. Dans le volet **Contrôle sur accès**, cliquez sur le bouton **Configurer**.
4. Cliquez sur l'onglet **Exclusions Windows**, **Exclusions Mac** ou **Exclusions Linux**. Pour ajouter des éléments dans la liste, cliquez sur **Ajouter** et saisissez le chemin complet dans la boîte de dialogue **Exclusion d'un élément**.  
Les éléments que vous pouvez exclure du contrôle diffèrent selon chaque type d'ordinateur. Reportez-vous à la section [Éléments pouvant être exclus du contrôle](#) à la page 79.

#### 7.1.7.3 Activation ou désactivation du contrôle sur accès

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - antivirus et HIPS** pour effectuer cette tâche. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Par défaut, Sophos Endpoint Security and Control contrôle les fichiers au moment où l'utilisateur tente d'y accéder et refuse leur accès à moins que ces fichiers soient sains.

Vous avez la possibilité de désactiver le contrôle sur accès sur les serveurs Exchange ou sur d'autres serveurs dont les performances pourraient être affectées. Dans ce cas, placez les serveurs

dans un groupe spécial et changez la stratégie antivirus et HIPS de ce groupe comme indiqué ci-dessous.

**Important :** si vous désactivez le contrôle sur accès sur un serveur, nous vous recommandons de paramétrer les contrôles planifiés sur les ordinateurs appropriés.

1. Vérifiez quelle stratégie antivirus et HIPS est utilisée par le ou les groupes d'ordinateurs que vous voulez configurer.  
Reportez-vous à la section [Vérification des stratégies utilisées par un groupe](#) à la page 23.
2. Dans le volet **Stratégies**, cliquez deux fois sur **Antivirus et HIPS**. Puis cliquez deux fois sur la stratégie que vous désirez changer.  
La boîte de dialogue **Stratégie antivirus et HIPS** apparaît.
3. Pour désactiver le contrôle sur accès, désélectionnez la case à cocher **Activer le contrôle sur accès**. Ensuite, dans le panneau **Contrôle planifié**, cliquez sur **Ajouter** et paramétrez un contrôle planifié.

Si, ultérieurement, vous désirez redémarrer le contrôle sur accès, sélectionnez de nouveau la case à cocher **Activer le contrôle sur accès**.

## 7.1.8 Contrôle planifié

### 7.1.8.1 Contrôle des ordinateurs à des heures définies

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - antivirus et HIPS** pour effectuer cette tâche. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Vous pouvez faire en sorte que vos ordinateurs soient contrôlés à des heures définies.

**Remarque :** les contrôles planifiés s'exécutent uniquement sur les ordinateurs Windows et Linux.

1. Vérifiez quelle stratégie antivirus et HIPS est utilisée par le ou les groupes d'ordinateurs que vous voulez configurer.  
Reportez-vous à la section [Vérification des stratégies utilisées par un groupe](#) à la page 23.
2. Dans le volet **Stratégies**, cliquez deux fois sur **Antivirus et HIPS**. Puis cliquez deux fois sur la stratégie que vous désirez changer.
3. Dans la boîte de dialogue **Stratégie antivirus et HIPS** puis dans la zone **Contrôle planifié**, cliquez sur **Ajouter**.
4. Dans la boîte de dialogue **Paramètres du contrôle planifié**, saisissez un nom de tâche de contrôle. Sélectionnez les éléments à contrôler (par défaut, tous les disques durs locaux ou les systèmes de fichiers montés sont contrôlés). Sélectionnez les jours et heures auxquels vous souhaitez procéder au contrôle.
5. Si vous souhaitez modifier d'autres options de contrôle ou configurer ce contrôle pour effectuer un nettoyage des ordinateurs, cliquez sur **Configurer** en bas de la boîte de dialogue.  
Pour de plus amples instructions sur le changement des options d'un contrôle planifié, reportez-vous à la section [Modification des paramètres du contrôle planifié](#) à la page 74.

**Remarque :** si le contrôle détecte les composants d'une menace dans la mémoire alors que vous n'avez pas paramétré ce contrôle pour qu'il effectue le nettoyage automatique, le contrôle s'arrête et une alerte est envoyée à Enterprise Manager. En effet, la poursuite du contrôle pourrait permettre à la menace de se propager. Nettoyez l'ordinateur de la menace avant d'exécuter de nouveau le contrôle.

### 7.1.8.2 Modification des paramètres du contrôle planifié

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - antivirus et HIPS** pour effectuer cette tâche. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Vous pouvez changer les paramètres du contrôle planifié :

1. Vérifiez quelle stratégie antivirus et HIPS est utilisée par le ou les groupes d'ordinateurs que vous voulez configurer.  
Reportez-vous à la section [Vérification des stratégies utilisées par un groupe](#) à la page 23.
2. Dans le volet **Stratégies**, cliquez deux fois sur **Antivirus et HIPS**. Puis cliquez deux fois sur la stratégie que vous désirez changer.
3. Dans la boîte de dialogue **Stratégie antivirus et HIPS** puis dans la zone **Contrôle planifié**, modifiez les paramètres selon le cas.

Vous pouvez modifier deux différentes sortes de paramètres :

- Pour modifier les types de fichiers contrôlés par *tous* les contrôles planifiés, cliquez sur **Extensions et Exclusions**.
- Pour modifier les paramètres spécifiques à chaque contrôle (ce qui est contrôlé, les heures, les options de contrôle, le nettoyage), mettez le contrôle en surbrillance et cliquez sur **Modifier**. Puis dans la boîte de dialogue **Paramètres du contrôle planifié**, cliquez sur **Configurer**.

**Remarque :** pour plus de détails sur l'utilisation des options de contrôle, reportez-vous aux sections [Contrôle à la recherche des fichiers suspects](#) à la page 65, [Recherche d'adwares et de PUA](#) à la page 68 et [Contrôle dans les fichiers archive](#) à la page 77. Pour plus de détails sur l'utilisation des options de nettoyage, reportez-vous à la section [Configuration du nettoyage automatique](#) à la page 45.

### 7.1.8.3 Exclusion d'éléments du contrôle planifié

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - antivirus et HIPS** pour effectuer cette tâche. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Vous pouvez exclure des éléments du contrôle planifié.

**Remarque :**

Les paramètres des "éléments exclus" des contrôles planifiés s'appliquent aussi aux contrôles intégraux du système exécutés depuis la console et à ceux "effectuer le contrôle de cet ordinateur" exécutés sur les ordinateurs en réseau. Reportez-vous à la section [Contrôle immédiat des ordinateurs](#) à la page 43.

Les contrôles planifiés ne sont pas pris en charge sur les ordinateurs Mac.

1. Vérifiez quelle stratégie antivirus et HIPS est utilisée par le ou les groupes d'ordinateurs que vous voulez configurer.  
Reportez-vous à la section [Vérification des stratégies utilisées par un groupe](#) à la page 23.
2. Dans le volet **Stratégies**, cliquez deux fois sur **Antivirus et HIPS**. Puis cliquez deux fois sur la stratégie que vous désirez changer.
3. La boîte de dialogue **Stratégie antivirus et HIPS** apparaît. Dans la zone **Contrôle planifié**, cliquez sur **Extensions et Exclusions**.
4. Cliquez sur l'onglet **Exclusions Windows** ou **Exclusions Linux**. Pour ajouter des éléments dans la liste, cliquez sur **Ajouter** et saisissez le chemin complet dans la boîte de dialogue **Exclusion d'un élément**.  
Les éléments que vous pouvez exclure du contrôle diffèrent selon chaque type d'ordinateur. Reportez-vous à la section [Éléments pouvant être exclus du contrôle](#) à la page 79.

## 7.1.9 Options de contrôle

### 7.1.9.1 Modification des types de fichiers contrôlés

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - antivirus et HIPS** pour effectuer cette tâche. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Par défaut, Sophos Endpoint Security and Control contrôle les types de fichiers vulnérables aux virus. Vous pouvez contrôler des types de fichiers supplémentaires ou choisir d'exempter du contrôle certains types de fichiers.

Les types de fichiers contrôlés par défaut diffèrent d'un système d'exploitation à l'autre et changent au fur et à mesure de la mise à jour du produit. Pour consulter une liste des types de fichiers, rendez-vous sur un ordinateur possédant le système d'exploitation approprié, ouvrez la fenêtre Sophos Endpoint Security and Control ou Sophos Anti-Virus et recherchez la page de configuration "Extensions".

#### **Remarque :**

Ces options s'appliquent aux ordinateurs Windows seulement.

Sous Windows 2000 ou supérieur, vous pouvez changer ces paramètres individuellement pour le contrôle sur accès et le contrôle planifié.

Vous pouvez apporter des modifications aux ordinateurs Mac OS X grâce au Sophos Update Manager, un utilitaire fourni avec Sophos Anti-Virus pour Mac OS X. Pour ouvrir Sophos Update Manager, sur un ordinateur Mac OS X, dans la fenêtre **Finder**, naviguez jusqu'au dossier Sophos Anti-Virus:ESOSX. Cliquez deux fois sur **Sophos Update Manager**. Pour de plus amples détails, reportez-vous à l'aide du Sophos Update Manager.

Vous pouvez effectuer des changements sur les ordinateurs Linux à l'aide des commandes savconfig et savscan comme le décrit le manuel utilisateur de Sophos Anti-Virus pour Linux.

Pour modifier les types de fichiers contrôlés :

1. Vérifiez quelle stratégie antivirus et HIPS est utilisée par le ou les groupes d'ordinateurs que vous voulez configurer.  
Reportez-vous à la section [Vérification des stratégies utilisées par un groupe](#) à la page 23.
2. Dans le volet **Stratégies**, cliquez deux fois sur **Antivirus et HIPS**. Puis cliquez deux fois sur la stratégie que vous désirez changer.
3. Dans la boîte de dialogue **Stratégie antivirus et HIPS**, définissez les options comme suit :
  - Pour configurer le contrôle sur accès, dans le volet **Configurer l'antivirus et HIPS**, assurez-vous que la case à cocher **Activer le contrôle sur accès** est sélectionnée. Cliquez sur le bouton **Configurer** près de la case à cocher.
  - Pour configurer les contrôles planifiés, dans le panneau **Contrôle planifié**, cliquez sur **Extensions et Exclusions**.
4. Sur l'onglet **Extensions**, sélectionnez **Contrôler les fichiers exécutables et infectables**.
  - Pour contrôler des types de fichiers supplémentaires, cliquez sur **Ajouter** puis saisissez l'extension du fichier, par exemple PDF, dans le champ **Extension**.
  - Pour exempter certains types de fichiers qui sont d'habitude contrôlés par défaut, cliquez sur **Exclure**. La boîte de dialogue **Exclusion d'extensions** s'ouvre. Saisissez l'extension du fichier.

Par défaut, les fichiers sans extension sont contrôlés.

**Remarque :** vous pouvez aussi choisir de contrôler tous les fichiers, toutefois, ceci affectera les performances de l'ordinateur.

### 7.1.9.2 Contrôle des fichiers Macintosh

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - antivirus et HIPS** pour effectuer cette tâche. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Vous pouvez permettre à Sophos Endpoint Security and Control de contrôler les fichiers Macintosh stockés sur les ordinateurs Windows.

**Remarque :** cette option s'applique uniquement à Sophos Endpoint Security and Control pour Windows 2000 et supérieur.

1. Vérifiez quelle stratégie antivirus et HIPS est utilisée par le ou les groupes d'ordinateurs que vous voulez configurer.  
Reportez-vous à la section [Vérification des stratégies utilisées par un groupe](#) à la page 23.
2. Dans le volet **Stratégies**, cliquez deux fois sur **Antivirus et HIPS**. Puis cliquez deux fois sur la stratégie que vous désirez changer.

3. Dans la boîte de dialogue **Stratégie antivirus et HIPS**, définissez les options comme suit :

■ **Contrôle sur accès**

Pour configurer le contrôle sur accès, dans le volet **Contrôle sur accès**, assurez-vous que la case à cocher **Activer le contrôle sur accès** est sélectionnée. Cliquez sur le bouton **Configurer** près de la case à cocher.

Dans l'onglet **Contrôle**, sous **Rechercher les**, sélectionnez la case **Virus Macintosh**.

■ **Contrôle planifié**

Pour configurer les contrôles planifiés, dans le volet **Contrôle planifié**, cliquez sur **Ajouter** (ou sélectionnez un contrôle existant et cliquez sur **Modifier**).

Dans la boîte de dialogue **Paramètres du contrôle planifié**, saisissez vos paramètres puis cliquez sur **Configurer**.

Dans la boîte de dialogue **Paramètres de contrôle et de nettoyage**, sur l'onglet **Contrôle**, sous **Rechercher les**, sélectionnez la case **Virus Macintosh**.

### 7.1.9.3 Contrôle à la recherche des rootkits

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - antivirus et HIPS** pour effectuer cette tâche. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Le contrôle à la recherche des rootkits s'effectue toujours lorsque vous exécutez un contrôle intégral du système d'un ordinateur (reportez-vous à la section [Contrôle immédiat des ordinateurs](#) à la page 43). En revanche, si vous voulez changer le paramètre d'un contrôle planifié, procédez ainsi.

**Remarque :** cette option s'applique uniquement à Sophos Endpoint Security and Control pour Windows 2000 et supérieur.

1. Vérifiez quelle stratégie antivirus et HIPS est utilisée par le ou les groupes d'ordinateurs que vous voulez configurer. Reportez-vous à la section [Vérification des stratégies utilisées par un groupe](#) à la page 23.
2. Dans le volet **Stratégies**, cliquez deux fois sur **Antivirus et HIPS**. Puis cliquez deux fois sur la stratégie que vous désirez changer.
3. Dans la boîte de dialogue **Stratégie antivirus et HIPS** dans le volet **Contrôle planifié**, cliquez sur **Ajouter** (ou sélectionnez un contrôle déjà existant et cliquez sur **Modifier**).
4. Dans la boîte de dialogue **Paramètres du contrôle planifié**, saisissez vos paramètres puis cliquez sur **Configurer**.
5. Dans la boîte de dialogue **Paramètres de contrôle et de nettoyage**, sur l'onglet **Contrôle**, sous **Rechercher les**, sélectionnez la case **Rootkits**. Cliquez sur **OK**.

### 7.1.9.4 Contrôle dans les fichiers archive

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - antivirus et HIPS** pour effectuer cette tâche. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

**Remarque :** le contrôle à l'intérieur de fichiers archive est beaucoup plus lent et généralement inutile. Même si vous ne sélectionnez pas l'option, lorsque vous tentez d'accéder à un fichier

extrait depuis le fichier archive, le fichier extrait est contrôlé. Sophos ne vous recommande donc pas de sélectionner cette option.

1. Vérifiez quelle stratégie antivirus et HIPS est utilisée par le ou les groupes d'ordinateurs que vous voulez configurer.  
Reportez-vous à la section [Vérification des stratégies utilisées par un groupe](#) à la page 23.
2. Dans le volet **Stratégies**, cliquez deux fois sur **Antivirus et HIPS**. Puis cliquez deux fois sur la stratégie que vous désirez changer.
3. Dans la boîte de dialogue **Stratégie antivirus et HIPS** dans le volet **Contrôle planifié**, cliquez sur **Ajouter** (ou sélectionnez un contrôle déjà existant et cliquez sur **Modifier**).
4. Dans la boîte de dialogue **Paramètres du contrôle planifié**, saisissez vos paramètres puis cliquez sur **Configurer** (en bas de la page).
5. Dans la boîte de dialogue **Paramètres de contrôle et de nettoyage**, sur l'onglet **Contrôle**, sous *Autres options de contrôle*, sélectionnez **Contrôler dans les fichiers archive**. Cliquez sur **OK**.

#### 7.1.9.5 Contrôle de la mémoire système

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - antivirus et HIPS** pour effectuer cette tâche. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Vous pouvez permettre à Endpoint Security and Control pour Windows de contrôler la mémoire système à la recherche de menaces. La *mémoire système* est utilisée par le système d'exploitation. Endpoint Security and Control peut contrôler périodiquement en tâche de fond la mémoire système si le contrôle sur accès est activé et dans le cadre d'un contrôle personnalisé.

Pour contrôler la mémoire système :

1. Vérifiez quelle stratégie antivirus et HIPS est utilisée par le ou les groupes d'ordinateurs que vous voulez configurer.  
Reportez-vous à la section [Vérification des stratégies utilisées par un groupe](#) à la page 23.
2. Dans le volet **Stratégies**, cliquez deux fois sur **Antivirus et HIPS**. Puis cliquez deux fois sur la stratégie que vous désirez changer.
3. Dans la boîte de dialogue **Stratégie antivirus et HIPS**, définissez les options comme suit :

##### ■ Contrôle sur accès

Pour configurer le contrôle sur accès, dans le volet **Contrôle sur accès**, assurez-vous que la case à cocher **Activer le contrôle sur accès** est sélectionnée. Cliquez sur le bouton **Configurer** près de la case à cocher.

Dans le volet **Autres options de contrôle** de l'onglet **Contrôle**, sélectionnez la case **Contrôle de la mémoire système**.

### ■ Contrôle planifié

Pour configurer les contrôles planifiés, dans le volet **Contrôle planifié**, cliquez sur **Ajouter** (ou sélectionnez un contrôle existant et cliquez sur **Modifier**).

Dans la boîte de dialogue **Paramètres du contrôle planifié**, saisissez vos paramètres puis cliquez sur **Configurer**.

Dans la boîte de dialogue **Paramètres de contrôle et de nettoyage**, sur l'onglet **Contrôle**, dans le volet **Autres options de contrôle**, sélectionnez la case à cocher **Contrôler la mémoire système**.

**Remarque :** si vous avez paramétré le nettoyage automatique des virus qui sont détectés par le contrôle sur accès, le nettoyage de certains de ces virus nécessite l'exécution d'un contrôle intégral du système qui essaye de nettoyer *tous* les virus présents sur votre ordinateur. Cette opération peut prendre du temps.

#### 7.1.9.6 Exécution d'un contrôle avec une priorité inférieure

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - antivirus et HIPS** pour effectuer cette tâche. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Vous pouvez configurer un contrôle personnalisé pour qu'il s'exécute avec une priorité inférieure afin qu'il ait un impact minimal sur les applications de l'utilisateur.

**Remarque :** cette option s'applique uniquement à Sophos Endpoint Security and Control pour Windows Vista et supérieur.

1. Vérifiez quelle stratégie antivirus et HIPS est utilisée par le ou les groupes d'ordinateurs que vous voulez configurer. Reportez-vous à la section [Vérification des stratégies utilisées par un groupe](#) à la page 23.
2. Dans le volet **Stratégies**, cliquez deux fois sur **Antivirus et HIPS**. Puis cliquez deux fois sur la stratégie que vous désirez changer.
3. Dans la boîte de dialogue **Stratégie antivirus et HIPS** dans le volet **Contrôle planifié**, cliquez sur **Ajouter** (ou sélectionnez un contrôle déjà existant et cliquez sur **Modifier**).
4. Dans la boîte de dialogue **Paramètres du contrôle planifié**, saisissez vos paramètres puis cliquez sur **Configurer**.
5. Dans la boîte de dialogue **Paramètres de contrôle et de nettoyage**, sur l'onglet **Contrôle**, sous *Autres options de contrôle*, sélectionnez la case à cocher **Exécuter le contrôle avec une priorité inférieure**. Cliquez sur **OK**.

#### 7.1.9.7 Éléments pouvant être exclus du contrôle

Sur chaque type d'ordinateur, il existe des limitations différentes concernant les éléments pouvant être exclus du contrôle.

##### Windows 2000 et supérieur

Sous Windows 2000 et supérieur, vous pouvez exclure des lecteurs, des dossiers et des fichiers.

Vous pouvez utiliser les caractères joker \* et ?

Le caractère joker ? peut seulement être utilisé dans un nom de fichier ou dans une extension. Il permet généralement de retrouver n'importe quel caractère. En revanche, lorsqu'il est utilisé

à la fin d'un nom de fichier ou d'une extension, il ne retrouve que les caractères uniques ou n'en retrouve pas. Par exemple, fichier?.txt permet de retrouver fichier.txt, fichier1.txt et fichier12.txt, mais pas fichier123.txt.

Le caractère joker \* peut seulement être utilisé dans un nom de fichier ou dans une extension, sous la forme [nomfichier].\* ou \*.\*[extension]. Par exemple, fichier\*.txt, fichier.txt\* et fichier.\*txt sont incorrects.

Pour plus de détails, reportez-vous à la section “Utilisation de Sophos Anti-Virus” dans l'aide des logiciels pour postes d'extrémité, Sophos Endpoint Security and Control version 9,7.

## Mac OS X

Sous Mac OS X, vous pouvez exclure des volumes, des dossiers et des fichiers.

Bien que les caractères joker ne soient pas pris en charge, vous pouvez spécifier quels éléments sont exclus en préfixant ou en suffixant l'exclusion par une barre oblique ou une double barre oblique.

Pour plus de détails, reportez-vous aux fichiers d'aide ou au manuel utilisateur de Sophos Anti-Virus pour Mac OS X.

## Linux

Sur Linux, vous pouvez exclure des répertoires et des fichiers en spécifiant un chemin (avec ou sans caractère joker).

**Remarque :** Enterprise Manager prend uniquement en charge les exclusions Linux basées sur des chemins. Vous pouvez aussi configurer d'autres types d'exclusions directement sur des ordinateurs administrés. Ensuite, vous pouvez utiliser des expressions régulières et exclure des types de fichiers et des systèmes de fichiers. Pour obtenir d'autres instructions, reportez-vous au *Manuel utilisateur de Sophos Anti-Virus pour Linux*.

Si vous configurez une autre exclusion basée sur un chemin sur un ordinateur Linux administré, cet ordinateur sera signalé à la console comme différent de la stratégie de groupe.

## 7.2 Configuration de la stratégie de pare-feu

### 7.2.1 Configuration de base du pare-feu

#### 7.2.1.1 Configuration d'une stratégie de pare-feu

Par défaut, le pare-feu est activé et bloque tout le trafic non indispensable. Par conséquent, vous devez le configurer pour qu'il autorise les applications que vous souhaitez utiliser puis le tester avant de procéder à son installation sur tous les ordinateurs. Consultez le *guide de configuration des stratégies de Sophos Enterprise Manager* pour plus de conseils.

Pour plus d'informations sur les paramètres par défaut du pare-feu, consultez l'article 57756 de la base de connaissances du support Sophos (<http://www.sophos.fr/support/knowledgebase/article/57756.html>).

Pour plus d'informations sur la prévention des ponts entre réseaux, reportez-vous à la section [À propos du contrôle des périphériques](#) à la page 111.

**Important :** lorsque vous appliquez une nouvelle stratégie ou une stratégie mise à jour sur les ordinateurs, les applications qui étaient autorisées auparavant peuvent être bloquées brièvement jusqu'à ce que la nouvelle stratégie soit entièrement appliquée. Avertissez vos utilisateurs de ce qui va se passer avant d'appliquer les nouvelles stratégies.

**Remarque :** si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - pare-feu** pour configurer une stratégie de pare-feu. Pour plus d'informations sur l'administration déléguée, reportez-vous à la section [À propos des rôles](#) à la page 15.

Pour configurer une stratégie de pare-feu :

1. Dans le volet **Stratégies**, cliquez deux fois sur **Pare-feu**.
2. Cliquez deux fois sur la stratégie **Par défaut** pour la modifier.

L'assistant de **Stratégie de pare-feu** apparaît. Suivez les instructions à l'écran. Retrouvez ci-dessous des informations supplémentaires sur certaines des options.

3. Sur la page **Configuration du pare-feu**, sélectionnez le type d'emplacement :
  - Sélectionnez **Emplacement unique** pour les ordinateurs qui sont toujours sur le réseau, par exemple, les stations de travail.
  - Sélectionnez **Emplacement double** si vous voulez que le pare-feu utilise des paramètres différents en fonction de l'emplacement où les ordinateurs sont utilisés, par exemple, au bureau (connecté au réseau) et en dehors du bureau (déconnecté du réseau). Il peut être judicieux de paramétrer un emplacement double pour les ordinateurs portables.

4. Sur la page **Mode de fonctionnement**, sélectionnez la manière dont le pare-feu va gérer le trafic entrant et sortant.

Mode	Description
<b>Bloquer le trafic entrant et sortant</b>	<ul style="list-style-type: none"> <li>■ Niveau par défaut. Offre le plus haut niveau de sécurité.</li> <li>■ Autorise uniquement le trafic essentiel via le pare-feu et authentifie les applications grâce aux sommes de contrôle.</li> <li>■ Pour autoriser les applications les plus fréquemment utilisées au sein de votre entreprise à communiquer par le biais du pare-feu, cliquez sur <b>Accepter</b>. Pour plus d'informations, reportez-vous à la section <a href="#">À propos des applications fiables</a> à la page 88.</li> </ul>
<b>Bloquer le trafic entrant et autoriser le trafic sortant</b>	<ul style="list-style-type: none"> <li>■ Offre un niveau de sécurité inférieur à <b>Bloquer le trafic entrant et sortant</b>.</li> <li>■ Autorise vos ordinateurs à accéder au réseau et à Internet sans qu'il vous soit nécessaire de créer de règles spéciales.</li> <li>■ Toutes les applications sont autorisées à communiquer par le biais du pare-feu.</li> </ul>
<b>Surveiller</b>	<ul style="list-style-type: none"> <li>■ Applique toutes les règles que vous avez définies au trafic réseau. Si le trafic n'a aucune règle de correspondance, il est signalé à la console, et il est autorisé uniquement s'il est sortant.</li> <li>■ Ce mode vous permet de collecter des informations sur votre réseau et, par la suite, de créer des règles appropriées avant de déployer le pare-feu sur tous vos ordinateurs. Pour plus d'informations, reportez-vous à la section <a href="#">À propos du mode surveillance</a> à la page 82.</li> </ul>

5. Sur la page **Partage de fichiers et d'imprimantes**, sélectionnez **Autoriser le partage de fichiers et d'imprimantes** si vous souhaitez autoriser les ordinateurs à partager les imprimantes et les dossiers locaux sur le réseau.

Après avoir paramétré le pare-feu, vous pouvez consulter les événements de pare-feu (par exemple, les applications bloquées par le pare-feu) dans **Pare-feu - Observateur d'événements**. Pour plus de détails, reportez-vous à la section [Affichage des événements du pare-feu](#) à la page 128.

Le nombre d'ordinateurs avec des événements au-dessus d'un seuil spécifié dans les sept derniers jours apparaît aussi sur le Tableau de bord.

### 7.2.1.2 À propos du mode surveillance

Activez le mode surveillance sur des ordinateurs de test et utilisez l'Observateur d'événements du pare-feu pour voir le trafic et voir quelles applications et quels processus sont utilisés.

Vous pouvez ensuite utiliser l'Observateur d'événements pour créer des règles qui autorisent ou bloquent le trafic, les applications et les processus signalés comme le décrit la section [Création d'une règle d'événement de pare-feu](#) à la page 85.

**Remarque :** lorsque vous créez une règle à l'aide de l'Observateur d'événements du pare-feu et que vous l'ajoutez à la stratégie de pare-feu, le mode du pare-feu passe de **Surveiller** à **Personnaliser**.

Si vous ne souhaitez pas autoriser le trafic inconnu par défaut, vous pouvez utiliser le *mode interactif*.

En mode interactif, le pare-feu demande à l'utilisateur d'autoriser ou de bloquer toutes les applications et tout le trafic pour lesquels ne s'appliquent aucune règle. Pour plus de détails, reportez-vous à la section [À propos du mode interactif](#) à la page 87 et consultez les autres rubriques à la section "Fonctionnement en mode interactif".

### 7.2.1.3 Ajout et acceptation d'une application

**Remarque :** si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - pare-feu** pour configurer une stratégie de pare-feu. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Les applications acceptées reçoivent un accès intégral et inconditionnel au réseau, y compris l'accès à Internet.

Pour ajouter une application dans la stratégie de pare-feu et l'accepter :

1. Vérifiez quelle stratégie de pare-feu est utilisée par le ou les groupes d'ordinateurs que vous désirez configurer.  
Reportez-vous à la section [Vérification des stratégies utilisées par un groupe](#) à la page 23.
2. Dans le volet **Stratégies**, cliquez deux fois sur **Pare-feu** puis cliquez deux fois sur la stratégie que vous souhaitez changer.
3. Sur la page **Mode de fonctionnement** de l'assistant **Stratégie de pare-feu**, cliquez sur **Accepter**.

La boîte de dialogue **Stratégie de pare-feu** apparaît.

4. Cliquez sur **Ajouter**.  
La boîte de dialogue **Stratégie de pare-feu - Ajouter une application fiable** apparaît.
5. Dans le champ **Période de recherche**, cliquez sur la flèche du menu déroulant et sélectionnez la période pour laquelle vous souhaitez afficher les événements d'applications.  
Vous pouvez sélectionner soit une période fixe, par exemple, **Depuis 24 heures**, soit **Personnalisée** et spécifiez votre propre période en sélectionnant les dates de début et de fin.
6. Si vous voulez consulter les événements d'applications d'un certain type, dans le champ **Type d'événement**, cliquez sur la flèche du menu déroulant et sélectionnez le type d'événement.
7. Si vous voulez consulter les événements d'applications pour un certain fichier, saisissez le nom du fichier dans le champ **Nom du fichier**.  
Si vous laissez ce champ vide, les événements d'applications de tous les fichiers apparaîtront.  
Vous pouvez utiliser des caractères joker dans ce champ. Utilisez ? pour remplacer un seul caractère du nom et \* pour remplacer une chaîne de caractères quelconque.
8. Cliquez sur **Rechercher** pour afficher une liste d'événements d'applications.

9. Sélectionnez un événement d'applications, puis cliquez sur **OK**.

L'application est ajoutée à la stratégie de pare-feu et marquée comme **Fiable**.

#### 7.2.1.4 Autorisation de tout le trafic sur un réseau local (LAN)

**Remarque :** si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - pare-feu** pour configurer une stratégie de pare-feu. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Pour autoriser tout le trafic entre les ordinateurs sur un réseau local :

1. Vérifiez quelle stratégie de pare-feu est utilisée par le ou les groupes d'ordinateurs que vous désirez configurer.  
Reportez-vous à la section [Vérification des stratégies utilisées par un groupe](#) à la page 23.
2. Dans le volet **Stratégies**, cliquez deux fois sur **Pare-feu** puis cliquez deux fois sur la stratégie que vous souhaitez changer.
3. Sur la page **Partage de fichiers et d'imprimantes** de l'assistant **Stratégie de pare-feu**, sélectionnez **Utiliser les paramètres personnalisés**, puis cliquez sur **Personnalisé**.
4. Dans la liste **Paramètres du réseau local**, sélectionnez la case **Fiable** pour un réseau.

#### Remarques

- Si vous autorisez tout le trafic entre les ordinateurs sur un réseau local (LAN), vous autorisez également le partage de fichiers et d'imprimantes.

#### 7.2.1.5 Autorisation du partage de fichiers et d'imprimantes

**Remarque :** si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - pare-feu** pour configurer une stratégie de pare-feu. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Pour autoriser les ordinateurs à partager les imprimantes et les dossiers locaux sur le réseau :

1. Vérifiez quelle stratégie de pare-feu est utilisée par le ou les groupes d'ordinateurs que vous désirez configurer.  
Reportez-vous à la section [Vérification des stratégies utilisées par un groupe](#) à la page 23.
2. Dans le volet **Stratégies**, cliquez deux fois sur **Pare-feu** puis cliquez deux fois sur la stratégie que vous souhaitez changer.
3. Sur la page **Partage de fichiers et d'imprimantes** de l'assistant **Stratégie de pare-feu**, sélectionnez **Autoriser le partage de fichiers et d'imprimantes**.

#### 7.2.1.6 Autorisation d'un contrôle plus souple du partage de fichiers et d'imprimantes

**Remarque :** si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - pare-feu** pour configurer une stratégie de pare-feu. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Si vous souhaitez assouplir le contrôle du partage de fichiers et d'imprimantes sur vos réseaux (par exemple, le trafic NetBIOS unidirectionnel), procédez de la manière suivante :

1. Autorisez le partage de fichiers et d'imprimantes sur d'autres réseaux locaux (LAN) que ceux figurant dans la liste **Paramètres du réseau local**. Cette opération permet aux règles de pare-feu de traiter le trafic NetBIOS sur ces réseaux locaux.
2. Créez des règles globales à haute priorité qui autorisent la communication vers/depuis les hôtes avec les ports et protocoles NetBIOS appropriés. Nous vous recommandons de créer des règles globales afin de bloquer tout le trafic de partage de fichiers et d'imprimantes indésirable plutôt que de laisser la règle par défaut le gérer.

Pour autoriser le partage de fichiers et d'imprimantes sur d'autres réseaux locaux que ceux de la liste des **Paramètres du réseau local** :

1. Vérifiez quelle stratégie de pare-feu est utilisée par le ou les groupes d'ordinateurs que vous désirez configurer.  
Reportez-vous à la section [Vérification des stratégies utilisées par un groupe](#) à la page 23.
2. Dans le volet **Stratégies**, cliquez deux fois sur **Pare-feu** puis cliquez deux fois sur la stratégie que vous souhaitez changer.
3. Sur la page **Partage de fichiers et d'imprimantes** de l'assistant **Stratégie de pare-feu**, sélectionnez **Utiliser les paramètres personnalisés**, puis cliquez sur **Personnalisé**.
4. Dessélectionnez la case à cocher **Bloquer le partage de fichiers et d'imprimantes pour d'autres réseaux**.

#### 7.2.1.7 Blocage du partage de fichiers et d'imprimantes non désiré

**Remarque :** si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - pare-feu** pour configurer une stratégie de pare-feu. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Pour bloquer le partage de fichiers et d'imprimantes sur d'autres réseaux locaux que ceux figurant dans la liste des **Paramètres du réseau local** sur l'onglet **Réseau local** :

1. Vérifiez quelle stratégie de pare-feu est utilisée par le ou les groupes d'ordinateurs que vous désirez configurer.  
Reportez-vous à la section [Vérification des stratégies utilisées par un groupe](#) à la page 23.
2. Dans le volet **Stratégies**, cliquez deux fois sur **Pare-feu** puis cliquez deux fois sur la stratégie que vous souhaitez changer.
3. Sur la page **Partage de fichiers et d'imprimantes** de l'assistant **Stratégie de pare-feu**, sélectionnez **Utiliser les paramètres personnalisés**, puis cliquez sur **Personnalisé**.
4. Sélectionnez la case à cocher **Bloquer le partage de fichiers et d'imprimantes pour d'autres réseaux**.

#### 7.2.1.8 Création d'une règle d'événement de pare-feu

**Remarque :** si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - pare-feu** pour configurer une stratégie de pare-feu. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Vous pouvez créer des règles pour tous les événements de pare-feu à l'exception des événements de "mémoire modifiée".

Pour créer une règle d'événement de pare-feu :

1. Dans le menu **Affichage**, cliquez sur **Événements du pare-feu**.

2. Dans la boîte de dialogue **Pare-feu - Observateur d'événements**, sélectionnez l'événement de l'application pour laquelle vous voulez créer une règle et cliquez sur **Créer une règle**.
3. Dans la boîte de dialogue qui apparaît, sélectionnez une option que vous voulez appliquer à l'application.
4. Sélectionnez l'emplacement auquel vous souhaitez appliquer la règle (principal, secondaire ou les deux). Si vous choisissez d'appliquer la règle à l'emplacement secondaire ou aux deux emplacements, la règle sera uniquement ajoutée aux stratégies dont l'emplacement secondaire est configuré. Cliquez sur **OK**.

**Remarque :** les événements “nouvelle application” et “application modifiée” ne sont liés à aucun emplacement (ils ajoutent des sommes de contrôle qui sont partagées entre les deux emplacements). Vous ne pouvez pas sélectionner un emplacement pour ces événements.

5. Dans la liste des stratégies de pare-feu, sélectionnez une ou plusieurs stratégies auxquelles vous voulez appliquer la règle. Cliquez sur **OK**.

**Remarque :** si vous souhaitez créer une règle d'applications directement depuis une stratégie de pare-feu à l'aide des pages de configuration de la stratégie de pare-feu avancée, reportez-vous à la section [Création d'une règle d'applications depuis une stratégie de pare-feu](#) à la page 103.

### 7.2.1.9 Désactivation temporaire du pare-feu

**Remarque :** si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - pare-feu** pour configurer une stratégie de pare-feu. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Par défaut, le pare-feu est activé. Il peut parfois être nécessaire de désactiver temporairement le pare-feu pour effectuer des opérations de maintenance ou pour résoudre des problèmes, puis de le réactiver.

Pour désactiver le pare-feu pour un groupe d'ordinateurs :

1. Vérifiez quelle stratégie de pare-feu est utilisée par le ou les groupes d'ordinateurs que vous désirez configurer.  
Reportez-vous à la section [Vérification des stratégies utilisées par un groupe](#) à la page 23.
2. Dans le volet **Stratégies**, cliquez deux fois sur **Pare-feu**. Puis cliquez deux fois sur la stratégie que vous désirez changer.

L'assistant de **Stratégie de pare-feu** apparaît.

3. Sur la page de bienvenue de l'assistant, procédez de la manière suivante :
  - Si vous souhaitez désactiver le pare-feu pour tous les emplacements que vous avez configuré (emplacement principal et emplacement secondaire, si vous en avez un de configuré), cliquez sur **Suivant**. Sur la page **Configuration du pare-feu**, sélectionnez **Autoriser tout le trafic (le pare-feu est désactivé)**. Fermez l'assistant.
  - Si vous souhaitez désactiver le pare-feu pour l'un des emplacements (principal ou secondaire), cliquez sur le bouton **Stratégie de pare-feu avancée**. Dans la boîte de dialogue **Stratégie de pare-feu** qui apparaît, sélectionnez la case **Autoriser tout le trafic** à côté de l'**Emplacement principal** ou de l'**Emplacement secondaire**. Cliquez sur **OK**. Fermez l'assistant de **Stratégie de pare-feu**.

Si vous désactivez le pare-feu, vos ordinateurs restent sans protection jusqu'à ce qu'il soit réactivé. Pour activer le pare-feu, désélectionnez la case **Autoriser tout le trafic**.

## 7.2.2 Configuration avancée du pare-feu

### 7.2.2.1 Ouverture des pages de configuration avancée

**Remarque :** si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - pare-feu** pour configurer une stratégie de pare-feu. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Si vous souhaitez avoir plus de contrôle sur les paramètres du pare-feu et pouvoir les ajuster plus précisément, vous pouvez utiliser les pages de configuration de la stratégie de pare-feu avancée pour configurer le pare-feu.

Pour ouvrir les pages de configuration de la stratégie de pare-feu avancée :

1. Cliquez deux fois sur la stratégie de pare-feu que vous désirez modifier.
2. Sur la page **Bienvenue** de l'assistant **Stratégie de pare-feu**, cliquez sur **Stratégie de pare-feu avancée**.
3. Sous **Configurations**, cliquez sur **Configurer** près de l'emplacement pour lequel vous voulez configurer le pare-feu.

### 7.2.2.2 Fonctionnement en mode interactif

#### 7.2.2.2.1 À propos du mode interactif

En mode interactif, le pare-feu affiche une boîte de dialogue d'apprentissage à chaque fois qu'une application ou un service inconnu demande l'accès au réseau. La boîte de dialogue d'apprentissage demande à l'utilisateur d'autoriser ou de bloquer le trafic ou de créer une règle pour ce type de trafic.

#### 7.2.2.2.2 Activation du mode interactif

**Remarque :** si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - pare-feu** pour configurer une stratégie de pare-feu. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Le pare-feu peut fonctionner en mode interactif en demandant à l'utilisateur comment il doit traiter le trafic détecté. Pour plus d'informations, reportez-vous à la section [À propos du mode interactif](#) à la page 87.

Pour mettre le pare-feu en mode interactif sur un groupe d'ordinateurs :

1. Vérifiez quelle stratégie de pare-feu est utilisée par le ou les groupes d'ordinateurs que vous désirez configurer.  
Reportez-vous à la section [Vérification des stratégies utilisées par un groupe](#) à la page 23.
2. Dans le volet **Stratégies**, cliquez deux fois sur **Pare-feu** puis cliquez deux fois sur la stratégie que vous souhaitez changer.
3. Sur la page de **Bienvenue** de l'assistant **Stratégie de pare-feu**, cliquez sur **Stratégie de pare-feu avancée**.
4. Sous **Configurations**, cliquez sur le bouton **Configurer** correspondant à l'emplacement que vous souhaitez configurer.

5. Sur l'onglet **Général**, sous **Mode de fonctionnement**, cliquez sur **Interactif**.

### 7.2.2.2.3 Passage en mode non interactif

**Remarque :** si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - pare-feu** pour configurer une stratégie de pare-feu. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Il existe deux modes non interactifs :

- Autoriser par défaut
- Bloquer par défaut

En modes non interactifs, le pare-feu traite le trafic réseau automatiquement en utilisant vos règles. Le trafic réseau sans règle de correspondance est soit entièrement autorisé (s'il est sortant), soit totalement bloqué.

Pour passer en mode non interactif sur un groupe d'ordinateurs :

1. Dans le volet **Stratégies**, cliquez deux fois sur **Pare-feu** puis cliquez deux fois sur la stratégie que vous souhaitez changer.
2. Sur la page de **Bienvenue** de l'assistant **Stratégie de pare-feu**, cliquez sur **Stratégie de pare-feu avancée**.
3. Sous **Configurations**, cliquez sur le bouton **Configurer** correspondant à l'emplacement que vous souhaitez configurer.
4. Cliquez sur l'onglet **Général**.
5. Sous **Mode de fonctionnement**, cliquez sur **Autoriser par défaut** ou sur **Bloquer par défaut**.

### 7.2.2.3 Configuration du pare-feu

#### 7.2.2.3.1 À propos des applications fiables

Pour vous aider à assurer la sécurité de vos ordinateurs, le pare-feu bloque le trafic provenant d'applications non reconnues sur vos ordinateurs. Toutefois, il est possible que les applications les plus fréquemment utilisées au sein de votre entreprise soient bloquées et empêchent vos utilisateurs d'effectuer leurs tâches quotidiennes.

Vous pouvez faire *confiance* à ces applications afin qu'elles puissent communiquer par le biais du pare-feu. Les applications fiables reçoivent un accès intégral et inconditionnel au réseau et à Internet.

**Remarque :** pour une sécurité renforcée, vous pouvez appliquer une ou plusieurs règles d'applications afin de spécifier les conditions d'exécution de l'application. Pour plus d'informations sur la manière de procéder, reportez-vous à la section [Création d'une règle d'applications](#) à la page 102 et aux autres rubriques de la section *Règles d'applications*.

#### 7.2.2.3.2 Ajout d'une application dans une stratégie de pare-feu

**Remarque :** si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - pare-feu** pour configurer une stratégie de pare-feu. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Pour ajouter une application dans une stratégie de pare-feu :

1. Vérifiez quelle stratégie de pare-feu est utilisée par le ou les groupes d'ordinateurs que vous désirez configurer.  
Reportez-vous à la section [Vérification des stratégies utilisées par un groupe](#) à la page 23.
2. Dans le volet **Stratégies**, cliquez deux fois sur **Pare-feu** puis cliquez deux fois sur la stratégie que vous souhaitez changer.
3. Sur la page de **Bienvenue** de l'assistant **Stratégie de pare-feu**, cliquez sur **Stratégie de pare-feu avancée**.
4. Sous **Configurations**, cliquez sur le bouton **Configurer** correspondant à l'emplacement que vous souhaitez configurer.
5. Cliquez sur l'onglet **Applications**
6. Cliquez sur **Ajouter**.

La boîte de dialogue **Stratégie de pare-feu - Ajouter une application** apparaît.

7. Dans le champ **Période de recherche**, cliquez sur la flèche du menu déroulant et sélectionnez la période pour laquelle vous souhaitez afficher les événements d'applications.  
Vous pouvez sélectionner soit une période fixe, par exemple, **Depuis 24 heures**, soit **Personnalisée** et spécifiez votre propre période en sélectionnant les dates de début et de fin.
8. Si vous voulez consulter les événements d'applications d'un certain type, dans le champ **Type d'événement**, cliquez sur la flèche du menu déroulant et sélectionnez le type d'événement.
9. Si vous voulez consulter les événements d'applications pour un certain fichier, saisissez le nom du fichier dans le champ **Nom du fichier**.  
Si vous laissez ce champ vide, les événements d'applications de tous les fichiers apparaîtront.  
Vous pouvez utiliser des caractères joker dans ce champ. Utilisez ? pour remplacer un seul caractère du nom et \* pour remplacer une chaîne de caractères quelconque.
10. Cliquez sur **Rechercher** pour afficher une liste d'événements d'applications.
11. Sélectionnez un événement d'applications, puis cliquez sur **OK**.

- L'application est ajoutée à la stratégie de pare-feu et marquée comme **Fiable**.
- La somme de contrôle de l'application est ajoutée à la liste des sommes de contrôle autorisées.

### 7.2.2.3.3 Suppression d'une application d'une stratégie de pare-feu

**Remarque:** si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - pare-feu** pour configurer une stratégie de pare-feu. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Pour supprimer une application d'une stratégie de pare-feu :

1. Vérifiez quelle stratégie de pare-feu est utilisée par le ou les groupes d'ordinateurs que vous désirez configurer.  
Reportez-vous à la section [Vérification des stratégies utilisées par un groupe](#) à la page 23.

2. Dans le volet **Stratégies**, cliquez deux fois sur **Pare-feu** puis cliquez deux fois sur la stratégie que vous souhaitez changer.
3. Sur la page de **Bienvenue** de l'assistant **Stratégie de pare-feu**, cliquez sur **Stratégie de pare-feu avancée**.
4. Sous **Configurations**, cliquez sur le bouton **Configurer** correspondant à l'emplacement que vous souhaitez configurer.
5. Cliquez sur l'onglet **Applications**
6. Sélectionnez l'application dans la liste et cliquez sur **Supprimer**.

#### 7.2.2.3.4 Acceptation d'une application

**Remarque:** si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - pare-feu** pour configurer une stratégie de pare-feu. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Pour accepter une application sur un groupe d'ordinateurs :

1. Vérifiez quelle stratégie de pare-feu est utilisée par le ou les groupes d'ordinateurs que vous désirez configurer.  
Reportez-vous à la section [Vérification des stratégies utilisées par un groupe](#) à la page 23.
2. Dans le volet **Stratégies**, cliquez deux fois sur **Pare-feu** puis cliquez deux fois sur la stratégie que vous souhaitez changer.
3. Sur la page de **Bienvenue** de l'assistant **Stratégie de pare-feu**, cliquez sur **Stratégie de pare-feu avancée**.
4. Sous **Configurations**, cliquez sur le bouton **Configurer** correspondant à l'emplacement que vous souhaitez configurer.
5. Cliquez sur l'onglet **Applications**  
Si l'application n'est pas dans la liste, suivez les instructions de la section [Ajout d'une application dans une stratégie de pare-feu](#) à la page 88 pour l'ajouter.
6. Sélectionnez l'application dans la liste et cliquez sur **Accepter**.
  - L'application est ajoutée à la stratégie de pare-feu et marquée comme **Fiable**.
  - La somme de contrôle de l'application est ajoutée à la liste des sommes de contrôle autorisées.

Les applications acceptées reçoivent un accès intégral et inconditionnel au réseau, y compris l'accès à Internet. Pour une sécurité renforcée, vous pouvez appliquer une ou plusieurs *règles d'applications* afin de spécifier les conditions d'exécution de l'application.

- [Création d'une règle d'applications](#) à la page 102
- [Application de règles d'applications prédéterminées](#) à la page 104

#### 7.2.2.3.5 Acceptation d'une application à l'aide de l'Observateur d'événements du pare-feu

**Remarque:** si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - pare-feu** pour configurer une stratégie de pare-feu. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Si le pare-feu signale une application inconnue ou bloque une application sur vos ordinateurs en réseau, un événement apparaît dans l'Observateur d'événements du pare-feu. Cette rubrique

vous décrit comment accepter une application depuis l'Observateur d'événements du pare-feu et comment appliquer la nouvelle règle aux stratégies de pare-feu de votre choix.

Pour retrouver plus de détails sur les applications signalées ou bloquées dans l'Observateur d'événements du pare-feu et pour les accepter ou créer de nouvelles règles pour ces applications :

1. Dans le menu **Affichage**, cliquez sur **Événements du pare-feu**.
  2. Dans la boîte de dialogue **Pare-feu - Observateur d'événements**, sélectionnez l'entrée de l'application pour laquelle vous voulez accepter ou créer une règle et cliquez ensuite sur **Créer une règle**.
  3. Dans la boîte de dialogue qui apparaît, indiquez si vous voulez accepter l'application ou lui créer une règle à l'aide d'une option prédéfinie existante.
  4. A partir de la liste des stratégies de pare-feu, sélectionnez celles auxquelles vous voulez appliquer la règle. Pour appliquer la règle à toutes les stratégies, cliquez sur **Tout sélectionner**, puis cliquez sur **OK**.
- Si vous utilisez des sommes de contrôle, ajoutez la somme de contrôle de l'application à la liste des sommes de contrôle autorisées. Reportez-vous à la section [Ajout d'une somme de contrôle d'application](#) à la page 93.
  - Vous pouvez aussi ajouter une application comme fiable directement dans une stratégie de pare-feu à l'aide des pages de configuration de la stratégie de pare-feu avancée. Reportez-vous à la section [Création d'une règle d'applications depuis une stratégie de pare-feu](#) à la page 103.

#### 7.2.2.3.6 Blocage d'une application

**Remarque:** si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - pare-feu** pour configurer une stratégie de pare-feu. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Pour bloquer une application sur un groupe d'ordinateurs :

1. Vérifiez quelle stratégie de pare-feu est utilisée par le ou les groupes d'ordinateurs que vous désirez configurer.  
Reportez-vous à la section [Vérification des stratégies utilisées par un groupe](#) à la page 23.
2. Dans le volet **Stratégies**, cliquez deux fois sur **Pare-feu** puis cliquez deux fois sur la stratégie que vous souhaitez changer.
3. Sur la page de **Bienvenue** de l'assistant **Stratégie de pare-feu**, cliquez sur **Stratégie de pare-feu avancée**.
4. Sous **Configurations**, cliquez sur le bouton **Configurer** correspondant à l'emplacement que vous souhaitez configurer.
5. Cliquez sur l'onglet **Applications**  
Si l'application n'est pas dans la liste, suivez les instructions de la section [Ajout d'une application dans une stratégie de pare-feu](#) à la page 88 pour l'ajouter.
6. Sélectionnez l'application dans la liste et cliquez sur **Bloquer**.

### 7.2.2.3.7 Autorisation de lancement des processus cachés aux applications

**Remarque:** si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - pare-feu** pour configurer une stratégie de pare-feu. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Une application lance parfois un autre processus caché afin qu'il lui trouve un accès au réseau.

Des applications malveillantes peuvent utiliser cette technique pour échapper aux pare-feu : au lieu de le faire elles-mêmes, elles lancent une application fiable pour qu'elle accède au réseau.

Pour autoriser des applications à lancer des processus cachés :

1. Cliquez deux fois sur la stratégie de pare-feu que vous désirez modifier.
2. Sur la page **Bienvenue** de l'assistant **Stratégie de pare-feu**, cliquez sur **Stratégie de pare-feu avancée**.
3. Sous **Configurations**, cliquez sur **Configurer** près de l'emplacement pour lequel vous voulez configurer le pare-feu.
4. Cliquez sur l'onglet **Processus**.
5. Dans la zone supérieure, cliquez sur le bouton **Ajouter**.

La boîte de dialogue **Stratégie de pare-feu - Ajouter une application** apparaît.

6. Dans le champ **Période de recherche**, cliquez sur la flèche du menu déroulant et sélectionnez la période pour laquelle vous souhaitez afficher les événements d'applications.

Vous pouvez sélectionner soit une période fixe, par exemple, **Depuis 24 heures**, soit **Personnalisée** et spécifiez votre propre période en sélectionnant les dates de début et de fin.

7. Si vous voulez consulter les événements d'applications d'un certain type, dans le champ **Type d'événement**, cliquez sur la flèche du menu déroulant et sélectionnez le type d'événement.
8. Si vous voulez consulter les événements d'applications pour un certain fichier, saisissez le nom du fichier dans le champ **Nom du fichier**.

Si vous laissez ce champ vide, les événements d'applications de tous les fichiers apparaîtront.

Vous pouvez utiliser des caractères joker dans ce champ. Utilisez ? pour remplacer un seul caractère du nom et \* pour remplacer une chaîne de caractères quelconque.

9. Cliquez sur **Rechercher** pour afficher une liste d'événements d'applications.
10. Sélectionnez un événement d'applications, puis cliquez sur **OK**.

Si vous activez le mode interactif, le pare-feu peut afficher une boîte de dialogue d'apprentissage sur le poste d'extrémité lorsqu'il détecte un nouveau programme de lancement. Pour plus de détails, reportez-vous à la section [Activation du mode interactif](#) à la page 87.

### 7.2.2.3.8 Autorisation d'utilisation des rawsockets aux applications

**Remarque:** si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - pare-feu** pour configurer une stratégie de pare-feu. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Certaines applications peuvent accéder au réseau par le biais des rawsockets, et ainsi avoir le contrôle sur tous les aspects des données qu'elles envoient sur le réseau.

Les applications malveillantes exploitent les rawsockets en contrefaisant leur adresse IP ou en envoyant des messages corrompus.

Pour autoriser les applications à accéder au réseau par le biais des rawsockets :

1. Cliquez deux fois sur la stratégie de pare-feu que vous désirez modifier.
2. Sur la page **Bienvenue** de l'assistant **Stratégie de pare-feu**, cliquez sur **Stratégie de pare-feu avancée**.
3. Sous **Configurations**, cliquez sur **Configurer** près de l'emplacement pour lequel vous voulez configurer le pare-feu.
4. Cliquez sur l'onglet **Processus**.
5. Dans la zone inférieure, cliquez sur le bouton **Ajouter**.

La boîte de dialogue **Stratégie de pare-feu - Ajouter une application** apparaît.

6. Dans le champ **Période de recherche**, cliquez sur la flèche du menu déroulant et sélectionnez la période pour laquelle vous souhaitez afficher les événements d'applications.  
Vous pouvez sélectionner soit une période fixe, par exemple, **Depuis 24 heures**, soit **Personnalisée** et spécifiez votre propre période en sélectionnant les dates de début et de fin.
7. Si vous voulez consulter les événements d'applications d'un certain type, dans le champ **Type d'événement**, cliquez sur la flèche du menu déroulant et sélectionnez le type d'événement.
8. Si vous voulez consulter les événements d'applications pour un certain fichier, saisissez le nom du fichier dans le champ **Nom du fichier**.  
Si vous laissez ce champ vide, les événements d'applications de tous les fichiers apparaîtront.  
Vous pouvez utiliser des caractères joker dans ce champ. Utilisez ? pour remplacer un seul caractère du nom et \* pour remplacer une chaîne de caractères quelconque.
9. Cliquez sur **Rechercher** pour afficher une liste d'événements d'applications.
10. Sélectionnez un événement d'applications, puis cliquez sur **OK**.

Si vous activez le mode interactif, le pare-feu peut afficher une boîte de dialogue d'apprentissage sur le poste d'extrémité lorsqu'une rawsocket est détectée. Pour plus de détails, reportez-vous à la section [Activation du mode interactif](#) à la page 87.

#### 7.2.2.3.9 Ajout d'une somme de contrôle d'application

**Remarque :** si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - pare-feu** pour configurer une stratégie de pare-feu. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Chaque version d'une application a une somme de contrôle unique. Le pare-feu peut utiliser cette somme de contrôle pour décider si une application est autorisée ou non.

Par défaut, le pare-feu vérifie la somme de contrôle de chaque application qui s'exécute. Si la somme de contrôle est inconnue ou a changé, le pare-feu la bloque.

Pour ajouter une somme de contrôle à la liste des sommes de contrôle autorisées :

1. Cliquez deux fois sur la stratégie de pare-feu que vous désirez modifier.

2. Sur la page **Bienvenue** de l'assistant **Stratégie de pare-feu**, cliquez sur **Stratégie de pare-feu avancée**.
3. Cliquez sur l'onglet **Sommes de contrôle**.
4. Cliquez sur **Ajouter**.  
La boîte de dialogue **Stratégie de pare-feu - Ajouter une somme de contrôle de l'application** apparaît.
5. Dans le champ **Période de recherche**, cliquez sur la flèche du menu déroulant et sélectionnez la période pour laquelle vous souhaitez afficher les événements d'applications.  
Vous pouvez sélectionner soit une période fixe, par exemple, **Depuis 24 heures**, soit **Personnalisée** et spécifiez votre propre période en sélectionnant les dates de début et de fin.
6. Dans le champ **Type d'événement**, cliquez sur la flèche du menu déroulant et indiquez si vous voulez ajouter une somme de contrôle pour une application modifiée ou pour une nouvelle application.
7. Si vous voulez consulter les événements d'applications pour un certain fichier, saisissez le nom du fichier dans le champ **Nom du fichier**.  
Si vous laissez ce champ vide, les événements d'applications de tous les fichiers apparaîtront.  
Vous pouvez utiliser des caractères joker dans ce champ. Utilisez ? pour remplacer un seul caractère du nom et \* pour remplacer une chaîne de caractères quelconque.
8. Cliquez sur **Rechercher** pour afficher une liste d'événements d'applications.
9. Sélectionnez l'événement d'application pour lequel vous voulez ajouter une somme de contrôle, puis cliquez sur **OK**.

La somme de contrôle d'une application est ajoutée à la liste des sommes de contrôle autorisées dans la boîte de dialogue **Stratégie de pare-feu**.

Si vous activez le mode interactif, le pare-feu peut afficher une boîte de dialogue d'apprentissage sur le poste d'extrémité lorsqu'il détecte une application nouvelle ou modifiée. Pour plus de détails, reportez-vous à la section [Activation du mode interactif](#) à la page 87.

#### 7.2.2.3.10 Activation ou désactivation du blocage des processus modifiés

**Remarque :** si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - pare-feu** pour configurer une stratégie de pare-feu. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Certains programmes malveillants tentent de contourner le pare-feu en modifiant un processus en mémoire lancé par un programme de confiance et en utilisant ensuite ce processus modifié pour accéder au réseau.

Vous pouvez configurer le pare-feu pour détecter et bloquer les processus qui ont été modifiés en mémoire.

Pour activer ou désactiver le blocage des processus modifiés :

1. Cliquez deux fois sur la stratégie de pare-feu que vous désirez modifier.
2. Sur la page **Bienvenue** de l'assistant **Stratégie de pare-feu**, cliquez sur **Stratégie de pare-feu avancée**.

3. Sous **Configurations**, cliquez sur **Configurer** près de l'emplacement pour lequel vous voulez configurer le pare-feu.
4. Sur l'onglet **Général**, sous **Blocage**, désélectionnez la case **Bloquer les processus si la mémoire est modifiée par une autre application** pour désactiver le blocage des processus modifiés.

Pour activer le blocage des processus modifiés, sélectionnez cette case à cocher.

Si le pare-feu détecte un processus modifié dans la mémoire, il ajoute une règle pour empêcher l'accès au réseau à ce processus modifié.

### Remarques

- Nous ne recommandons pas la désactivation permanente du blocage des processus modifiés. Désactivez cette option uniquement lorsque cela est nécessaire.
- Le blocage des processus modifiés n'est pas pris en charge par les versions 64 bits de Windows.
- Seul le processus modifié est bloqué. Le programme effectuant la modification n'est pas bloqué et a donc accès au réseau.

#### 7.2.2.3.11 Filtrage des messages ICMP

**Remarque :** si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - pare-feu** pour configurer une stratégie de pare-feu. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Les messages ICMP (Internet Control Message Protocol) autorisent les ordinateurs d'un réseau à partager les informations sur les erreurs et sur leur état. Vous pouvez autoriser ou bloquer des types spécifiques de messages ICMP entrants ou sortants.

Filtrez uniquement les messages ICMP si vous êtes familier avec les protocoles réseau. Pour plus d'explications sur les types de message ICMP, reportez-vous à la section [Explication des types de message ICMP](#) à la page 95.

Pour filtrer les messages ICMP :

1. Cliquez deux fois sur la stratégie de pare-feu que vous désirez modifier.
2. Sur la page **Bienvenue** de l'assistant **Stratégie de pare-feu**, cliquez sur **Stratégie de pare-feu avancée**.
3. Sous **Configurations**, cliquez sur **Configurer** près de l'emplacement pour lequel vous voulez configurer le pare-feu.
4. Sur l'onglet **ICMP**, sélectionnez la case **Entrant** ou **Sortant** pour autoriser les types de messages entrants ou sortants spécifiés.

#### 7.2.2.3.12 Explication des types de message ICMP

<b>Demande d'écho, Réponse d'écho</b>	Utilisées pour tester l'accessibilité et l'état de la destination. Un hôte envoie une <b>Demande d'écho</b> et attend de recevoir la <b>Réponse d'écho</b> correspondante. Ces opérations sont généralement effectuées en utilisant la commande <b>ping</b> .
---------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

<b>Destination injoignable, Réponse d'écho</b>	Envoyé par un routeur lorsqu'il ne peut pas transmettre un datagramme IP. Un datagramme est l'unité de données ou le paquet transmis dans un réseau TCP/IP.
<b>Source éteinte</b>	Envoyé par un hôte ou un routeur lorsqu'il est saturé par le volume de données qu'il reçoit. Ce message demande à la source de réduire sa vitesse de transmission des datagrammes.
<b>Rediriger</b>	Envoyé par un routeur lorsqu'il reçoit un datagramme devant être envoyé à un routeur différent. Le message contient l'adresse vers laquelle la source doit rediriger les prochains datagrammes. Cette opération est utilisée pour optimiser l'acheminement du trafic réseau.
<b>Annonce routeur, Sollicitation routeur</b>	Autorise les hôtes à découvrir l'existence des routeurs. Les routeurs diffusent régulièrement leurs adresses IP via les messages d' <b>Annonce routeur</b> . Les hôtes peuvent aussi demander l'adresse d'un routeur en diffusant un message <b>Sollicitation routeur</b> auquel un routeur répond par une <b>Annonce routeur</b> .
<b>Temps dépassé pour un datagramme</b>	Envoyé par un routeur si le datagramme a atteint la limite maximum de routeurs par le biais desquels il est transporté.
<b>Problème de paramétrage pour un datagramme</b>	Envoyé par un routeur en cas de problème de transmission d'un datagramme entraînant l'impossibilité d'achever l'opération. L'origine de ce genre de problème peut être un en-tête de datagramme incorrect.
<b>Demande d'horodatage, Réponse d'horodatage</b>	Utilisé pour synchroniser les horloges entre les hôtes et pour estimer la durée d'acheminement.
<b>Demande Informations, Réponse Informations</b>	Obsolète. Ces messages étaient auparavant utilisés par les hôtes pour déterminer leurs adresses inter-réseau mais sont désormais obsolètes et ne doivent pas être utilisés.
<b>Demande masque d'adresse, Réponse masque d'adresse</b>	Utilisé pour retrouver le masque du sous-réseau (c'est-à-dire quels bits de l'adresse définissent le réseau). Un hôte envoie une <b>Demande masque d'adresse</b> à un routeur et reçoit une <b>Réponse masque d'adresse</b> en retour.

#### 7.2.2.4 Règles de pare-feu

##### 7.2.2.4.1 À propos des règles du pare-feu

###### Règles globales

Les règles globales s'appliquent à toutes les communications réseau et aux applications même si elles ont des règles d'applications.

###### Règles d'applications

Vous pouvez avoir une ou plusieurs règles pour une application. Vous pouvez soit utiliser des règles prédéfinies créées par Sophos soit créer des règles personnalisées qui vous procureront un contrôle précis sur l'accès autorisé à une application.

#### 7.2.2.4.2 À propos de l'ordre dans lequel les règles sont appliquées

Pour les connexions qui utilisent les rawsockets, seules les règles globales sont vérifiées.

Pour les connexions qui n'utilisent *pas* les rawsockets, de nombreuses règles sont vérifiées selon que la connexion soit établie ou non sur une adresse réseau figurant sur l'onglet **Réseau local**.

Si l'adresse réseau figure dans la liste sur l'onglet **Réseau local**, les règles suivantes sont vérifiées :

- Si l'adresse a été marquée comme **Fiable**, tout le trafic sur la connexion est autorisé sans vérifications supplémentaires.
- Si l'adresse a été marquée comme **NetBIOS**, le partage de fichiers et d'imprimantes sur toute connexion satisfaisant aux critères demandés est autorisé :

Connexion	Port	Plage
TCP	Distant	137-139 ou 445
TCP	Local	137-139 ou 445
UDP	Distant	137 ou 138
UDP	Local	137 ou 138

Si l'adresse réseau ne figure *pas* dans la liste sur l'onglet **Réseau local**, d'autres règles de pare-feu sont vérifiées dans l'ordre suivant :

1. Tout le trafic **NetBIOS** qui n'a pas été autorisé via l'onglet **Réseau local** est géré selon que la case **Bloquer le partage de fichiers et d'imprimantes pour d'autres réseaux** ait été sélectionnée ou non :
  - Si la case est sélectionnée, le trafic est bloqué.
  - Si la case est dessélectionnée, le trafic est traité par les règles restantes.
2. Les règles globales à priorité élevée sont vérifiées dans l'ordre où elles apparaissent dans la liste.
3. Si aucune règle n'a encore été appliquée à la connexion, les règles d'applications sont vérifiées.
4. Si la connexion n'a pas encore été traitée, les règles globales à priorité normale sont vérifiées dans l'ordre où elles apparaissent dans la liste.
5. Si aucune règle n'a été trouvée pour traiter la connexion :
  - En mode **Autoriser par défaut**, le trafic est autorisé (s'il est sortant).
  - En mode **Bloquer par défaut**, le trafic est bloqué.
  - En mode **Interactif**, l'utilisateur décide de l'action à mener.

**Remarque :** si vous n'avez pas changé le mode de fonctionnement, le pare-feu est en mode **Bloquer par défaut**.

#### 7.2.2.4.3 À propos de la détection du réseau local

Vous pouvez affecter le réseau local d'un ordinateur à des règles de pare-feu.

Lorsqu'il démarre, le pare-feu détermine le réseau local de l'ordinateur, puis surveille tout changement pendant son fonctionnement. Si un quelconque changement est détecté, le pare-feu met à jour toutes les règles du réseau local avec la nouvelle plage d'adresses de ce même réseau.



**Avvertissement :** nous vous conseillons d'être extrêmement vigilants lors de l'utilisation des règles du réseau local comme configurations secondaires. S'il s'agit d'un ordinateur portable utilisé en dehors du bureau, il peut se connecter à un réseau local inconnu. Dans ce cas, il est possible que les règles de pare-feu de la configuration secondaire qui utilisent le réseau local comme adresse autorisent le trafic inconnu.

#### 7.2.2.4.4 Règles globales

##### 7.2.2.4.4.1 Paramètres des règles globales par défaut

Cette section décrit les conditions et les actions pour les règles globales par défaut. Utilisez ces paramètres si vous voulez créer une nouvelle règle globale par défaut.

##### **Autoriser la résolution DNS (TCP)**

- Protocole : TCP
- Direction : sortante
- Port distant : DOMAINE
- Action : autoriser

##### **Autoriser la résolution DNS (UDP)**

- Protocole : UDP
- Direction : sortante
- Port distant : DNS
- Action : autoriser inspection dynamique

##### **Autoriser DHCP sortant**

- Protocole : UDP
- Port local : BOOTPS,BOOTPC,546,547
- Action : autoriser

##### **Autoriser identification sortante**

- Protocole : TCP
- Direction : entrante
- Port local : AUTH
- Action : autoriser

**Autoriser bouclage**

- Protocole : TCP
- Direction : entrante
- Port local : 127.0.0.0 (255.255.255.0)
- Action : autoriser

**Autoriser le protocole GRE**

- Protocole : TCP
- Type de protocole : sortant
- Action : autoriser

**Autoriser connexion contrôle PPTP**

- Protocole : TCP
- Direction : sortante
- Port distant : PPTP
- Port local : 1024-65535
- Action : autoriser

**Bloquer l'appel RPC (TCP)**

- Protocole : TCP
- Direction : entrante
- Port local : DCOM
- Action : bloquer

**Bloquer l'appel RPC (UDP)**

- Protocole : UDP
- Port local : 135
- Action : bloquer

**Bloquer le protocole Server Message Block (TCP)**

- Protocole : TCP
- Direction : entrante
- Port local : MICROSOFT\_DS
- Action : bloquer

**Bloquer le protocole Server Message (UDP)**

- Protocole : TCP
- Port local : 445
- Action : bloquer

#### **Autoriser connexion Localhost UDP**

- Protocole : UDP
- Hôte distant : 255.255.255.255 (0.0.0.0)
- Hôte local : 255.255.255.255 (0.0.0.0)
- Où le port local correspond au port distant : Vrai
- Action : autoriser

#### **7.2.2.4.4.2** *Création d'une règle globale*

**Remarque :** si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - pare-feu** pour configurer une stratégie de pare-feu. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

**Important :** nous vous recommandons de créer des règles globales uniquement si vous êtes familier avec les protocoles réseau.

Les règles globales s'appliquent à toutes les communications réseau et applications qui n'ont pas encore de règle.

Pour créer une règle globale :

1. Cliquez deux fois sur la stratégie de pare-feu que vous désirez modifier.
2. Sur la page **Bienvenue** de l'assistant **Stratégie de pare-feu**, cliquez sur **Stratégie de pare-feu avancée**.
3. Sous **Configurations**, cliquez sur **Configurer** près de l'emplacement pour lequel vous voulez configurer le pare-feu.
4. Cliquez sur l'onglet **Règles globales**.
5. Cliquez sur **Ajouter**.
6. Sous **Nom de la règle**, saisissez un nom pour la règle.  
Le nom de la règle doit être unique dans la liste des règles. Deux règles globales ne peuvent pas avoir le même nom.
7. Pour appliquer la règle avant toute règle d'applications ou toute règle globale à priorité normale, sélectionnez la case **Règle à priorité élevée**.  
Pour plus d'informations sur l'ordre dans lequel les règles sont appliquées, reportez-vous à la section [À propos de l'ordre dans lequel les règles sont appliquées](#) à la page 97.
8. Sous **Sélectionner les événements que la règle traitera**, sélectionnez les conditions auxquelles la connexion doit correspondre pour que la règle s'applique.
9. Sous **Sélectionner les actions avec lesquelles la règle répondra**, sélectionnez soit **Autoriser** soit **Bloquer**.
10. Procédez de l'une des manières suivantes :
  - Pour autoriser d'autres connexions vers et depuis la même adresse distante tout en conservant la connexion initiale existante, sélectionnez **Connexions concurrentes**.  
**Remarque :** cette option est uniquement disponible pour les règles TCP qui sont en mode dynamique par défaut.

- Pour autoriser les réponses depuis l'ordinateur distant qui seront basées sur la connexion initiale, sélectionnez **Inspection dynamique**.

11. Sous **Description de la règle**, cliquez sur une valeur soulignée. Par exemple, si vous cliquez sur le lien **TCP**, la boîte de dialogue **Sélection du protocole** s'ouvre.

#### 7.2.2.4.4.3 Modification d'une règle globale

**Remarque:** si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - pare-feu** pour configurer une stratégie de pare-feu. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

**Important :** nous vous recommandons de modifier les règles globales uniquement si vous êtes familier avec les protocoles réseau.

Pour modifier une règle globale :

1. Cliquez deux fois sur la stratégie de pare-feu que vous désirez modifier.
2. Sur la page **Bienvenue** de l'assistant **Stratégie de pare-feu**, cliquez sur **Stratégie de pare-feu avancée**.
3. Sous **Configurations**, cliquez sur **Configurer** près de l'emplacement pour lequel vous voulez configurer le pare-feu.
4. Cliquez sur l'onglet **Règles globales**.
5. Dans la liste **Règle**, sélectionnez la règle que vous souhaitez modifier.
6. Cliquez sur **Modifier**.

Pour plus d'informations sur le paramétrage des règles globales, reportez-vous à la section [Paramètres des règles globales par défaut](#) à la page 98.

#### 7.2.2.4.4.4 Copie d'une règle globale

**Remarque:** si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - pare-feu** pour configurer une stratégie de pare-feu. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Pour copier une règle globale et l'ajouter à la liste des règles :

1. Cliquez deux fois sur la stratégie de pare-feu que vous désirez modifier.
2. Sur la page **Bienvenue** de l'assistant **Stratégie de pare-feu**, cliquez sur **Stratégie de pare-feu avancée**.
3. Sous **Configurations**, cliquez sur **Configurer** près de l'emplacement pour lequel vous voulez configurer le pare-feu.
4. Cliquez sur l'onglet **Règles globales**.
5. Dans la liste **Règle**, sélectionnez la règle que vous souhaitez copier.
6. Cliquez sur **Copier**.

#### 7.2.2.4.4.5 *Suppression d'une règle globale*

**Remarque:** si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - pare-feu** pour configurer une stratégie de pare-feu. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

1. Cliquez deux fois sur la stratégie de pare-feu que vous désirez modifier.
2. Sur la page **Bienvenue** de l'assistant **Stratégie de pare-feu**, cliquez sur **Stratégie de pare-feu avancée**.
3. Sous **Configurations**, cliquez sur **Configurer** près de l'emplacement pour lequel vous voulez configurer le pare-feu.
4. Cliquez sur l'onglet **Règles globales**.
5. Dans la liste **Règle**, sélectionnez la règle que vous souhaitez supprimer.
6. Cliquez sur **Supprimer**.

#### 7.2.2.4.4.6 *Modification de l'ordre dans lequel les règles sont appliquées*

**Remarque:** si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - pare-feu** pour configurer une stratégie de pare-feu. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Les règles globales sont appliquées dans l'ordre dans lequel elles apparaissent en partant du haut de la liste.

Pour modifier l'ordre dans lequel les règles globales sont appliquées :

1. Cliquez deux fois sur la stratégie de pare-feu que vous désirez modifier.
2. Sur la page **Bienvenue** de l'assistant **Stratégie de pare-feu**, cliquez sur **Stratégie de pare-feu avancée**.
3. Sous **Configurations**, cliquez sur **Configurer** près de l'emplacement pour lequel vous voulez configurer le pare-feu.
4. Cliquez sur l'onglet **Règles globales**.
5. Dans la liste **Règle**, cliquez sur la règle que vous souhaitez faire monter ou descendre dans la liste.
6. Cliquez sur **Monter** ou **Descendre**.

#### 7.2.2.4.5 **Règles d'applications**

##### 7.2.2.4.5.1 *Création d'une règle d'applications*

**Remarque:** si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - pare-feu** pour configurer une stratégie de pare-feu. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Pour créer une règle personnalisée qui vous permettra d'ajuster avec précision l'accès autorisé pour une application :

1. Cliquez deux fois sur la stratégie de pare-feu que vous désirez modifier.
2. Sur la page **Bienvenue** de l'assistant **Stratégie de pare-feu**, cliquez sur **Stratégie de pare-feu avancée**.

3. Sous **Configurations**, cliquez sur **Configurer** près de l'emplacement pour lequel vous voulez configurer le pare-feu.
4. Cliquez sur l'onglet **Applications**
5. Sélectionnez l'application dans la liste et cliquez sur la flèche près du bouton **Personnaliser**.
6. Dans la boîte de dialogue **Règles d'applications**, cliquez sur **Ajouter**.
7. Sous **Nom de la règle**, saisissez un nom pour la règle.  
Le nom de la règle doit être unique dans la liste des règles. Deux règles d'applications ne peuvent pas avoir le même nom, en revanche, deux applications peuvent chacune avoir une règle portant le même nom.
8. Sous **Sélectionner les événements que la règle traitera**, sélectionnez les conditions auxquelles la connexion doit correspondre pour que la règle s'applique.
9. Sous **Sélectionner les actions avec lesquelles la règle répondra**, sélectionnez soit **Autoriser** soit **Bloquer**.
10. Pour autoriser les réponses depuis l'ordinateur distant qui seront basées sur la connexion initiale, sélectionnez **Inspection dynamique**.
11. Sous **Description de la règle**, cliquez sur une valeur soulignée. Par exemple, si vous cliquez sur le lien **TCP**, la boîte de dialogue **Sélection du protocole** s'ouvre.

#### 7.2.2.4.5.2 *Création d'une règle d'applications depuis une stratégie de pare-feu*

**Remarque:** si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - pare-feu** pour configurer une stratégie de pare-feu. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Vous pouvez créer une règle d'applications directement depuis une stratégie de pare-feu à l'aide des pages de configuration de la stratégie de pare-feu avancée.

Pour créer une règle d'applications depuis une stratégie de pare-feu :

1. Cliquez deux fois sur la stratégie que vous désirez modifier.
2. Sur la page de bienvenue de l'assistant **Stratégie de pare-feu**, cliquez sur le bouton **Stratégie de pare-feu avancée**.
3. Dans la boîte de dialogue **Stratégie de pare-feu** qui apparaît, cliquez sur le bouton **Configurer** situé à côté de l'emplacement pour lequel vous souhaitez configurer le pare-feu.
4. Procédez de l'une des manières suivantes :
  - Si vous souhaitez ajouter une application à la stratégie de pare-feu, dans la boîte de dialogue qui apparaît, allez dans l'onglet **Applications** et cliquez sur **Ajouter**.
  - Si vous souhaitez autoriser une application à lancer des processus cachés, allez dans l'onglet **Processus** et cliquez sur **Ajouter** dans la zone supérieure.
  - Si vous souhaitez autoriser une application à accéder au réseau à l'aide de rawsockets, allez dans l'onglet **Processus** et cliquez sur **Ajouter** dans la zone inférieure.

La boîte de dialogue **Stratégie de pare-feu - Ajouter une application** apparaît.

5. Si vous ajoutez une application, dans la boîte **Type d'événements**, vous pouvez choisir d'ajouter une application modifiée, une nouvelle application ou une application pour laquelle aucune règle d'applications n'est définie dans la stratégie de pare-feu.

6. Sélectionnez une entrée pour l'application que vous souhaitez ajouter ou autoriser à lancer des processus cachés ou à utiliser des rawsockets et cliquez sur **OK**.

L'application est ajoutée à la stratégie de pare-feu.

Si vous avez ajouté une application sur l'onglet **Applications**, celle-ci est ajoutée comme fiable. Si vous le souhaitez, vous pouvez la bloquer ou lui créer une règle personnalisée.

#### 7.2.2.4.5.3 Modification d'une règle d'applications

**Remarque :** si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - pare-feu** pour configurer une stratégie de pare-feu. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

1. Cliquez deux fois sur la stratégie de pare-feu que vous désirez modifier.
2. Sur la page **Bienvenue** de l'assistant **Stratégie de pare-feu**, cliquez sur **Stratégie de pare-feu avancée**.
3. Sous **Configurations**, cliquez sur **Configurer** près de l'emplacement pour lequel vous voulez configurer le pare-feu.
4. Cliquez sur l'onglet **Applications**
5. Sélectionnez l'application dans la liste et cliquez sur la flèche près du bouton **Personnaliser**.
6. Dans la boîte de dialogue **Règles d'applications**, cliquez sur **Modifier**.
7. Sous **Nom de la règle**, saisissez un nom pour la règle.  
Le nom de la règle doit être unique dans la liste des règles. Deux règles d'applications ne peuvent pas avoir le même nom, en revanche, deux applications peuvent chacune avoir une règle portant le même nom.
8. Sous **Sélectionner les événements que la règle traitera**, sélectionnez les conditions auxquelles la connexion doit correspondre pour que la règle s'applique.
9. Sous **Sélectionner les actions avec lesquelles la règle répondra**, sélectionnez soit **Autoriser** soit **Bloquer**.
10. Pour autoriser les réponses depuis l'ordinateur distant qui seront basées sur la connexion initiale, sélectionnez **Inspection dynamique**.
11. Sous **Description de la règle**, cliquez sur une valeur soulignée. Par exemple, si vous cliquez sur le lien **TCP**, la boîte de dialogue **Sélection du protocole** s'ouvre.

#### 7.2.2.4.5.4 Application de règles d'applications prédéterminées

**Remarque :** si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - pare-feu** pour configurer une stratégie de pare-feu. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Une prédétermination est une série de règles d'applications créées par Sophos. Pour ajouter des règles prédéterminées à la liste des règles pour une application :

1. Cliquez deux fois sur la stratégie de pare-feu que vous désirez modifier.
2. Sur la page **Bienvenue** de l'assistant **Stratégie de pare-feu**, cliquez sur **Stratégie de pare-feu avancée**.

3. Sous **Configurations**, cliquez sur **Configurer** près de l'emplacement pour lequel vous voulez configurer le pare-feu.
4. Cliquez sur l'onglet **Applications**
5. Sélectionnez l'application dans la liste et cliquez sur la flèche près du bouton **Personnaliser**.
6. Pointez votre curseur sur **Ajouter des règles prédéterminées** et cliquez sur une prédétermination.

#### 7.2.2.4.5.5 Copie d'une règle d'applications

**Remarque :** si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - pare-feu** pour configurer une stratégie de pare-feu. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Pour copier une règle d'applications et l'ajouter à la liste des règles :

1. Cliquez deux fois sur la stratégie de pare-feu que vous désirez modifier.
2. Sur la page **Bienvenue** de l'assistant **Stratégie de pare-feu**, cliquez sur **Stratégie de pare-feu avancée**.
3. Sous **Configurations**, cliquez sur **Configurer** près de l'emplacement pour lequel vous voulez configurer le pare-feu.
4. Cliquez sur l'onglet **Applications**
5. Sélectionnez l'application dans la liste et cliquez sur la flèche près du bouton **Personnaliser**.
6. Dans la boîte de dialogue **Règles d'applications**, cliquez sur **Copier**.

#### 7.2.2.4.5.6 Suppression d'une règle d'applications

**Remarque :** si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - pare-feu** pour configurer une stratégie de pare-feu. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

1. Cliquez deux fois sur la stratégie de pare-feu que vous désirez modifier.
2. Sur la page **Bienvenue** de l'assistant **Stratégie de pare-feu**, cliquez sur **Stratégie de pare-feu avancée**.
3. Sous **Configurations**, cliquez sur **Configurer** près de l'emplacement pour lequel vous voulez configurer le pare-feu.
4. Cliquez sur l'onglet **Applications**
5. Sélectionnez l'application dans la liste et cliquez sur la flèche près du bouton **Personnaliser**.
6. Dans la boîte de dialogue **Règles d'applications**, cliquez sur **Supprimer**.

#### 7.2.2.4.5.7 Modification de l'ordre dans lequel les règles d'applications sont appliquées

**Remarque :** si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - pare-feu** pour configurer une stratégie de pare-feu. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Les règles d'applications sont appliquées dans l'ordre dans lequel elles apparaissent en partant du haut de la liste.

Pour modifier l'ordre dans lequel les règles d'applications sont appliquées :

1. Cliquez deux fois sur la stratégie de pare-feu que vous désirez modifier.
2. Sur la page **Bienvenue** de l'assistant **Stratégie de pare-feu**, cliquez sur **Stratégie de pare-feu avancée**.
3. Sous **Configurations**, cliquez sur **Configurer** près de l'emplacement pour lequel vous voulez configurer le pare-feu.
4. Cliquez sur l'onglet **Applications**
5. Sélectionnez l'application dans la liste et cliquez sur la flèche près du bouton **Personnaliser**.
6. Dans la liste **Règle**, cliquez sur la règle que vous souhaitez faire monter ou descendre dans la liste.
7. Cliquez sur **Monter** ou **Descendre**.

### 7.2.2.5 Connexion intuitive selon l'emplacement

#### 7.2.2.5.1 À propos de la connexion intuitive selon l'emplacement

La connexion intuitive selon l'emplacement est une fonction de Sophos Client Firewall qui attribue une configuration de pare-feu à chaque adaptateur réseau sur votre ordinateur selon l'emplacement où se trouvent les adaptateurs réseau de l'ordinateur.

Cette fonction est généralement utilisée lorsque un employé travaille depuis son domicile sur un ordinateur portable professionnel. Il utilise deux connexions réseau en même temps :

- Pour son usage professionnel, il se connecte au réseau de l'entreprise par le biais d'un client VPN et d'un **adaptateur réseau virtuel**.
- Pour son usage privé, il se connecte à son fournisseur de services par le biais d'un câble réseau et d'un **adaptateur réseau physique**.

Dans ce cas de figure, la configuration professionnelle doit être appliquée à la connexion professionnelle virtuelle tandis que la configuration privée, généralement plus limitée, doit être appliquée à la connexion du fournisseur de services privé.

**Remarque :** la configuration privée nécessite l'instauration de certaines règles afin de permettre d'établir la connexion professionnelle "virtuelle".

#### 7.2.2.5.2 À propos de la configuration de la connexion intuitive selon l'emplacement

1. Définissez la liste des adresses MAC de la passerelle ou les noms de domaine de vos emplacements principaux. Généralement, il s'agit de vos réseaux professionnels.
2. Créez la configuration du pare-feu à utiliser pour vos emplacements principaux. Généralement, cette configuration est moins restrictive.
3. Créez une configuration de pare-feu secondaire. Généralement, cette configuration est plus restrictive.
4. Choisissez une configuration à appliquer.

Selon la méthode de détection que vous utilisez, le pare-feu récupère l'adresse DNS ou de la passerelle des adaptateurs réseau pour chacun de vos ordinateurs et la compare à votre liste d'adresses.

- Si une adresse de votre liste correspond à l'adresse d'un adaptateur réseau, l'adaptateur est affecté à la configuration de l'**emplacement principal**.
- Si aucune des adresses de votre liste ne correspond à l'adresse d'un adaptateur réseau, l'adaptateur est affecté à la stratégie de l'**emplacement secondaire**.

**Important :** la configuration secondaire passe du mode **Interactif** au mode **Bloquer par défaut** sur un ordinateur lorsque les deux conditions suivantes sont rencontrées :

- Les deux emplacements sont actifs.
- La configuration principale n'est *pas* interactive.

### 7.2.2.5.3 Définition des emplacements principaux

1. Cliquez deux fois sur la stratégie de pare-feu que vous désirez modifier.
2. Sur la page **Bienvenue** de l'assistant **Stratégie de pare-feu**, cliquez sur **Stratégie de pare-feu avancée**.
3. Sous **Configurations**, cliquez sur **Configurer** près de l'emplacement pour lequel vous voulez configurer le pare-feu.
4. Cliquez sur l'onglet **Détection de l'emplacement**.
5. Sous **Méthode de détection**, cliquez sur le bouton **Configurer** correspondant à la méthode que vous souhaitez utiliser pour définir vos emplacements principaux :

Option	Description
<b>Recherche DNS</b>	Vous créez une liste de noms de domaine et d'adresses IP attendues qui correspondent à vos emplacements principaux.
<b>Détection d'adresses MAC</b>	Vous créez une liste d'adresses MAC de la passerelle qui correspondent à vos emplacements principaux.

6. Suivez les instructions à l'écran.

### 7.2.2.5.4 Création d'une configuration secondaire

1. Cliquez deux fois sur la stratégie de pare-feu que vous désirez modifier.
2. Sur la page **Bienvenue** de l'assistant **Stratégie de pare-feu**, cliquez sur **Stratégie de pare-feu avancée**.
3. Sous **Configurations**, cliquez sur **Configurer** près de l'emplacement pour lequel vous voulez configurer le pare-feu.
4. Sélectionnez la case à cocher **Ajout d'une configuration pour un second emplacement**.

Paramétrez maintenant votre configuration secondaire. Pour plus d'informations sur la manière de procéder, reportez-vous à la section *Configuration du pare-feu*.



**Avvertissement :** nous vous conseillons d'être extrêmement vigilants lors de l'utilisation des règles du réseau local comme configurations secondaires. S'il s'agit d'un ordinateur portable utilisé en dehors du bureau, il peut se connecter à un réseau local inconnu. Dans ce cas, il est

possible que les règles de pare-feu de la configuration secondaire qui utilisent le réseau local comme adresse autorisent le trafic inconnu.

#### 7.2.2.5.5 Sélection de la configuration à appliquer

1. Cliquez deux fois sur la stratégie de pare-feu que vous désirez modifier.
2. Sur la page **Bienvenue** de l'assistant **Stratégie de pare-feu**, cliquez sur **Stratégie de pare-feu avancée**.
3. Sous **Configurations**, cliquez sur **Configurer** près de l'emplacement pour lequel vous voulez configurer le pare-feu.
4. Dans l'onglet **Général**, sous **Emplacement appliqué**, cliquez sur l'une des options suivantes :

Option	Description
Appliquer la configuration pour l'emplacement détecté	Le pare-feu applique soit la configuration principale, soit la configuration secondaire à chaque connexion réseau selon les paramètres de détection de la connexion intuitive selon l'emplacement (comme le décrit la section <a href="#">À propos de la configuration de la connexion intuitive selon l'emplacement</a> à la page 106).
Appliquer la configuration pour l'emplacement principal	Le pare-feu applique la configuration principale à toutes les connexions réseau.
Appliquer la configuration pour l'emplacement secondaire	Le pare-feu applique la configuration secondaire à toutes les connexions réseau.

#### 7.2.2.6 Signalement du pare-feu

##### 7.2.2.6.1 À propos des rapports du pare-feu

Par défaut, le pare-feu sur un ordinateur d'extrémité signale les changements d'état, les événements et les erreurs à Enterprise Manager.

##### Modifications d'état du pare-feu

Le pare-feu signale les modifications d'état suivantes :

- Modifications du mode de fonctionnement
- Modifications de la version du logiciel
- Modifications de la configuration du pare-feu pour autoriser tout le trafic
- Modifications du pare-feu pour qu'il soit conforme à la stratégie

Lorsque vous travaillez en mode interactif, la configuration de votre pare-feu peut volontairement différer de la stratégie appliquée par Enterprise Manager. Dans ce cas, vous pouvez décider de ne **pas** envoyer d'alertes "Diffère de la stratégie" à Enterprise Manager lorsque vous modifiez certaines parties de la configuration de votre pare-feu.

Pour plus d'informations, reportez-vous à la section [Activation ou désactivation du signalement des modifications locales](#) à la page 109.

##### Événements du pare-feu

Un *événement* est lorsque le système d'exploitation de l'ordinateur d'extrémité ou une application connue sur l'ordinateur d'extrémité tente de communiquer avec un autre ordinateur via une connexion réseau.

Vous pouvez empêcher le pare-feu de signaler les événements à Enterprise Manager.

Pour plus d'informations, reportez-vous à la section [Désactivation du signalement du trafic réseau inconnu](#) à la page 109

#### 7.2.2.6.2 Activation ou désactivation du signalement des modifications locales

**Remarque :** si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - pare-feu** pour configurer une stratégie de pare-feu. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Si la configuration du pare-feu sur les postes d'extrémité diffère de la stratégie, vous pouvez **désactiver le signalement des modifications locales**.

La désactivation du signalement des modifications locales empêche le pare-feu d'envoyer des alertes "diffère de la stratégie" à Enterprise Manager concernant les modifications apportées aux règles globales, aux applications, aux processus ou aux sommes de contrôle. Vous pouvez, si vous le souhaitez, exécuter cette opération, par exemple, lorsque les ordinateurs d'extrémité sont en mode interactif, car il s'agit de paramètres qui peuvent être changés à l'aide des boîtes de dialogue d'apprentissage.

Si la configuration du pare-feu sur les ordinateurs d'extrémité est prévue pour être conforme à la stratégie, **activez le signalement des modifications locales**.

Pour désactiver le signalement des modifications locales :

1. Cliquez deux fois sur la stratégie de pare-feu que vous désirez modifier.
2. Sur la page **Bienvenue** de l'assistant **Stratégie de pare-feu**, cliquez sur **Stratégie de pare-feu avancée**.
3. Sous **Configurations**, cliquez sur **Configurer** près de l'emplacement pour lequel vous voulez configurer le pare-feu.
4. Cliquez sur l'onglet **Général**.
5. Sous **Signalement**, procédez de l'une des manières suivantes :
  - Pour activer le signalement des modifications locales, sélectionnez la case à cocher **Afficher une alerte sur la console d'administration en cas de modifications locales de règles globales, d'applications, de processus ou de sommes de contrôle**.
  - Pour désactiver le signalement des modifications locales, dessélectionnez la case à cocher **Afficher une alerte sur la console d'administration en cas de modifications locales de règles globales, d'applications, de processus ou de sommes de contrôle**.

#### 7.2.2.6.3 Désactivation du signalement du trafic réseau inconnu

**Remarque :** si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - pare-feu** pour configurer une stratégie de pare-feu. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Vous pouvez empêcher le pare-feu sur les ordinateurs d'extrémité de signaler le trafic réseau inconnu à Enterprise Manager. Le pare-feu considère le trafic comme inconnu s'il n'a pas de règle.

Pour empêcher le pare-feu sur les ordinateurs d'extrémité de signaler le trafic réseau inconnu à Enterprise Manager :

1. Cliquez deux fois sur la stratégie de pare-feu que vous désirez modifier.
2. Sur la page **Bienvenue** de l'assistant **Stratégie de pare-feu**, cliquez sur **Stratégie de pare-feu avancée**.
3. Sous **Configurations**, cliquez sur **Configurer** près de l'emplacement pour lequel vous voulez configurer le pare-feu.
4. Cliquez sur l'onglet **Général**.
5. Sous **Blocage**, sélectionnez la case **Utiliser les sommes de contrôle pour authentifier les applications**.
6. Sous **Signalement**, désélectionnez la case à cocher **Signaler les applications et le trafic inconnus à la console d'administration**.

#### 7.2.2.6.4 Désactivation du signalement des erreurs de pare-feu

**Important :** nous vous déconseillons de désactiver en permanence le signalement des erreurs de pare-feu. Désactivez le signalement seulement si vous avez besoin.

Pour empêcher le pare-feu sur les ordinateurs d'extrémité de signaler les erreurs à Enterprise Manager :

1. Cliquez deux fois sur la stratégie de pare-feu que vous désirez modifier.
2. Sur la page **Bienvenue** de l'assistant **Stratégie de pare-feu**, cliquez sur **Stratégie de pare-feu avancée**.
3. Sous **Configurations**, cliquez sur **Configurer** près de l'emplacement pour lequel vous voulez configurer le pare-feu.
4. Cliquez sur l'onglet **Général**.
5. Sous **Signalement**, désélectionnez la case à cocher **Signaler les erreurs à la console d'administration**.

#### 7.2.2.7 Importation ou exportation de la configuration du pare-feu

**Remarque :** si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - pare-feu** pour configurer une stratégie de pare-feu. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Vous pouvez importer ou exporter les paramètres généraux ainsi que les règles du pare-feu sous un fichier de configuration (\*.conf). Vous pouvez utiliser cette fonction pour effectuer les opérations suivantes :

- Sauvegarder et restaurer la configuration de votre pare-feu.
- Importer les règles d'application créées sur un ordinateur et les utiliser pour créer une stratégie pour d'autres ordinateurs exécutant la même série d'applications.
- Fusionner les configurations créés sur plusieurs ordinateurs différents pour créer une stratégie valide pour un ou plusieurs groupes d'ordinateurs sur le réseau.

Pour importer ou exporter la configuration du pare-feu :

1. Vérifiez quelle stratégie de pare-feu est utilisée par le ou les groupes d'ordinateurs que vous désirez configurer.  
Reportez-vous à la section [Vérification des stratégies utilisées par un groupe](#) à la page 23.
2. Dans le volet **Stratégies**, cliquez deux fois sur **Pare-feu** puis cliquez deux fois sur la stratégie que vous souhaitez importer ou exporter.
3. Sur la page de **Bienvenue** de l'assistant **Stratégie de pare-feu**, cliquez sur **Stratégie de pare-feu avancée**.
4. Dans la boîte de dialogue **Stratégie de pare-feu**, sur l'onglet **Général**, sous **Gestion de la configuration**, cliquez sur **Importer** ou sur **Exporter**.

## 7.3 Configuration de la stratégie de contrôle des périphériques

### 7.3.1 À propos du contrôle des périphériques

**Important :** le contrôle des périphériques Sophos ne doit pas être déployé en parallèle à des logiciels de contrôle des périphériques d'autres éditeurs.

Le contrôle des périphériques vous permet d'empêcher les utilisateurs d'utiliser sur leurs ordinateurs des périphériques de stockage externes, des supports de stockage amovibles et des technologies de connexion sans fil non autorisés. Ceci réduit considérablement votre exposition aux pertes accidentelles de données et limite les possibilités pour les utilisateurs d'introduire des logiciels n'appartenant pas à votre environnement réseau.

Les périphériques de stockage amovibles, les unités de disque optiques et les lecteurs de disquettes peuvent également être paramétrés pour fournir un accès en lecture seule.

Grâce au contrôle des périphériques, vous réduisez aussi considérablement les risques de création de ponts entre un réseau professionnel et un réseau non professionnel. Le mode **Bloquer le pont** est disponible pour les types de périphériques à la fois sans fil et modem. Ce mode fonctionne en désactivant les adaptateurs réseau sans fil ou modem lorsqu'un ordinateur d'extrémité est connecté à un réseau physique (généralement, via une connexion Ethernet). Une fois l'ordinateur déconnecté du réseau physique, les adaptateurs réseau sans fil ou modem sont réactivés de manière transparente.

Par défaut, le contrôle des périphériques est désactivé et tous les périphériques sont autorisés.

Si vous voulez activer le contrôle des périphériques pour la première fois, nous vous conseillons de :

- Sélectionner les types de périphériques à contrôler.
- Détecter les périphériques sans les bloquer.
- Utiliser les événements de contrôle des périphériques pour décider quels types de périphériques bloquer et, le cas échéant, lesquels doivent être exemptés.
- Détecter et bloquer ou autoriser l'accès en lecture seule aux périphériques de stockage.

Pour plus d'informations sur les paramètres conseillés pour le contrôle des périphériques, reportez-vous au *Guide de configuration des stratégies de Sophos Enterprise Manager* .

**Remarque :** si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - contrôle des périphériques** pour configurer une stratégie de contrôle des périphériques. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

### 7.3.2 À propos des événements du contrôle des périphériques

Lorsqu'un événement de contrôle des périphériques se produit, par exemple, un périphérique de stockage amovible a été bloqué, l'événement est envoyé à Enterprise Manager et est visible dans la boîte de dialogue **Contrôle des périphériques - Observateur d'événements**.

Dans la boîte de dialogue **Contrôle des périphériques - Observateur d'événements**, vous pouvez utiliser des filtres pour n'afficher que les événements qui vous intéressent. Vous pouvez aussi exporter dans un fichier la liste des événements du contrôle des périphériques. Pour plus de détails, reportez-vous aux sections [Affichage des événements du contrôle des périphériques](#) à la page 127 et [Exportation dans un fichier de la liste des événements](#) à la page 130.

Vous pouvez utiliser les événements de contrôle des périphériques pour ajouter des exemptions pour des périphériques spécifiques ou des modèles de périphériques aux stratégies de contrôle des périphériques. Pour plus d'informations sur l'exemption de périphériques, reportez-vous aux sections [Exemption d'un périphérique d'une seule stratégie](#) à la page 116 ou [Exemption d'un périphérique de toutes les stratégies](#) à la page 115.

Le nombre d'ordinateurs avec des événements de contrôle des périphériques au-dessus d'un seuil spécifié dans les sept derniers jours apparaît sur le Tableau de bord. Pour plus d'informations sur la manière de configurer le seuil, reportez-vous à la section [Configuration du Tableau de bord](#) à la page 36.

Vous pouvez aussi configurer l'envoi des alertes par courriel aux destinataires de votre choix lorsqu'un événement de contrôle des périphériques s'est produit. Pour plus de détails, reportez-vous à la section [Configuration des alertes et des messages du contrôle des périphériques](#) à la page 124.

### 7.3.3 Quels types de périphériques peuvent être contrôlés ?

Le contrôle des périphériques vous permet de bloquer trois types de périphériques : *stockage*, *réseau* et *courte portée*.

#### **Stockage**

- Périphériques de stockage amovible (par exemple, les clés USB à mémoire flash, les lecteurs de cartes PC et les lecteurs de disques durs externes)
- Lecteurs de supports optiques (lecteurs de CD-ROM/DVD/Blu-ray)
- Lecteurs de disquette
- Périphériques de stockage amovibles sécurisés (clés USB à mémoire flash SanDisk Cruzer Enterprise, SanDisk Cruzer Enterprise FIPS Edition, Kingston Data Traveler Vault - Privacy Edition, Kingston Data Traveler BlackBox et IronKey Enterprise Basic Edition avec chiffrement matériel)

A l'aide de la catégorie de stockage amovible sécurisé, vous pouvez facilement autoriser l'utilisation de périphériques de stockage amovibles sécurisés pris en charge tout en bloquant d'autres. Pour avoir une liste à jour des périphériques de stockage amovibles sécurisés pris en charge, consultez l'article 63102 de la base de connaissances du support de Sophos (<http://www.sophos.fr/support/knowledgebase/article/63102.html>).

## Réseau

- Modems
- Sans fil (interfaces Wi-Fi, norme 802.11)

Pour les interfaces réseau, vous pouvez aussi sélectionner le mode **Bloquer le pont** qui aide à réduire considérablement tout risque de création de ponts réseaux, par exemple entre un réseau professionnel et un réseau non professionnel. Ce mode fonctionne en désactivant les adaptateurs réseau sans fil ou modem lorsqu'un ordinateur d'extrémité est connecté à un réseau physique (généralement, via une connexion Ethernet). Une fois l'ordinateur déconnecté du réseau physique, les adaptateurs réseau sans fil ou modem sont réactivés de manière transparente.

## Courte portée

- Interfaces Bluetooth
- Infrarouge (interfaces infrarouge IrDA)

Le contrôle des périphériques bloque à la fois les périphériques et les interfaces internes et externes. Par exemple, une stratégie bloquant les interfaces Bluetooth bloquera :

- L'interface Bluetooth incorporée dans un ordinateur
- Tous les adaptateurs Bluetooth de type USB connectés à l'ordinateur

### 7.3.4 Sélection des types de périphériques à contrôler

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - contrôle des périphériques** pour modifier une stratégie de contrôle des périphériques. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

**Important :** ne bloquez pas les connexions Wi-Fi sur les ordinateurs qui sont administrés par Enterprise Manager via Wi-Fi.

1. Vérifiez quelle stratégie de contrôle des applications est utilisée par le ou les groupes d'ordinateurs que vous souhaitez configurer.  
Reportez-vous à la section [Vérification des stratégies utilisées par un groupe](#) à la page 23.
2. Dans le volet **Stratégies**, cliquez deux fois sur **Contrôle des données**. Puis cliquez deux fois sur la stratégie que vous désirez changer.
3. Dans la boîte de dialogue **Stratégie de contrôle des périphériques**, sur l'onglet **Configuration**, sous **Stockage**, sélectionnez le type de périphérique de stockage que vous voulez contrôler.

4. Cliquez dans la colonne **État** près du type de périphérique, puis cliquez sur la flèche du menu déroulant qui apparaît. Sélectionnez le type d'accès que vous voulez autoriser.  
Par défaut, les périphériques ont un accès complet. Pour les périphériques de stockage amovibles, les unités de disque optiques et les lecteurs de disquettes, vous pouvez changer en "Bloquées" ou en "Lecture seule". Pour les périphériques de stockage amovibles sécurisés, vous pouvez changer en "Bloqué".
5. Sous **Réseau**, sélectionnez le type de périphérique réseau que vous voulez bloquer.
6. Cliquez dans la colonne **État** près du type de périphérique réseau, puis cliquez sur la flèche du menu déroulant qui apparaît.
  - Sélectionnez "Bloqué" si vous voulez bloquer le type de périphérique.
  - Sélectionnez "Bloquer le pont" si vous voulez empêcher la création d'un pont entre un réseau professionnel et un réseau non professionnel. Le type de périphérique sera bloqué lorsqu'un ordinateur d'extrémité sera connecté à un réseau physique (généralement via une connexion Ethernet). Une fois que l'ordinateur d'extrémité est déconnecté du réseau physique, le type de périphérique sera réactivé.
7. Sous **Courte portée**, sélectionnez le type de périphérique de courte portée que vous voulez bloquer. Dans la colonne **État** près du type de périphérique, sélectionnez "Bloqué".  
Cliquez sur **OK**.

### 7.3.5 Détection des périphériques sans les bloquer

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - contrôle des périphériques** pour modifier une stratégie de contrôle des périphériques. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Vous pouvez détecter des périphériques sans les bloquer. Ceci est utile si vous avez l'intention de bloquer des périphériques à l'avenir, mais voulez d'abord détecter et exempter les périphériques dont vous avez besoin.

Pour détecter les périphériques sans les bloquer, activez le contrôle des périphériques dans une stratégie de contrôle des périphériques et activez le mode *détection seulement*. Changez le statut des périphériques que vous voulez détecter en "Bloqué". Ceci générera des événements pour les périphériques utilisés sur les ordinateurs d'extrémité si la stratégie est enfreinte, mais les périphériques ne seront pas bloqués.

Pour plus d'informations sur la consultation des événements de contrôle des périphériques, reportez-vous à la section [Affichage des événements du contrôle des périphériques](#) à la page 127.

Pour détecter des périphériques sans les bloquer :

1. Vérifiez quelle stratégie de contrôle des applications est utilisée par le ou les groupes d'ordinateurs que vous souhaitez configurer.  
Reportez-vous à la section [Vérification des stratégies utilisées par un groupe](#) à la page 23.
2. Dans le volet **Stratégies**, cliquez deux fois sur **Contrôle des données**. Puis cliquez deux fois sur la stratégie que vous désirez changer.
3. Dans la boîte de dialogue **Stratégie de contrôle des périphériques**, sur l'onglet **Configuration**, sélectionnez **Activer le contrôle des périphériques**.

4. Sélectionnez **Détecter mais ne pas bloquer les périphériques**.
5. Si vous ne l'avez pas encore fait, changez le statut des périphériques que vous voulez détecter en “Bloqué” (pour plus de détails, reportez-vous à la section [Sélection des types de périphériques à contrôler](#) à la page 113).  
Cliquez sur **OK**.

### 7.3.6 Détection et blocage des périphériques

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - contrôle des périphériques** pour modifier une stratégie de contrôle des périphériques. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

1. Vérifiez quelle stratégie de contrôle des applications est utilisée par le ou les groupes d'ordinateurs que vous souhaitez configurer.  
Reportez-vous à la section [Vérification des stratégies utilisées par un groupe](#) à la page 23.
2. Dans le volet **Stratégies**, cliquez deux fois sur **Contrôle des données**. Puis cliquez deux fois sur la stratégie que vous désirez changer.
3. Dans la boîte de dialogue **Stratégie de contrôle des périphériques**, sur l'onglet **Configuration**, sélectionnez la case à cocher **Activer le contrôle des périphériques**.
4. Deselectionnez la case à cocher **Détecter mais ne pas bloquer les périphériques**.
5. Si vous ne l'avez pas encore fait, changez le statut des périphériques que vous voulez bloquer en “Bloqué” (pour plus de détails, reportez-vous à la section [Sélection des types de périphériques à contrôler](#) à la page 113).  
Cliquez sur **OK**.

### 7.3.7 Exemption d'un périphérique de toutes les stratégies

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - contrôle des périphériques** pour modifier une stratégie de contrôle des périphériques. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Vous pouvez exempter un périphérique de toutes les stratégies, y compris de celle par défaut. Cette exception sera alors ajoutée à toutes les stratégies que vous créez.

Vous pouvez exempter une instance (“ce périphérique uniquement”) ou un modèle (“tous les périphériques de ce modèle”) de périphérique. Ne paramétrez pas d'exemptions à la fois au niveau du modèle et de l'instance du périphérique. Si les deux sont définis, le niveau de l'instance du périphérique aura priorité.

Pour exempter un périphérique de toutes les stratégies de contrôle des périphériques :

1. Dans le menu **Affichage**, cliquez sur **Événements du contrôle des périphériques**.  
La boîte de dialogue **Contrôle des périphériques - Observateur d'événements** apparaît.

2. Si vous voulez afficher certains événements seulement, dans le volet **Critères de recherche**, définissez les filtres de façon appropriée et cliquez sur **Rechercher** pour afficher les événements.

Pour plus d'informations, reportez-vous à la section [Affichage des événements du contrôle des périphériques](#) à la page 127.

3. Sélectionnez l'entrée du périphérique que vous voulez exempter des stratégies, puis cliquez sur **Exempter un périphérique**.

La boîte de dialogue **Exemption d'un périphérique** apparaît. Sous **Détails du périphérique**, le type, le modèle et l'identification du périphérique apparaissent. Sous **Détails de l'exemption, Etendue**, les mots "Toutes les stratégies" apparaissent.

**Remarque :** s'il n'y a aucun événement pour le périphérique que vous voulez exempter, par exemple, un lecteur de CD-ROM ou de DVD sur un ordinateur d'extrémité, allez sur l'ordinateur contenant le périphérique et activez ce dernier dans le Gestionnaire de périphériques (pour y accéder, cliquez avec le bouton droit de la souris sur **Poste de travail**, cliquez sur **Gérer**, puis cliquez sur **Gestionnaire de périphériques**). Ceci génère un nouvel événement "blocage" qui apparaîtra dans la boîte de dialogue **Contrôle des périphériques - Observateur d'événements**. Vous pouvez ensuite exempter le périphérique comme le décrit plus haut cette étape.

4. Indiquez si vous voulez exempter ce périphérique seulement ou tous les périphériques de ce modèle.
5. Indiquez si vous voulez autoriser un accès complet ou un accès en lecture seule au périphérique.
6. Dans le champ **Commentaire**, saisissez si vous le souhaitez un commentaire. Par exemple, vous pouvez spécifier qui a fait la demande d'exemption du périphérique.
7. Cliquez sur **OK**.

### 7.3.8 Exemption d'un périphérique d'une seule stratégie

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - contrôle des périphériques** pour modifier une stratégie de contrôle des périphériques. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Vous pouvez exempter un périphérique donné d'une stratégie de contrôle des périphériques.

Vous pouvez exempter une instance ("ce périphérique uniquement") ou un modèle ("tous les périphériques de ce modèle") de périphérique. Ne paramétrez pas d'exemptions à la fois au niveau du modèle et de l'instance du périphérique. Si les deux sont définis, le niveau de l'instance du périphérique aura priorité.

Pour exempter un périphérique d'une stratégie :

1. Vérifiez quelle stratégie de contrôle des applications est utilisée par le ou les groupes d'ordinateurs que vous souhaitez configurer.

Reportez-vous à la section [Vérification des stratégies utilisées par un groupe](#) à la page 23.

2. Dans le volet **Stratégies**, cliquez deux fois sur **Contrôle des données**. Puis cliquez deux fois sur la stratégie que vous désirez changer.

3. Dans la boîte de dialogue **Stratégie de contrôle des périphériques**, sur l'onglet **Configuration**, sélectionnez **Ajouter exemption**.

La boîte de dialogue **Contrôle des périphériques - Observateur d'événements** apparaît.

4. Si vous voulez afficher certains événements seulement, dans le volet **Critères de recherche**, définissez les filtres de façon appropriée et cliquez sur **Rechercher** pour afficher les événements.

Pour plus d'informations, reportez-vous à la section [Affichage des événements du contrôle des périphériques](#) à la page 127.

5. Sélectionnez l'entrée du périphérique que vous voulez exempter de la stratégie, puis cliquez sur **Exempter un périphérique**.

La boîte de dialogue **Exemption d'un périphérique** apparaît. Sous **Détails du périphérique**, le type, le modèle et l'identification du périphérique apparaissent. Sous **Détails de l'exemption, Etendue**, les mots "Cette stratégie seulement" apparaissent.

**Remarque :** s'il n'y a aucun événement pour le périphérique que vous voulez exempter, par exemple, un lecteur de CD-ROM ou de DVD sur un ordinateur d'extrémité, allez sur l'ordinateur contenant le périphérique et activez ce dernier dans le Gestionnaire de périphériques (pour y accéder, cliquez avec le bouton droit de la souris sur **Poste de travail**, cliquez sur **Gérer**, puis cliquez sur **Gestionnaire de périphériques**). Ceci génère un nouvel événement "blocage" qui apparaîtra dans la boîte de dialogue **Contrôle des périphériques - Observateur d'événements**. Vous pouvez ensuite exempter le périphérique comme le décrit plus haut cette étape.

6. Indiquez si vous voulez exempter ce périphérique seulement ou tous les périphériques de ce modèle.
7. Indiquez si vous voulez autoriser un accès complet ou un accès en lecture seule au périphérique.
8. Dans le champ **Commentaire**, saisissez si vous le souhaitez un commentaire. Par exemple, vous pouvez spécifier qui a fait la demande d'exemption du périphérique.
9. Cliquez sur **OK**.

### 7.3.9 Affichage ou modification de la liste de périphériques exemptés

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - contrôle des périphériques** pour modifier une stratégie de contrôle des périphériques. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Pour voir ou modifier la liste de périphériques exemptés :

1. Vérifiez quelle stratégie de contrôle des applications est utilisée par le ou les groupes d'ordinateurs que vous souhaitez configurer.  
Reportez-vous à la section [Vérification des stratégies utilisées par un groupe](#) à la page 23.
2. Dans le volet **Stratégies**, cliquez deux fois sur **Contrôle des données**. Puis cliquez deux fois sur la stratégie que vous désirez changer.

3. Dans la boîte de dialogue **Stratégie de contrôle des périphériques**, sur l'onglet **Configuration**, sélectionnez le type de périphérique pour lequel vous voulez visualiser les exemptions, par exemple, le lecteur optique. Cliquez sur **Voir les exemptions**.

La boîte de dialogue **Exemptions de <Type de périphérique>** apparaît. Si une exemption concerne tous les périphériques de ce modèle, le champ **ID périphérique** est vierge.

4. Si vous voulez modifier la liste des périphériques exemptés, effectuez l'une des opérations suivantes :
  - Si vous voulez ajouter une exemption, cliquez sur **Ajouter**. Pour plus d'informations, reportez-vous à la section [Exemption d'un périphérique d'une seule stratégie](#) à la page 116.
  - Si vous voulez modifier une exemption, sélectionnez-la et cliquez sur **Modifier**. Modifiez les paramètres dans la boîte de dialogue **Exemption d'un périphérique** comme vous le souhaitez.
  - Si vous voulez supprimer une exemption, sélectionnez le périphérique exempté et cliquez sur **Supprimer**.

Ceci le supprime de la stratégie que vous modifiez. Si vous voulez supprimer le périphérique d'autres stratégies, répétez les étapes de cette tâche pour chaque stratégie.

## 7.4 Configuration de la stratégie de protection antialtération

### 7.4.1 À propos de la protection antialtération

La protection antialtération vous permet d'interdire aux utilisateurs non autorisés (administrateurs locaux et utilisateurs avec peu d'expérience technique) ainsi qu'aux programmes malveillants de désinstaller les logiciels de sécurité de Sophos ou de les désactiver par le biais de l'interface Sophos Endpoint Security and Control.

**Remarque :** la protection antialtération n'est pas conçue pour assurer la protection contre les utilisateurs expérimentés techniquement. Elle n'assure pas non plus la protection contre les programmes malveillants spécifiquement conçus pour corrompre le système d'exploitation afin d'éviter d'être détecté. Ce type de programmes malveillants est uniquement détecté en effectuant un contrôle à la recherche de menaces et de comportements suspects (pour plus d'informations, reportez-vous à la section [À propos de la stratégie antivirus et HIPS](#) à la page 63).

Après avoir activé la protection antialtération et créé un mot de passe, un membre du groupe SophosAdministrator sur l'ordinateur d'extrémité qui ne connaît pas le mot de passe ne pourra pas :

- Reconfigurer les paramètres du contrôle sur accès ou de la détection des comportements suspects dans Sophos Endpoint Security and Control.
- Désactiver la protection antialtération.
- Désinstaller les composants de Sophos Endpoint Security and Control (Sophos Anti-Virus, Sophos Client Firewall, Sophos AutoUpdate ou Sophos Remote Management System).
- Désinstaller Sophos SafeGuard Disk Encryption.

Si vous voulez permettre aux SophosAdministrators d'exécuter ces tâches, vous devez leur fournir le mot de passe de la protection antialtération afin qu'ils puissent s'authentifier.

La protection antialtération n'affecte pas les membres des groupes SophosUser et SophosPowerUser. Lorsque la protection antialtération est activée, ils peuvent effectuer toutes les tâches qu'ils sont habituellement autorisés à effectuer sans avoir à saisir de mot de passe pour la protection antialtération.

**Remarque:** si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - protection antialtération** pour configurer une stratégie de protection antialtération. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

### Événements de protection antialtération

En cas d'événement de protection antialtération, (lorsque, par exemple, une tentative non autorisée de désinstaller Sophos Anti-Virus depuis un ordinateur d'extrémité a été bloquée), l'événement est consigné dans le journal des événements et peut être consulté depuis Enterprise Manager. Pour plus de détails, reportez-vous à la section [Affichage des événements de protection antialtération](#) à la page 128.

Il y a deux types d'événements de protection antialtération :

- Les événements réussis d'authentification de la protection antialtération affichant le nom de l'utilisateur authentifié et l'heure d'authentification.
- Les tentatives ratées de modifications affichant le nom du produit ou du composant Sophos pris pour cible, l'heure de la tentative et des informations détaillées sur l'utilisateur responsable de cette tentative.

## 7.4.2 Activation ou désactivation de la protection antialtération

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - protection antialtération** pour configurer une stratégie de protection antialtération. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Pour démarrer ou arrêter la protection antialtération :

1. Vérifiez quelle stratégie de protection antialtération est utilisée par le ou les groupes d'ordinateurs que vous souhaitez configurer.  
Reportez-vous à la section [Vérification des stratégies utilisées par un groupe](#) à la page 23.
2. Dans le volet **Stratégies**, cliquez deux fois sur **Protection antialtération**. Puis cliquez deux fois sur la stratégie que vous désirez changer.
3. Dans la boîte de dialogue **Stratégie de protection antialtération**, sélectionnez ou désélectionnez la case **Activer la protection antialtération**.  
Si vous souhaitez activer la protection antialtération pour la première fois, cliquez sur **Définir** sous le champ **Mot de passe**. Dans la boîte de dialogue **Mot de passe de la protection antialtération**, saisissez et confirmez un mot de passe.

**Astuce :** nous vous recommandons d'utiliser un mot de passe contenant au minimum 8 caractères incluant une combinaison de minuscules, de majuscules et de chiffres.

### 7.4.3 Changement du mot de passe de la protection antialtération

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - protection antialtération** pour configurer une stratégie de protection antialtération. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Pour changer le mot de passe de la protection antialtération :

1. Vérifiez quelle stratégie de protection antialtération est utilisée par le ou les groupes d'ordinateurs que vous souhaitez configurer.  
Reportez-vous à la section [Vérification des stratégies utilisées par un groupe](#) à la page 23.
2. Dans le volet **Stratégies**, cliquez deux fois sur **Protection antialtération**. Puis cliquez deux fois sur la stratégie que vous désirez changer.
3. Dans la boîte de dialogue **Stratégie de protection antialtération**, cliquez sur **Changer** sous le champ **Mot de passe**. Dans la boîte de dialogue **Mot de passe de la protection antialtération**, saisissez et confirmez le nouveau mot de passe.

**Astuce :** le mot de passe doit contenir au minimum 8 caractères incluant une combinaison de minuscules, de majuscules et de chiffres.

## 8 Paramétrage des alertes et des messages

### 8.1 À propos des alertes et des messages

Plusieurs méthodes d'alerte sont utilisées dans Enterprise Manager.

#### ■ Alertes affichées dans la console

Si un élément demandant votre attention est trouvé sur un ordinateur ou si une erreur s'est produite, Sophos Endpoint Security and Control envoie une alerte à Enterprise Manager. L'alerte apparaît dans la liste des ordinateurs. Pour plus d'informations sur le traitement de telles alertes, reportez-vous à la section [Traitement des alertes sur les éléments détectés](#) à la page 40.

Ces alertes sont toujours affichées. Il n'est pas nécessaire de les paramétrer.

#### ■ Événements affichés dans la console

Lorsqu'un événement de pare-feu, de contrôle des périphériques ou de protection antialtération se produit sur un système d'extrémité, par exemple, une application a été bloquée par le pare-feu, cet événement est envoyé à Enterprise Manager et est visible dans l'observateur d'événements correspondant.

#### ■ Alertes et messages envoyés par la console aux destinataires de votre choix

Par défaut, lorsqu'un élément est trouvé sur un ordinateur, un message apparaît sur le bureau de l'ordinateur et une entrée est ajoutée dans le journal des événements Windows. Lorsqu'un événement de contrôle des périphériques se produit, un message apparaît sur le bureau de l'ordinateur.

Vous pouvez aussi configurer les alertes par courriel ou les messages SNMP pour les administrateurs.

Cette section décrit comment paramétrer les alertes à envoyer aux destinataires de votre choix.

### 8.2 Configuration des alertes d'abonnement logiciels

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Configuration système** pour réaliser cette tâche. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

L'Enterprise Manager affiche les alertes émises par le gestionnaire de mise à jour dans la colonne **Alertes** de la vue **Gestionnaires de mise à jour**.

Vous pouvez aussi paramétrer l'envoi des alertes par courriel à vos destinataires choisis lorsque la version du produit auquel vous vous êtes abonné est en instance de retrait ou retiré.

1. Dans le menu **Outils**, sélectionnez **Configurer les alertes par courriel**.

La boîte de dialogue **Configuration des alertes par courriel** apparaît.

2. Si les paramètres SMTP n'ont pas été configurés ou si vous voulez visualiser ou changer les paramètres, cliquez sur **Configurer**.

Dans la boîte de dialogue **Configuration des paramètres SMTP**, saisissez les détails comme décrit ci-dessous :

- a) Dans la zone de texte **Adresse du serveur**, saisissez le nom d'hôte ou l'adresse IP du serveur SMTP.
  - b) Dans la zone de texte **Expéditeur**, saisissez une adresse électronique à laquelle les messages renvoyés et les rapports de non-distribution peuvent être envoyés.
  - c) Cliquez sur **Tester** pour tester la connexion.
3. Dans le volet **Destinataires**, cliquez sur **Ajouter**.
- La boîte de dialogue **Ajout d'un nouveau destinataire d'alerte par courriel** apparaît.
4. Dans le champ **Adresse électronique**, saisissez l'adresse de votre destinataire.
  5. Dans le champ **Langue**, sélectionnez la langue dans laquelle vous souhaitez que soient envoyées les alertes par courriel.
  6. Dans le volet **Abonnements**, sélectionnez les "Abonnements logiciels" que vous souhaitez envoyer à ce destinataire. Il y a deux alertes auxquelles vous pouvez vous abonner :
    - Un abonnement logiciels inclut la version d'un produit en instance de retrait à Sophos.
    - Un abonnement logiciels inclut la version d'un produit qui a été retiré à Sophos.

### 8.3 Configuration des alertes par courriel antivirus et HIPS

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - antivirus et HIPS** pour effectuer cette tâche. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

En cas de découverte d'un virus, d'un comportement suspect, d'une application indésirable ou d'une erreur sur un des ordinateurs du groupe, vous pouvez automatiser l'envoi d'alertes par courriel à des utilisateurs donnés.

**Important :** les ordinateurs Mac OS X peuvent envoyer ces alertes à une seule adresse seulement.

1. Dans le volet **Stratégies**, cliquez deux fois sur la stratégie antivirus et HIPS que vous désirez modifier.
2. Dans la boîte de dialogue **Stratégie antivirus et HIPS**, dans le volet **Configurer l'antivirus et HIPS**, cliquez sur **Messagerie**.
3. Dans la boîte de dialogue **Messagerie**, choisissez l'onglet **Alertes par courriel** et sélectionnez **Activer les alertes par courriel**.
4. Dans le volet **Messages à envoyer**, sélectionnez les événements pour lesquels vous voulez envoyer des alertes par courriel.

**Remarque :** les paramètres **Détection des comportements suspects**, **Détection des fichiers suspects** et **Détection et nettoyage des adwares et des PUA** s'appliquent seulement à Windows 2000 et supérieur. Le paramètre **Autres erreurs** s'applique uniquement à Windows.

5. Dans le volet **Destinataires**, cliquez sur **Ajouter** ou sur **Supprimer** pour respectivement ajouter ou supprimer des adresses électroniques auxquelles les alertes par courriel doivent être envoyées. Cliquez sur **Renommer** pour changer une adresse électronique que vous avez ajoutée.

**Important :** les ordinateurs Mac OS X envoient uniquement des messages au premier destinataire de la liste.

6. Cliquez sur **Configurer SMTP** pour changer les paramètres du serveur SMTP et la langue des alertes par courriel.
7. Dans la boîte de dialogue **Configuration des paramètres SMTP**, saisissez les détails comme décrit ci-dessous :

- Dans la zone de texte **Serveur SMTP**, saisissez le nom d'hôte ou l'adresse IP du serveur SMTP. Cliquez sur **Tester** pour vérifier si l'envoi de l'alerte par courriel fonctionne.
- Dans la zone de texte **Adresse expéditeur SMTP**, saisissez une adresse électronique à laquelle les messages renvoyés et les rapports de non-distribution peuvent être envoyés.
- Dans la zone de texte **Adresse réponse SMTP**, vous pouvez saisir une adresse électronique à laquelle les réponses aux alertes par courriel peuvent être envoyées. Les alertes par courriel sont envoyées depuis une boîte aux lettres sans surveillance.

**Remarque :** les ordinateurs Linux ignorent les adresses expéditeur et réponse SMTP et utilisent l'adresse root@<nomhôte>.

- Dans le volet **Langue**, cliquez sur la flèche du menu déroulant et sélectionnez la langue dans laquelle les alertes par courriel doivent être envoyées.

## 8.4 Configuration de la messagerie SNMP antivirus et HIPS

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - antivirus et HIPS** pour effectuer cette tâche. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Il est possible de faire envoyer les messages SNMP à des utilisateurs particuliers lorsqu'un virus ou une erreur est rencontré sur un des ordinateurs du groupe.

**Remarque :** ces paramètres s'appliquent seulement à Windows 2000 et supérieur.

1. Dans le volet **Stratégies**, cliquez deux fois sur la stratégie antivirus et HIPS que vous désirez modifier.
2. Dans la boîte de dialogue **Stratégie antivirus et HIPS**, dans le volet **Configurer l'antivirus et HIPS**, cliquez sur **Messagerie**.
3. Dans la boîte de dialogue **Messagerie**, allez dans l'onglet **Messagerie SNMP** et sélectionnez **Activer la messagerie SNMP**.
4. Dans le volet **Messages à envoyer**, sélectionnez les types d'événements pour lesquels vous voulez que Sophos Endpoint Security and Control envoie des messages SNMP.
5. Dans la zone de texte **Destination de déroutement SNMP**, saisissez l'adresse IP du destinataire.

6. Dans la zone de texte **Nom de la communauté SNMP**, saisissez le nom de la communauté SNMP.

## 8.5 Configuration de la messagerie de bureau antivirus et HIPS

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - antivirus et HIPS** pour effectuer cette tâche. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Par défaut, les messages du bureau sont affichés sur l'ordinateur sur lequel un virus, un élément suspect ou une application potentiellement indésirable est trouvé. Vous pouvez configurer ces messages.

1. Dans le volet **Stratégies**, cliquez deux fois sur la stratégie antivirus et HIPS que vous désirez modifier.
2. Dans la boîte de dialogue **Stratégie antivirus et HIPS**, dans le volet **Configurer l'antivirus et HIPS**, cliquez sur **Messagerie**.
3. Dans la boîte de dialogue **Messagerie**, cliquez sur l'onglet **Messagerie de bureau**.

Par défaut, **Activer la messagerie de bureau** et toutes les options du volet **Messages à envoyer** sont sélectionnées. Modifiez ces paramètres, si nécessaire.

**Remarque :** les paramètres **Détection des comportements suspects**, **Détection des fichiers suspects** et **Détection des adwares et des PUA** s'appliquent seulement à Windows 2000 et supérieur.

4. Dans la zone de texte **Message défini par l'utilisateur**, vous pouvez saisir un message qui sera ajouté à la fin du message de bureau standard.

## 8.6 Configuration des alertes et des messages du contrôle des périphériques

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - contrôle des périphériques** pour modifier une stratégie de contrôle des périphériques. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Enterprise Manager utilise des alertes et des messages pour signaler la détection ou le blocage d'un périphérique contrôlé.

Pour plus d'informations sur la consultation des événements de contrôle des périphériques, reportez-vous à la section [À propos du contrôle des périphériques](#) à la page 111.

Lorsque le contrôle des périphériques est activé, les événements et messages suivants sont consignés ou affichés par défaut :

- Les événements de contrôle des périphériques sont consignés sur la station de travail.
- Les événements de contrôle des périphériques sont envoyés à Enterprise Manager et sont visibles dans le **Contrôle des périphériques - Observateur d'événements** (pour ouvrir l'observateur d'événements, dans le menu **Affichage**, cliquez sur **Événements du contrôle des données**).

- Le nombre d'ordinateurs avec des événements de contrôle des périphériques au-dessus d'un seuil spécifié dans les sept derniers jours apparaît sur le Tableau de bord.
- Des messages apparaissent sur le bureau de la station de travail.

Vous pouvez aussi configurer Enterprise Manager pour envoyer les messages suivants :

<b>Alertes par courriel</b>	Un message électronique est envoyé aux destinataires que vous spécifiez.
<b>Messages SNMP</b>	Un message SNMP est envoyé aux destinataires spécifiés dans vos paramètres de stratégie antivirus et HIPS.

Pour configurer la messagerie du contrôle des périphériques :

1. Vérifiez quelle stratégie de contrôle des applications est utilisée par le ou les groupes d'ordinateurs que vous souhaitez configurer.  
Reportez-vous à la section [Vérification des stratégies utilisées par un groupe](#) à la page 23.
2. Dans le volet **Stratégies**, cliquez deux fois sur **Contrôle des données**. Puis cliquez deux fois sur la stratégie que vous désirez changer.
3. Dans la boîte de dialogue **Stratégie de contrôle des périphériques**, sur l'onglet **Messagerie**, la messagerie de bureau est activée par défaut. Pour une configuration avancée de la messagerie, procédez ainsi :
  - *Pour saisir un texte de message pour la messagerie de bureau*, dans la zone **Corps du message**, saisissez un message qui sera ajouté à la fin du message standard.  
Vous pouvez saisir un maximum de 100 caractères. Vous pouvez également ajouter un lien HTML au message, par exemple, `<a href="http://www.sophos.fr">À propos de Sophos</a>`.
  - *Pour activer les alertes par courriel*, sélectionnez la case à cocher **Activer les alertes par courriel**. Dans le champ **Destinataires des courriels**, saisissez les adresses électroniques des destinataires. Séparez chaque adresse par un point-virgule (;).
  - *Pour activer la messagerie SNMP*, sélectionnez la case à cocher **Activer la messagerie SNMP**.

Les paramètres du serveur de messagerie et de déroutement SNMP sont configurés via la stratégie antivirus et HIPS.

## 8.7 Configuration des alertes par courriel sur l'état du réseau

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Configuration système** pour configurer les alertes par courriel sur l'état du réseau. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Vous pouvez configurer l'envoi des alertes par courriel aux destinataires de votre choix lorsqu'un niveau d'alerte ou critique a été dépassé pour une section du tableau de bord.

1. Dans le menu **Outils**, sélectionnez **Configurer les alertes par courriel**.

La boîte de dialogue **Configuration des alertes par courriel** apparaît.

2. Si les paramètres SMTP n'ont pas été configurés ou si vous voulez visualiser ou changer les paramètres, cliquez sur **Configurer**. Dans la boîte de dialogue **Configuration des paramètres SMTP**, saisissez les détails comme décrit ci-dessous :
  - a) Dans la zone de texte **Adresse du serveur**, saisissez le nom d'hôte ou l'adresse IP du serveur SMTP.
  - b) Dans la zone de texte **Expéditeur**, saisissez une adresse électronique à laquelle les messages renvoyés et les rapports de non-distribution peuvent être envoyés.
  - c) Cliquez sur **Tester** pour tester la connexion.
3. Dans le volet **Destinataires**, cliquez sur **Ajouter**.

La boîte de dialogue **Ajout d'un nouveau destinataire d'alerte par courriel** apparaît.
4. Dans le champ **Adresse électronique**, saisissez l'adresse de votre destinataire.
5. Dans le champ **Langue**, sélectionnez la langue dans laquelle vous souhaitez que soient envoyées les alertes par courriel.
6. Dans le volet **Abonnements**, sélectionnez les alertes par courriel “niveau d'alerte dépassé” et “niveau critique dépassé” que vous souhaitez envoyer au destinataire.

## 8.8 Configuration de la journalisation des événements Windows

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de stratégie - antivirus et HIPS** pour effectuer cette tâche. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Par défaut, Sophos Endpoint Security and Control ajoute des alertes au journal des événements Windows 2000 ou supérieur lorsqu'un virus ou spyware est détecté ou nettoyé, un comportement ou un fichier suspect est détecté ou un adware ou PUA est détecté ou nettoyé.

Pour modifier ces paramètres :

1. Dans le volet **Stratégies**, cliquez deux fois sur la stratégie antivirus et HIPS que vous désirez modifier.
2. Dans la boîte de dialogue **Stratégie antivirus et HIPS**, dans le volet **Configurer l'antivirus et HIPS**, cliquez sur **Messagerie**.
3. Dans la boîte de dialogue **Messages**, allez sur l'onglet **Journalisation des événements**.

Par défaut, la journalisation des événements est activée. Modifiez, le cas échéant, les paramètres.

**Erreurs de contrôle** inclut des instances où l'accès à un élément que Sophos Endpoint Security and Control tente de contrôler lui est refusé.

## 8.9 Affichage des événements

### 8.9.1 À propos des événements

Lorsqu'un événement de pare-feu, de contrôle des périphériques ou de protection antialtération se produit sur un système d'extrémité, par exemple, une application a été bloquée par le

pare-feu, cet événement est envoyé à Enterprise Manager et est visible dans l'observateur d'événements correspondant.

Grâce aux observateurs d'événements, vous pouvez voir les événements qui ont eu lieu sur le réseau. Vous pouvez aussi générer une liste des événements basés sur un filtre que vous configurez, par exemple, une liste de tous les événements de contrôle des périphériques ces sept derniers jours générés par un utilisateur donné.

Le nombre d'ordinateurs avec des événements au-dessus d'un seuil spécifié dans les sept derniers jours apparaît sur le Tableau de bord (sauf pour les événements de protection antialtération). Pour plus d'informations sur la manière de configurer le seuil, reportez-vous à la section [Configuration du Tableau de bord](#) à la page 36.

Vous pouvez aussi configurer l'envoi des alertes par courriel aux destinataires de votre choix lorsqu'un événement s'est produit. Pour plus d'informations, reportez-vous à la section [À propos des alertes et des messages](#) à la page 121.

## 8.9.2 Affichage des événements du contrôle des périphériques

Pour consulter les événements du contrôle des périphériques :

1. Dans le menu **Affichage**, cliquez sur **Événements du contrôle des périphériques**.  
La boîte de dialogue **Contrôle des périphériques - Observateur d'événements** apparaît.
2. Dans le champ **Période de recherche**, cliquez sur la flèche du menu déroulant et sélectionnez la période pour laquelle vous souhaitez afficher les événements.  
Vous pouvez sélectionner soit une période fixe, par exemple, **Depuis 24 heures**, soit **Personnalisée** et spécifiez votre propre période en sélectionnant les dates de début et de fin.
3. Si vous voulez consulter les événements d'un type de périphérique donné, dans le champ **Type de périphérique**, cliquez sur la flèche du menu déroulant et sélectionnez le type de périphérique.  
Par défaut, l'observateur d'événements affiche les événements de tous les types de périphériques.
4. Si vous voulez consulter des événements pour un utilisateur ou un ordinateur donné, saisissez son nom dans le champ prévu.  
Si vous laissez les champs vides, les événements de tous les utilisateurs et ordinateurs apparaîtront.  
Vous pouvez utiliser des caractères joker dans ces champs. Utilisez ? pour remplacer un seul caractère du nom et \* pour remplacer une chaîne de caractères quelconque.
5. Cliquez sur **Rechercher** pour afficher une liste d'événements.

Dans la boîte de dialogue **Contrôle des périphériques - Observateur d'événements**, vous pouvez exempter un périphérique des stratégies de contrôle des périphériques. Pour plus de détails, reportez-vous à la section [Exemption d'un périphérique de toutes les stratégies](#) à la page 115.

Vous pouvez exporter dans un fichier la liste des événements du contrôle des périphériques. Pour plus de détails, reportez-vous à la section [Exportation dans un fichier de la liste des événements](#) à la page 130.

### 8.9.3 Affichage des événements du pare-feu

Les événements de pare-feu sont seulement envoyés une seule fois depuis un ordinateur d'extrémité vers la console. Les événements identiques provenant de différents ordinateurs d'extrémité sont regroupés dans **Pare-feu - Observateur d'événements**. Dans la colonne **Décompte**, vous pouvez voir le nombre total de fois qu'un événement a été envoyé depuis différents ordinateurs d'extrémité.

Pour consulter les événements du pare-feu :

1. Dans le menu **Affichage**, cliquez sur **Événements du pare-feu**.

La boîte de dialogue **Pare-feu - Observateur d'événements** apparaît.

2. Dans le champ **Période de recherche**, cliquez sur la flèche du menu déroulant et sélectionnez la période pour laquelle vous souhaitez afficher les événements.

Vous pouvez sélectionner soit une période fixe, par exemple, **Depuis 24 heures**, soit **Personnalisée** et spécifiez votre propre période en sélectionnant les dates de début et de fin.

3. Si vous voulez consulter les événements d'un certain type, dans le champ **Type d'événement**, cliquez sur la flèche du menu déroulant et sélectionnez le type d'événement.

Par défaut, l'observateur d'événements affiche tous les types d'événements.

4. Si vous voulez consulter les événements pour un certain fichier, saisissez le nom du fichier dans le champ **Nom du fichier**.

Si vous laissez ce champ vide, les événements de tous les fichiers apparaîtront.

Vous pouvez utiliser des caractères joker dans ce champ. Utilisez ? pour remplacer un seul caractère du nom et \* pour remplacer une chaîne de caractères quelconque.

5. Cliquez sur **Rechercher** pour afficher une liste d'événements.

Dans la boîte de dialogue **Pare-feu - Observateur d'événements**, vous pouvez créer une règle de pare-feu comme le décrit la section [Création d'une règle d'événement de pare-feu](#) à la page 85.

Vous pouvez exporter dans un fichier la liste des événements du pare-feu. Pour plus de détails, reportez-vous à la section [Exportation dans un fichier de la liste des événements](#) à la page 130.

### 8.9.4 Affichage des événements de protection antialtération

Il y a deux types d'événements de protection antialtération :

- Les événements réussis d'authentification de la protection antialtération affichant le nom de l'utilisateur authentifié et l'heure d'authentification.
- Les tentatives ratées de modifications affichant le nom du produit ou du composant Sophos pris pour cible, l'heure de la tentative et des informations détaillées sur l'utilisateur responsable de cette tentative.

Pour afficher les événements de protection antialtération :

1. Dans le menu **Affichage**, cliquez sur **Événements de protection antialtération**.  
La boîte de dialogue **Protection antialtération - Observateur d'événements** apparaît.
2. Dans le champ **Période de recherche**, cliquez sur la flèche du menu déroulant et sélectionnez la période pour laquelle vous souhaitez afficher les événements.  
Vous pouvez sélectionner soit une période fixe, par exemple, **Depuis 24 heures**, soit **Personnalisée** et spécifiez votre propre période en sélectionnant les dates de début et de fin.
3. Si vous souhaitez voir certains types d'événements, dans le champ **Type d'événements**, cliquez sur la flèche du menu déroulant et sélectionnez le type d'événements.  
Par défaut, l'observateur d'événements affiche les événements de tous les types.
4. Si vous voulez consulter des événements pour un utilisateur ou un ordinateur donné, saisissez son nom dans le champ prévu.  
Si vous laissez les champs vides, les événements de tous les utilisateurs et ordinateurs apparaîtront.  
Vous pouvez utiliser des caractères joker dans ces champs. Utilisez ? pour remplacer un seul caractère du nom et \* pour remplacer une chaîne de caractères quelconque.
5. Cliquez sur **Rechercher** pour afficher une liste d'événements.

Vous pouvez exporter la liste des événements dans un fichier. Pour plus de détails, reportez-vous à la section [Exportation dans un fichier de la liste des événements](#) à la page 130.

### 8.9.5 Affichage des sites Web bloqués

Vous pouvez afficher la liste des sites Web qui ont récemment été bloqués sur un ordinateur d'extrémité.

Pour afficher les sites Web bloqués récemment :

1. Dans la vue **Ordinateurs d'extrémité**, dans la liste des ordinateurs, cliquez deux fois sur l'ordinateur pour lequel vous souhaitez afficher les sites Web bloqués.
2. Dans la boîte de dialogue **Détails de l'ordinateur**, défilez vers le bas jusqu'à **Derniers sites Web bloqués**.

Vous pouvez aussi afficher le nombre de sites Web qui ont été bloqués pour un utilisateur en générant un rapport. Pour plus d'informations, reportez-vous à la section [Configuration du rapport Événements par utilisateur](#) à la page 138.

## 8.9.6 Exportation dans un fichier de la liste des événements

Vous pouvez exporter dans un fichier CSV la liste des événements de pare-feu, du contrôle des périphériques ou de protection antialtération.

1. Dans le menu **Affichage**, cliquez sur l'une des options "événements", en fonction de la liste d'événements que vous voulez exporter.

La boîte de dialogue **Observateur d'événements** apparaît.

2. Si vous voulez afficher certains événements seulement, dans le volet **Critères de recherche**, définissez les filtres de façon appropriée et cliquez sur **Rechercher** pour afficher les événements.

Pour plus d'informations, reportez-vous aux sections [Affichage des événements du contrôle des périphériques](#) à la page 127, [Affichage des événements du pare-feu](#) à la page 128 ou [Affichage des événements de protection antialtération](#) à la page 128.

3. Cliquez sur **Exporter**.
4. Dans la boîte de dialogue **Enregistrer sous**, saisissez un nom de fichier et naviguez pour sélectionner une destination pour le fichier.

## 9 Génération de rapports

### 9.1 À propos des rapports

Les rapports fournissent des informations textuelles et graphiques sur de nombreux aspects de l'état de sécurité de votre réseau.

Les rapports sont disponibles via le **Gestionnaire des rapports**. À l'aide du **Gestionnaire des rapports**, vous pouvez rapidement créer un rapport basé sur un modèle existant, changer la configuration d'un rapport existant et planifier un rapport pour qu'il s'exécute à intervalles réguliers, et avoir les résultats envoyés aux destinataires de votre choix sous la forme d'une pièce jointe à un courriel. Vous pouvez aussi imprimer des rapports et les exporter dans un certain nombre de formats.

Sophos fournit un certain nombre de rapports prêts à l'emploi ou que vous pouvez configurer selon vos besoins. Ces rapports sont les suivants :

- Historique des alertes et des événements
- Récapitulatif des alertes
- Alertes et événements par nom d'élément
- Alertes et événements par heure
- Alertes et événements par emplacement
- Non-conformité à la stratégie des ordinateurs d'extrémité
- Événements par utilisateur
- Protection des ordinateurs d'extrémité administrés
- Hiérarchie de mise à jour

#### Rapports et administration déléguée

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Configuration du rapport** pour créer, modifier ou supprimer un rapport. Si vous ne disposez pas de ce droit, vous pouvez seulement exécuter un rapport. Pour plus d'informations sur l'administration déléguée, reportez-vous à la section [À propos des rôles](#) à la page 15.

### 9.2 Création d'un nouveau rapport

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Configuration du rapport** pour réaliser cette tâche. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Pour créer un rapport :

1. Cliquez sur l'icône **Rapports** dans la barre d'outils.
2. Dans la boîte de dialogue **Gestionnaire des rapports**, cliquez sur **Créer**.

3. Dans la boîte de dialogue **Création d'un nouveau rapport**, sélectionnez un modèle de rapport et cliquez sur **OK**.

Un assistant vous guide tout au long de la création du rapport d'après votre modèle choisi.

Si vous ne voulez pas utiliser l'assistant, dans la boîte de dialogue **Création d'un nouveau rapport**, désélectionnez la case à cocher **Utiliser l'assistant pour créer le rapport**. Vous pouvez alors configurer votre nouveau rapport dans la boîte de dialogue des propriétés du rapport. Pour plus d'informations, reportez-vous à la section sur la configuration du rapport approprié.

### 9.3 Configuration du rapport Historique des alertes et des événements

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Configuration du rapport** pour réaliser cette tâche. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Le rapport **Historique des alertes et des événements** affiche les alertes et les événements par période de signalement spécifiée.

1. Cliquez sur l'icône **Rapports** dans la barre d'outils.
2. Dans la boîte de dialogue **Gestionnaire des rapports**, sélectionnez **Historique des alertes et des événements** et cliquez sur **Propriétés**.
3. Dans la boîte de dialogue **Propriétés - Historique des alertes et des événements**, sur l'onglet **Configuration**, configurez les options désirées.
  - a) Dans le volet **Détails du rapport**, modifiez le nom et la description du rapport, si vous le souhaitez.
  - b) Dans la zone de texte **Période du rapport**, dans la zone de texte **Période**, cliquez sur la flèche de déroulement et sélectionnez une période de temps.

Vous pouvez soit sélectionner une période de temps définie comme par exemple, **Le mois dernier**, soit sélectionner l'option **Personnalisée** et définir votre propre période de temps dans les cases **Début** et **Fin**.
  - c) Dans le volet **Emplacement du rapport**, cliquez sur **Groupe d'ordinateurs** ou **Ordinateur individuel**. Puis cliquez sur la flèche de déroulement pour spécifier un nom de groupe ou d'ordinateur.
  - d) Dans le volet **Types d'alertes et d'événements à inclure**, sélectionnez des types d'alertes que vous voulez inclure dans le rapport.

Par défaut, le rapport affiche tous les types d'alertes et d'événements.

Autrement, vous pouvez configurer le rapport pour qu'il affiche uniquement les emplacements ayant signalé une alerte ou un événement particulier. Pour spécifier une alerte ou un événement particulier, cliquez sur **Avancés** et cliquez sur un nom d'alerte ou d'événement dans la liste. Pour définir plusieurs alertes ou événements, saisissez un nom dans la zone de texte en utilisant des caractères joker. Utilisez ? pour la substitution d'un seul caractère du nom et \* pour la substitution d'une chaîne de caractères. Par exemple, W32/\* correspond à tous les virus dont le nom commence par W32/.

4. Sur l'onglet **Options d'affichage**, sélectionnez la manière dont vous souhaitez trier les alertes et les événements.  
Par défaut, les détails des alertes et des événements sont triés en fonction du **Nom de l'alerte et de l'événement**. Toutefois, les rapports peuvent aussi être triés en fonction du **Nom d'ordinateur**, du **Nom de groupe** de l'ordinateur, ou de la **Date et heure**.
5. Sur l'onglet **Planification**, sélectionnez **Planifier ce rapport** si vous voulez exécuter le rapport à intervalles réguliers, avec les résultats envoyés aux destinataires choisis sous la forme de pièces jointes à un courriel. Saisissez les dates de début et de fin ainsi que la fréquence avec laquelle le rapport sera généré, spécifiez le format et la langue de sortie et saisissez les adresses électroniques des destinataires du rapport.

## 9.4 Configuration du rapport Récapitulatif des alertes

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Configuration du rapport** pour réaliser cette tâche. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Le rapport **Récapitulatif des alertes** contient des statistiques sur l'état de santé général de votre réseau.

1. Cliquez sur l'icône **Rapports** dans la barre d'outils.
2. Dans la boîte de dialogue **Gestionnaire des rapports**, sélectionnez **Récapitulatif des alertes** et cliquez sur **Propriétés**.
3. Dans la boîte de dialogue **Propriétés - Récapitulatif des alertes**, sur l'onglet **Configuration**, configurez les options désirées.
  - a) Dans le volet **Détails du rapport**, modifiez le nom et la description du rapport, si vous le souhaitez.
  - b) Dans la zone de texte **Période du rapport**, dans la zone de texte **Période**, cliquez sur la flèche de déroulement et sélectionnez une période de temps.  
Vous pouvez soit sélectionner une période de temps définie comme par exemple, **Le mois dernier**, soit sélectionner l'option **Personnalisée** et définir votre propre période de temps dans les cases **Début** et **Fin**.
4. Sur l'onglet **Options d'affichage**, sous **Afficher les résultats par**, spécifiez les intervalles de temps auxquels la non-conformité est mesurée, par exemple toutes les heures ou tous les jours, cliquez sur la flèche du menu déroulant et sélectionnez un intervalle.
5. Sur l'onglet **Planification**, sélectionnez **Planifier ce rapport** si vous voulez exécuter le rapport à intervalles réguliers, avec les résultats envoyés aux destinataires choisis sous la forme de pièces jointes à un courriel. Saisissez les dates de début et de fin ainsi que la fréquence avec laquelle le rapport sera généré, spécifiez le format et la langue de sortie et saisissez les adresses électroniques des destinataires du rapport.

## 9.5 Configuration du rapport Alertes et événements par nom d'élément

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Configuration du rapport** pour réaliser cette tâche. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Le rapport **Alertes et événements par nom d'élément** contient des statistiques sur toutes les alertes et tous les événements issus de tous les ordinateurs sur une période sélectionnée, regroupées par nom d'élément.

Pour configurer le rapport :

1. Cliquez sur l'icône **Rapports** dans la barre d'outils.
2. Dans la boîte de dialogue **Gestionnaire des rapports**, sélectionnez **Alertes et événements par nom d'élément** et cliquez sur **Propriétés**.
3. Dans la boîte de dialogue **Propriétés - Alertes et événements par nom d'élément**, sur l'onglet **Configuration**, configurez les options désirées.
  - a) Dans le volet **Détails du rapport**, modifiez le nom et la description du rapport, si vous le souhaitez.
  - b) Dans la zone de texte **Période du rapport**, dans la zone de texte **Période**, cliquez sur la flèche de déroulement et sélectionnez une période de temps.  
Vous pouvez soit sélectionner une période de temps définie comme par exemple, **Le mois dernier**, soit sélectionner l'option **Personnalisée** et définir votre propre période de temps dans les cases **Début** et **Fin**.
  - c) Dans le volet **Emplacement du rapport**, cliquez sur **Groupe d'ordinateurs** ou **Ordinateur individuel**. Puis cliquez sur la flèche de déroulement pour spécifier un nom de groupe ou d'ordinateur.
  - d) Dans le volet **Types d'alertes et d'événements à inclure**, sélectionnez des types d'alertes que vous voulez inclure dans le rapport.  
Par défaut, le rapport affiche tous les types d'alertes et d'événements.
4. Sur l'onglet **Options d'affichage**, sous **Affichage**, choisissez quels alertes et événements vous souhaitez voir apparaître dans le rapport.

Par défaut, le rapport affiche toutes les alertes et tous les événements ainsi que le nombre d'occurrences pour chacun d'entre eux.

Vous pouvez aussi configurer le rapport pour qu'il indique uniquement :

- les  $n$  premières alertes et événements (où  $n$  est un nombre que vous définissez), ou
- les alertes et les événements avec  $m$  occurrences ou plus (où  $m$  est un nombre que vous définissez).

5. Sous **Trier par**, sélectionnez si vous voulez trier les alertes et les événements par leur numéro ou par leur nom.  
Par défaut, le rapport répertorie les alertes et les événements dans l'ordre décroissant du nombre d'occurrences.
6. Sur l'onglet **Planification**, sélectionnez **Planifier ce rapport** si vous voulez exécuter le rapport à intervalles réguliers, avec les résultats envoyés aux destinataires choisis sous la forme de pièces jointes à un courriel. Saisissez les dates de début et de fin ainsi que la fréquence avec laquelle le rapport sera généré, spécifiez le format et la langue de sortie et saisissez les adresses électroniques des destinataires du rapport.

## 9.6 Configuration du rapport Alertes et événements par heure

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Configuration du rapport** pour réaliser cette tâche. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Le rapport **Alertes et événements par heure** affiche les alertes et les événements récapitulés à des intervalles donnés.

1. Cliquez sur l'icône **Rapports** dans la barre d'outils.
2. Dans la boîte de dialogue **Gestionnaire des rapports**, sélectionnez **Alertes et événements par heure** et cliquez sur **Propriétés**.
3. Dans la boîte de dialogue **Propriétés - Alertes et événements par heure**, sur l'onglet **Configuration**, configurez les options désirées.
  - a) Dans le volet **Détails du rapport**, modifiez le nom et la description du rapport, si vous le souhaitez.
  - b) Dans la zone de texte **Période du rapport**, dans la zone de texte **Période**, cliquez sur la flèche de déroulement et sélectionnez une période de temps.  
Vous pouvez soit sélectionner une période de temps définie comme par exemple, **Le mois dernier**, soit sélectionner l'option **Personnalisée** et définir votre propre période de temps dans les cases **Début** et **Fin**.
  - c) Dans le volet **Emplacement du rapport**, cliquez sur **Groupe d'ordinateurs** ou **Ordinateur individuel**. Puis cliquez sur la flèche de déroulement pour spécifier un nom de groupe ou d'ordinateur.
  - d) Dans le volet **Types d'alertes et d'événements à inclure**, sélectionnez des types d'alertes que vous voulez inclure dans le rapport.  
Par défaut, le rapport affiche tous les types d'alertes et d'événements.  
Autrement, vous pouvez configurer le rapport pour qu'il affiche uniquement les emplacements ayant signalé une alerte ou un événement particulier. Pour spécifier une alerte ou un événement particulier, cliquez sur **Avancés** et cliquez sur un nom d'alerte ou d'événement dans la liste. Pour définir plusieurs alertes ou événements, saisissez un nom dans la zone de texte en utilisant des caractères joker. Utilisez ? pour la substitution d'un seul caractère du nom et \* pour la substitution d'une chaîne de caractères. Par exemple, W32/\* correspond à tous les virus dont le nom commence par W32/.

4. Sur l'onglet **Options d'affichage**, spécifiez les intervalles de temps auxquels la fréquence des alertes et des événements doit être calculée, par exemple toutes les heures ou tous les jours, cliquez sur la flèche du menu déroulant et sélectionnez un intervalle.
5. Sur l'onglet **Planification**, sélectionnez **Planifier ce rapport** si vous voulez exécuter le rapport à intervalles réguliers, avec les résultats envoyés aux destinataires choisis sous la forme de pièces jointes à un courriel. Saisissez les dates de début et de fin ainsi que la fréquence avec laquelle le rapport sera généré, spécifiez le format et la langue de sortie et saisissez les adresses électroniques des destinataires du rapport.

## 9.7 Configuration du rapport Alertes et événements par emplacement

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Configuration du rapport** pour réaliser cette tâche. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Le rapport **Alertes et événements par emplacement** contient des statistiques sur toutes les alertes issues de tous les ordinateurs sur une période sélectionnée, regroupées par emplacement.

1. Cliquez sur l'icône **Rapports** dans la barre d'outils.
2. Dans la boîte de dialogue **Gestionnaire des rapports**, sélectionnez **Alertes et événements par emplacement** et cliquez sur **Propriétés**.
3. Dans la boîte de dialogue **Propriétés - Alertes et événements par emplacement**, sur l'onglet **Configuration**, configurez les options désirées.
  - a) Dans le volet **Détails du rapport**, modifiez le nom et la description du rapport, si vous le souhaitez.
  - b) Dans la zone de texte **Période du rapport**, dans la zone de texte **Période**, cliquez sur la flèche de déroulement et sélectionnez une période de temps.

Vous pouvez soit sélectionner une période de temps définie comme par exemple, **Le mois dernier**, soit sélectionner l'option **Personnalisée** et définir votre propre période de temps dans les cases **Début** et **Fin**.
  - c) Dans le volet **Emplacement du rapport**, cliquez sur **Ordinateurs** pour afficher les alertes par ordinateur ou sur **Groupe** pour afficher les alertes pour chaque groupe d'ordinateurs.
  - d) Dans le volet **Types d'alertes et d'événements à inclure**, sélectionnez des types d'alertes que vous voulez inclure dans le rapport.

Par défaut, le rapport affiche tous les types d'alertes et d'événements.

Autrement, vous pouvez configurer le rapport pour qu'il affiche uniquement les emplacements ayant signalé une alerte ou un événement particulier. Pour spécifier une alerte ou un événement particulier, cliquez sur **Avancés** et cliquez sur un nom d'alerte ou d'événement dans la liste. Pour définir plusieurs alertes ou événements, saisissez un nom dans la zone de texte en utilisant des caractères joker. Utilisez ? pour la substitution d'un seul caractère du nom et \* pour la substitution d'une chaîne de caractères. Par exemple, W32/\* correspond à tous les virus dont le nom commence par W32/.

4. Sur l'onglet **Options d'affichage**, sous **Affichage**, choisissez quels emplacements vous voulez que le rapport affiche.

Par défaut, le rapport affiche tous les ordinateurs et groupes ainsi que le nombre d'occurrences pour chacun d'entre eux. Vous pouvez le configurer pour qu'il affiche uniquement :

- les  $n$  premiers emplacements qui ont enregistré le plus d'alertes et d'événements (ou  $n$  est un nombre que vous définissez), ou
  - les emplacements avec  $m$  alertes et événements ou plus (où  $m$  est un nombre que vous définissez).
5. Sous **Trier par**, sélectionnez si vous voulez trier les emplacements par le nombre d'éléments détectés ou par leur nom.  
Par défaut, le rapport répertorie les emplacements dans l'ordre décroissant du nombre d'alertes et d'événements par emplacement. Sélectionnez **Emplacement** si vous souhaitez qu'ils soient classés par nom dans l'ordre alphabétique.
  6. Sur l'onglet **Planification**, sélectionnez **Planifier ce rapport** si vous voulez exécuter le rapport à intervalles réguliers, avec les résultats envoyés aux destinataires choisis sous la forme de pièces jointes à un courriel. Saisissez les dates de début et de fin ainsi que la fréquence avec laquelle le rapport sera généré, spécifiez le format et la langue de sortie et saisissez les adresses électroniques des destinataires du rapport.

## 9.8 Configuration du rapport Non-conformité à la stratégie des systèmes d'extrémité

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Configuration du rapport** pour réaliser cette tâche. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Le rapport **Non-conformité à la stratégie des systèmes d'extrémité** affiche le pourcentage ou le nombre d'ordinateurs qui ne sont pas en conformité avec la stratégie de leur groupe, récapitulé à des intervalles donnés.

1. Cliquez sur l'icône **Rapports** dans la barre d'outils.
2. Dans la boîte de dialogue **Gestionnaire des rapports**, sélectionnez **Non-conformité à la stratégie des systèmes d'extrémité** et cliquez sur **Propriétés**.
3. Dans la boîte de dialogue **Propriétés - Non-conformité à la stratégie des systèmes d'extrémité**, sur l'onglet **Configuration**, configurez les options désirées.
  - a) Dans le volet **Détails du rapport**, modifiez le nom et la description du rapport, si vous le souhaitez.
  - b) Dans la zone de texte **Période du rapport**, dans la zone de texte **Période**, cliquez sur la flèche de déroulement et sélectionnez une période de temps.

Vous pouvez soit sélectionner une période de temps définie comme par exemple, **Le mois dernier**, soit sélectionner l'option **Personnalisée** et définir votre propre période de temps dans les cases **Début** et **Fin**.

- c) Dans le volet **Affichage**, sélectionnez les stratégies que vous voulez afficher dans le rapport. Par défaut, seule la stratégie **antivirus et HIPS** est sélectionnée.
4. Sur l'onglet **Options d'affichage**, sous **Afficher les résultats par**, spécifiez les intervalles de temps auxquels la non-conformité est mesurée, par exemple toutes les heures ou tous les jours, cliquez sur la flèche du menu déroulant et sélectionnez un intervalle.
5. Sous **Afficher les résultats sous la forme de**, sélectionnez si vous voulez afficher les résultats sous la forme de pourcentages ou de nombres.
6. Sur l'onglet **Planification**, sélectionnez **Planifier ce rapport** si vous voulez exécuter le rapport à intervalles réguliers, avec les résultats envoyés aux destinataires choisis sous la forme de pièces jointes à un courriel. Saisissez les dates de début et de fin ainsi que la fréquence avec laquelle le rapport sera généré, spécifiez le format et la langue de sortie et saisissez les adresses électroniques des destinataires du rapport.

## 9.9 Configuration du rapport Événements par utilisateur

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Configuration du rapport** pour réaliser cette tâche. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Le rapport **Événements par utilisateur** affiche les événements de pare-feu et de contrôle des périphériques et regroupe également les sites Web bloqués par utilisateur.

1. Cliquez sur l'icône **Rapports** dans la barre d'outils.
2. Dans la boîte de dialogue **Gestionnaire des rapports**, sélectionnez **Événements par utilisateur** et cliquez sur **Propriétés**.
3. Dans la boîte de dialogue **Propriétés - Événements par utilisateur**, sur l'onglet **Configuration**, configurez les options désirées.
  - a) Dans le volet **Détails du rapport**, modifiez le nom et la description du rapport, si vous le souhaitez.
  - b) Dans la zone de texte **Période du rapport**, dans la zone de texte **Période**, cliquez sur la flèche de déroulement et sélectionnez une période de temps.

Vous pouvez soit sélectionner une période de temps définie comme par exemple, **Le mois dernier**, soit sélectionner l'option **Personnalisée** et définir votre propre période de temps dans les cases **Début** et **Fin**.
  - c) Sous **Types d'événements à inclure**, sélectionnez les fonctionnalités pour lesquelles vous voulez afficher les événements.

4. Sur l'onglet **Options d'affichage**, sous **Affichage**, choisissez quels utilisateurs vous voulez que le rapport affiche.

Par défaut, le rapport affiche tous les utilisateurs ainsi que le nombre d'événements pour chacune d'entre elles. Vous pouvez le configurer pour qu'il affiche uniquement :

- les  $n$  premiers utilisateurs qui ont enregistré le plus d'événements (ou  $n$  est un nombre que vous définissez), ou
  - les utilisateurs avec  $m$  événements ou plus (où  $m$  est un nombre que vous définissez).
5. Sous **Trier par**, sélectionnez si vous voulez trier les utilisateurs par le nombre d'événements ou par leur nom.  
Par défaut, le rapport répertorie les utilisateurs dans l'ordre décroissant du nombre d'événements par utilisateur. Sélectionnez **Utilisateur** si vous souhaitez qu'ils soient classés par nom dans l'ordre alphabétique.
  6. Sur l'onglet **Planification**, sélectionnez **Planifier ce rapport** si vous voulez exécuter le rapport à intervalles réguliers, avec les résultats envoyés aux destinataires choisis sous la forme de pièces jointes à un courriel. Saisissez les dates de début et de fin ainsi que la fréquence avec laquelle le rapport sera généré, spécifiez le format et la langue de sortie et saisissez les adresses électroniques des destinataires du rapport.

## 9.10 Configuration du rapport Protection des ordinateurs d'extrémité administrés

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Configuration du rapport** pour réaliser cette tâche. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Le rapport **Protection des ordinateurs d'extrémité administrés** indique le pourcentage ou le nombre d'ordinateurs protégés, récapitulés à des intervalles donnés.

1. Cliquez sur l'icône **Rapports** dans la barre d'outils.
2. Dans la boîte de dialogue **Gestionnaire des rapports**, sélectionnez **Protection des ordinateurs d'extrémité administrés** et cliquez sur **Propriétés**.
3. Dans la boîte de dialogue **Propriétés - Protection des ordinateurs d'extrémité administrés**, sur l'onglet **Configuration**, configurez les options désirées.
  - a) Dans le volet **Identité du rapport**, modifiez le nom et la description du rapport, si vous le souhaitez.
  - b) Dans la zone de texte **Période du rapport**, dans la zone de texte **Période**, cliquez sur la flèche de déroulement et sélectionnez une période de temps.  
Vous pouvez soit sélectionner une période de temps définie comme par exemple, **Le mois dernier**, soit sélectionner l'option **Personnalisée** et définir votre propre période de temps dans les cases **Début** et **Fin**.
  - c) Dans le volet **Affichage**, sélectionnez les fonctionnalités que vous voulez afficher dans le rapport.

4. Sur l'onglet **Options d'affichage**, sous **Afficher les résultats par**, spécifiez les intervalles de temps auxquels la non-conformité est mesurée, par exemple toutes les heures ou tous les jours, cliquez sur la flèche du menu déroulant et sélectionnez un intervalle.
5. Sous **Afficher les résultats sous la forme de**, sélectionnez si vous voulez afficher les résultats sous la forme de pourcentages ou de nombres.
6. Sur l'onglet **Planification**, sélectionnez **Planifier ce rapport** si vous voulez exécuter le rapport à intervalles réguliers, avec les résultats envoyés aux destinataires choisis sous la forme de pièces jointes à un courriel. Saisissez les dates de début et de fin ainsi que la fréquence avec laquelle le rapport sera généré, spécifiez le format et la langue de sortie et saisissez les adresses électroniques des destinataires du rapport.

## 9.11 Rapport Hiérarchie des mises à jour

Le rapport **Hiérarchie des mises à jour** affiche le gestionnaire de mise à jour sur votre réseau, les partages de mise à jour qu'il gère et le nombre d'ordinateurs qui se mettent à jour depuis ces partages.

Vous ne pouvez pas configurer le rapport **Hiérarchie des mises à jour**. Vous pouvez exécuter le rapport comme le décrit la section [Exécution d'un rapport](#) à la page 140.

## 9.12 Planification d'un rapport

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Configuration du rapport** pour réaliser cette tâche. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Vous pouvez planifier un rapport à exécuter à des intervalles réguliers, avec envoi des résultats aux destinataires de votre choix sous la forme de pièces jointes à un courriel.

1. Cliquez sur l'icône **Rapports** dans la barre d'outils.
2. Dans la boîte de dialogue **Gestionnaire des rapports**, sélectionnez le rapport que vous voulez planifier et cliquez sur **Planifier**.
3. Dans la boîte de dialogue qui apparaît, sur l'onglet **Planification**, sélectionnez **Planifier ce rapport**.
4. Saisissez la date de début et de fin ainsi que la fréquence avec laquelle le rapport sera généré.
5. Spécifiez le format et la langue du fichier de sortie.
6. Saisissez les adresses électroniques des destinataires du rapport.

## 9.13 Exécution d'un rapport

1. Cliquez sur l'icône **Rapports** dans la barre d'outils.
2. Dans la boîte de dialogue **Gestionnaire des rapports**, sélectionnez le rapport que vous voulez exécuter et cliquez sur **Exécuter**.

La fenêtre **Edition de rapports**, affichant le rapport, apparaît.

Vous pouvez changer la mise en page du rapport, l'imprimer ou l'exporter dans un fichier.

## 9.14 Affichage d'un rapport sous forme de tableau ou de diagramme

Certains rapports peuvent être affichés sous la forme d'un tableau et d'un diagramme. Si c'est le cas, deux onglets apparaissent, **Tableau** et **Diagramme** dans la fenêtre **Edition de rapports** affichant le rapport.

1. Cliquez sur l'icône **Rapports** dans la barre d'outils.
2. Dans la boîte de dialogue **Gestionnaire des rapports**, sélectionnez le rapport que vous voulez exécuter, par exemple, **Alertes et événements par emplacement**, et cliquez sur **Exécuter**.

La fenêtre **Edition de rapports**, affichant le rapport, apparaît.

3. Pour voir le rapport sous la forme d'un tableau ou d'un diagramme, allez sur l'onglet approprié.

## 9.15 Impression d'un rapport

Pour imprimer un rapport, cliquez sur l'icône **Imprimer** de la barre d'outils en haut du rapport.



## 9.16 Exportation d'un rapport dans un fichier

Pour exporter un rapport dans un fichier :

1. Cliquez sur l'icône **Exporter** de la barre d'outils en haut du rapport.



2. Dans la boîte de dialogue **Exportation du rapport**, sélectionnez le type de document ou de feuille de calcul vers lequel vous souhaitez exporter le rapport.

Les options sont :

- PDF (Acrobat)
  - HTML
  - Microsoft Excel
  - Microsoft Word
  - Format texte enrichi (RTF)
  - Valeurs séparées par des virgules (CSV)
  - XML
3. Cliquez sur le bouton de navigation **Nom du fichier** pour sélectionner un emplacement. Puis saisissez un nom. Cliquez sur **OK**.

## 9.17 Modification de la mise en page du rapport

Vous pouvez modifier la mise en page utilisée pour les rapports. Par exemple, vous pouvez afficher un rapport au format paysage (largeur de page).

1. Cliquez sur l'icône de mise en page de la barre d'outils en haut du rapport.



2. Dans la boîte de dialogue **Mise en page**, définissez la taille, l'orientation et les marges de la page. Cliquez sur **OK**.

Le rapport s'affichera ensuite avec ces paramètres de mise en page.

Ces paramètres de mise en page seront aussi utilisés lorsque vous imprimerez ou exporterez le rapport.

## 10 Copie ou impression des données depuis Enterprise Manager

### 10.1 Copie de données depuis la liste des ordinateurs

Dans la vue **Ordinateurs d'extrémité**, vous pouvez copier les informations affichées dans la liste des ordinateurs dans le Presse-papiers, puis les coller dans un autre document dans un format séparé par des tabulations.

1. Dans la vue **Ordinateurs d'extrémité**, dans le volet **Groupes**, sélectionnez le groupe d'ordinateurs pour lesquels vous voulez copier les données.
2. Dans la liste déroulante **Vue**, sélectionnez les ordinateurs que vous souhaitez afficher, par exemple, les **Ordinateurs avec des problèmes éventuels**.
3. Si le groupe contient des sous-groupes, sélectionnez également si vous souhaitez afficher les ordinateurs **A ce niveau seulement** ou **A ce niveau et au-dessous**.
4. Dans la liste des ordinateurs, allez dans l'onglet que vous voulez afficher, par exemple, **Détails de l'antivirus**.
5. Cliquez n'importe où dans la liste des ordinateurs pour vous y concentrer.
6. Dans le menu **Édition**, cliquez sur **Copier** pour copier les données dans le Presse-papiers.

### 10.2 Impression de données depuis la liste des ordinateurs

Vous pouvez imprimer des informations affichées dans la liste des ordinateurs, dans la vue **Ordinateurs d'extrémité**.

1. Dans la vue **Ordinateurs d'extrémité**, dans le volet **Groupes**, sélectionnez le groupe d'ordinateurs pour lesquels vous voulez imprimer les données.
2. Dans la liste déroulante **Vue**, sélectionnez les ordinateurs que vous souhaitez afficher, par exemple, les **Ordinateurs avec des problèmes éventuels**.
3. Si le groupe contient des sous-groupes, sélectionnez également si vous souhaitez afficher les ordinateurs **A ce niveau seulement** ou **A ce niveau et au-dessous**.
4. Dans la liste des ordinateurs, allez dans l'onglet que vous voulez afficher, par exemple, **Détails de l'antivirus**.
5. Cliquez n'importe où dans la liste des ordinateurs pour vous y concentrer.
6. Dans le menu **Fichier**, cliquez sur **Imprimer**.

### 10.3 Copie des détails d'un ordinateur

Vous pouvez copier des informations depuis la boîte de dialogue **Détails de l'ordinateur** dans le Presse-papiers, puis les coller dans un autre document. Les informations incluent le nom de l'ordinateur, le système d'exploitation, les versions du logiciel de sécurité installé, toutes les alertes et les erreurs à traiter, le statut de mise à jour, et ainsi de suite.

1. Dans la vue **Ordinateurs d'extrémité**, dans la liste des ordinateurs, cliquez deux fois sur l'ordinateur dont vous voulez copier les données.

2. Dans la boîte de dialogue **Détails de l'ordinateur**, cliquez sur **Copier** pour copier les données dans le Presse-papiers.

## 10.4 Impression des détails d'un ordinateur

Vous pouvez imprimer les informations depuis la boîte de dialogue **Détails de l'ordinateur**. Les informations incluent le nom de l'ordinateur, le système d'exploitation, les versions du logiciel de sécurité installé, toutes les alertes et les erreurs à traiter, le statut de mise à jour, et ainsi de suite.

1. Dans la vue **Ordinateurs d'extrémité**, dans la liste des ordinateurs, cliquez deux fois sur l'ordinateur dont vous voulez imprimer les données.
2. Dans la boîte de dialogue **Détails de l'ordinateur**, cliquez sur **Imprimer**.

## 11 Résolution des problèmes

### 11.1 Les ordinateurs n'utilisent pas le contrôle sur accès

Si vous avez des ordinateurs sur lesquels le contrôle sur accès ne fonctionne pas :

1. Vérifiez quelle stratégie antivirus et HIPS est utilisée par ces ordinateurs.  
Pour plus de détails, reportez-vous à la section [Vérification des stratégies utilisées par un groupe](#) à la page 23.
2. Assurez-vous que le contrôle sur accès est activé dans cette stratégie et que les ordinateurs sont conformes à la stratégie.  
Pour plus de détails, reportez-vous aux sections [Activation ou désactivation du contrôle sur accès](#) à la page 72 et [Application de la stratégie de groupe par les ordinateurs](#) à la page 27.

### 11.2 Le pare-feu est désactivé

S'il existe des ordinateurs dont le pare-feu est désactivé :

1. Vérifiez quelle stratégie de pare-feu est utilisée par ces ordinateurs.  
Pour plus de détails, reportez-vous à la section [Vérification des stratégies utilisées par un groupe](#) à la page 23.
2. Assurez-vous que le pare-feu est activé dans cette stratégie et que les ordinateurs sont conformes à la stratégie.  
Pour plus de détails, reportez-vous aux sections [Désactivation temporaire du pare-feu](#) à la page 86 et [Application de la stratégie de groupe par les ordinateurs](#) à la page 27.

### 11.3 Le pare-feu n'est pas installé

**Remarque :** si vous utilisez l'administration déléguée, vous devez disposer du droit **Recherche des ordinateurs, protection et groupes** pour installer le pare-feu. Pour plus d'informations, reportez-vous à la section [À propos des rôles](#) à la page 15.

Avant d'essayer d'installer le pare-feu client sur les ordinateurs d'extrémité, assurez-vous que :

- Votre licence inclut le pare-feu.
- Les ordinateurs exécutent Windows 2000 ou une version supérieure.

**Remarque :** vous ne pouvez pas installer le pare-feu sur des ordinateurs exécutant des systèmes d'exploitation serveur ou Windows Vista Starter.

S'il y a des ordinateurs sur lesquels vous voulez installer le pare-feu :

1. Sélectionnez ces ordinateurs, cliquez dessus avec le bouton droit de la souris et sélectionnez **Protéger les ordinateurs**.  
L'**Assistant de protection des ordinateurs** apparaît. Cliquez sur **Suivant**.

2. Lorsque vous êtes invité à sélectionner des fonctionnalités, sélectionnez **Pare-feu**. Fermez l'assistant.

Si le problème persiste, veuillez contacter le support technique de Sophos.

## 11.4 Ordinateurs avec des alertes à traiter

- En cas de présence d'un virus ou d'une application indésirable sur des ordinateurs, reportez-vous à la section [Nettoyage immédiat des ordinateurs](#) à la page 43.
- En cas de présence *souhaitée* d'un adware ou de toute autre application potentiellement indésirable sur des ordinateurs, reportez-vous à la section [Autorisation des adwares et des PUA](#) à la page 69.
- Si des ordinateurs ne sont pas à jour, reportez-vous à la section [Mise à jour des ordinateurs non à jour](#) à la page 61 pour obtenir de l'aide sur le diagnostic et corriger le problème.

**Remarque :** si l'affichage de l'alerte n'est plus nécessaire, vous pouvez l'effacer. Sélectionnez le ou les ordinateurs affichant des alertes, cliquez dessus avec le bouton droit de la souris et sélectionnez **Résoudre les alertes et les erreurs**. Vous devez disposer du droit **Actualisation - nettoyage** pour approuver (effacer) les alertes et les erreurs.

## 11.5 Les ordinateurs ne sont pas administrés par la console

Les ordinateurs doivent être administrés par Enterprise Manager afin de pouvoir être mis à jour et sous surveillance.

**Remarque :** les nouveaux ordinateurs ajoutés au réseau ne s'affichent pas ou ne sont pas administrés automatiquement par la console. Cliquez sur **Rechercher de nouveaux ordinateurs** dans la barre d'outils pour les rechercher et les placer dans le groupe **Non affectés**.

Si un ordinateur n'est pas administré, les détails le concernant sur l'onglet **Etat** sont grisés.

Pour lancer l'administration des ordinateurs non administrés :

1. Dans la liste déroulante **Vue**, sélectionnez **Ordinateurs non administrés**.
2. Sélectionnez tous les ordinateurs qui sont répertoriés. Cliquez avec le bouton droit de la souris et sélectionnez **Protéger les ordinateurs** pour installer une version administrée de Sophos Endpoint Security and Control.
3. Si Enterprise Manager ne parvient pas à installer Sophos Endpoint Security and Control automatiquement sur certains ordinateurs, procédez à une installation manuelle.

Pour plus de détails, reportez-vous au *Guide de démarrage de Sophos Enterprise Manager* .

## 11.6 Impossible de protéger les ordinateurs du groupe Non affectés

Le groupe **Non affectés** sert seulement à conserver les ordinateurs qui ne sont pas encore dans des groupes que vous avez créés et auxquels des stratégies peuvent être appliquées. Vous ne pouvez pas protéger les ordinateurs tant que vous ne les avez pas placés dans un groupe.

## 11.7 L'installation de Sophos Endpoint Security and Control a échoué

Si l'**Assistant de protection des ordinateurs** ne parvient pas à installer Sophos Endpoint Security and Control sur les ordinateurs, c'est probablement parce que :

- Enterprise Manager ne reconnaît pas le système d'exploitation exécuté par les ordinateurs. Ceci est probablement dû au fait que vous n'avez pas saisi votre nom utilisateur au format domaine\utilisateur lors de la recherche d'ordinateurs.
- L'installation automatique est impossible sur ce système d'exploitation. Effectuez une installation manuelle. Retrouvez plus d'instructions dans le *Guide de démarrage de Sophos Enterprise Manager* .
- Les ordinateurs exécutent un pare-feu.
- Le "Partage de fichiers simple" n'a pas été désactivé sur les ordinateurs Windows XP.
- L'option "Utiliser l'Assistant Partage" n'a pas été désactivée sur les ordinateurs Windows Vista.
- Vous avez choisi d'installer une fonction qui n'est pas prise en charge par les systèmes d'exploitation des ordinateurs.

Si l'installation de l'agent de conformité échoue ou si une erreur survient au cours de l'installation, vous pouvez consulter le journal d'installation de l'agent de conformité. Le journal se trouve dans le dossier %tmp%.

Pour une liste complète des configurations requises pour les fonctions de Sophos Endpoint Security and Control, consultez la page des configurations requises sur le site Web de Sophos (<http://www.sophos.fr/products/all-sysreqs.html>).

## 11.8 Les ordinateurs ne sont pas mis à jour

Reportez-vous à la section [Mise à jour des ordinateurs non à jour](#) à la page 61 pour obtenir de l'aide sur le diagnostic et la correction du problème.

## 11.9 Impossible de créer une nouvelle stratégie

Si les options **Créer une stratégie** et **Dupliquer une stratégie** sont désactivées, cela signifie que vous avez atteint le nombre maximum de stratégies que vous pouvez créer. Vous pouvez créer un maximum de quatre nouvelles stratégies de chaque type (c'est-à-dire, quatre nouvelles stratégies antivirus et HIPS, etc.).

## 11.10 Les paramètres antivirus ne s'appliquent pas sur Macintosh

Certains paramètres antivirus ne peuvent s'appliquer aux ordinateurs Mac. Dans ce cas, un avertissement apparaît sur cette page de paramètres.

Vous pouvez modifier les paramètres antivirus sur les ordinateurs Mac avec Sophos Update Manager, un utilitaire fourni avec Sophos Anti-Virus pour Mac. Pour ouvrir Sophos Update Manager, sur un ordinateur Mac, dans la fenêtre **Finder**, naviguez jusqu'au dossier Sophos

Anti-Virus:ESOSX. Cliquez deux fois sur **Sophos Update Manager**. Pour de plus amples détails, reportez-vous à l'aide du Sophos Update Manager.

### 11.11 Les paramètres antivirus ne s'appliquent pas sur Linux

Certains paramètres antivirus ne peuvent s'appliquer aux ordinateurs Linux. Dans ce cas, un avertissement apparaît sur cette page de paramètres.

Vous pouvez modifier les paramètres antivirus des ordinateurs Linux à l'aide des commandes **savconfig** et **savscan** comme le décrit le *Manuel utilisateur de Sophos Anti-Virus pour Linux*.

### 11.12 L'ordinateur Linux n'applique pas la stratégie

Si vous utilisez un fichier de configuration d'entreprise dans le CID, et si le fichier contient une valeur de configuration en conflit avec la stratégie, l'ordinateur apparaît comme non conforme avec la stratégie.

La sélection de l'option **Appliquer la stratégie** met l'ordinateur en conformité seulement temporairement, jusqu'à ce que la configuration de type CID soit réappliquée.

Pour résoudre le problème, parcourez le fichier de configuration d'entreprise et, le cas échéant, remplacez-le par une configuration basée sur la console.

### 11.13 Apparition inattendue d'un nouveau contrôle sur Windows 2000 ou supérieur

Si vous regardez la copie locale de Sophos Endpoint Security and Control sur les ordinateurs Windows 2000 ou supérieur, vous remarquerez qu'un nouveau "Contrôle disponible" est répertorié alors que l'utilisateur n'en a pas créé.

Ce nouveau contrôle est en fait un contrôle planifié que vous avez configuré depuis la console. Ne le supprimez pas.

### 11.14 Problèmes de connectivité et de délai

Si les communications entre Enterprise Manager et un ordinateur en réseau sont lentes ou si l'ordinateur ne répond pas, il se peut qu'il y ait un problème de connectivité.

Vérifiez le rapport sur les communications réseau Sophos qui présente un aperçu de l'état actuel des communications entre un ordinateur et Enterprise Manager. Pour voir le rapport, rendez-vous sur l'ordinateur concerné par le problème. Sur la barre des tâches, cliquez sur le bouton **Démarrer**, sélectionnez **Tous les programmes|Sophos|Sophos Endpoint Security and Control** et cliquez sur **Voir le rapport sur les communications réseau Sophos**.

Le rapport indique les zones à problèmes éventuelles et, en cas de détection d'un problème, les actions à prendre pour y remédier.

## 11.15 Les adwares et les PUA ne sont pas détectés

Si des adwares et autres applications potentiellement indésirables (PUA) ne sont pas détectés, assurez-vous que :

- La détection a été activée. Reportez-vous à la section [Recherche d'adwares et de PUA](#) à la page 68.
- Les applications figurent sur un ordinateur exécutant Windows 2000 ou supérieur.

## 11.16 Élément partiellement détecté

Sophos Endpoint Security and Control peut signaler qu'un élément (par exemple, un cheval de Troie ou une application potentiellement indésirable) est "partiellement détecté". Ceci signifie qu'il n'a pas trouvé tous les composants de cette application.

Pour trouver d'autres composants, il est nécessaire que vous lanciez un contrôle intégral du système du ou des ordinateurs affectés. Sur les ordinateurs exécutant Windows 2000 ou supérieur, vous pouvez exécuter cette opération en sélectionnant le ou les ordinateurs, en cliquant avec le bouton droit de la souris et en sélectionnant **Contrôle intégral du système**. Vous pouvez aussi configurer un contrôle planifié à la recherche d'adwares et d'autres applications potentiellement indésirables. Reportez-vous à la section [Recherche d'adwares et de PUA](#) à la page 68.

Si l'application n'a toujours pas été intégralement détectée, il se peut que ce soit parce que :

- Vos droits d'accès sont insuffisants
- Certains lecteurs ou dossiers de l'ordinateur, contenant les composants de l'application, sont exclus du contrôle.

S'il s'agit du dernier cas, vérifiez la liste des éléments exclus du contrôle (reportez-vous à la section [Exclusion des éléments du contrôle sur accès](#) à la page 72). Si certains éléments figurent dans la liste, supprimez-les de la liste et lancez un nouveau contrôle de l'ordinateur.

Il se peut que Sophos Endpoint Security and Control ne soit pas en mesure de détecter intégralement ou de supprimer les adwares et les applications potentiellement indésirables dont les composants sont installés sur des lecteurs réseau.

Pour plus de conseils, contactez le support technique Sophos.

## 11.17 Fréquentes alertes concernant les applications potentiellement indésirables

Il est possible que vous receviez un très grand nombre d'alertes à propos d'applications potentiellement indésirables, y compris de nombreux rapports concernant la même application.

Ceci peut survenir parce que certains types d'application potentiellement indésirable "surveillent" les fichiers et essaient d'y accéder régulièrement. Si le contrôle sur accès est activé, Sophos Endpoint Security and Control détecte chaque accès à un fichier et envoie une alerte.

Procédez de la manière suivante :

- Désactivez le contrôle sur accès des adwares et des PUA. Vous pouvez utiliser un contrôle planifié à la place.
- Autorisez l'application (si vous désirez qu'elle soit exécutée sur vos ordinateurs). Reportez-vous à la section [Autorisation des adwares et des PUA](#) à la page 69.
- Nettoyez le ou les ordinateurs en supprimant les applications que vous n'avez pas autorisées. Reportez-vous à la section [Nettoyage immédiat des ordinateurs](#) à la page 43.

## 11.18 Échec du nettoyage

Si Sophos Endpoint Security and Control ne parvient pas à nettoyer les éléments ("Echec du nettoyage"), c'est probablement pour la raison suivante :

- Il n'a pas trouvé tous les composants d'un élément à plusieurs composants. Exécutez un contrôle intégral du système du ou des ordinateurs pour trouver les autres composants. Reportez-vous à la section [Contrôle immédiat des ordinateurs](#) à la page 43.
- Certains lecteurs ou dossiers contenant les composants de l'élément sont exclus du contrôle. Vérifiez les éléments exclus du contrôle (reportez-vous à la section [Exclusion des éléments du contrôle sur accès](#) à la page 72). Si certains éléments figurent dans la liste, supprimez-les de la liste.
- Vos droits d'accès sont insuffisants
- Il ne parvient pas à nettoyer ce type d'élément.
- Un fragment de virus a été découvert plutôt qu'une correspondance virale exacte.
- L'élément se trouve sur une disquette ou un CD-ROM protégé en écriture.
- L'élément se trouve sur un volume NTFS (Windows 2000 ou supérieur) protégé en écriture.

## 11.19 Guérison des effets secondaires des virus

Le nettoyage peut supprimer un virus des ordinateurs mais ne peut pas toujours neutraliser les effets secondaires.

Certains virus ne laissent aucun effet secondaire. D'autres peuvent apporter des modifications ou corrompre des données de telle manière qu'il est très difficile de les détecter. Pour gérer ce problème, procédez comme suit :

- Cliquer sur **Informations sur la sécurité** dans le menu **Aide**. Cette opération vous connecte au site Web de Sophos sur lequel vous pouvez consulter l'analyse du virus.
- Utilisez des sauvegardes ou des copies originales des programmes pour remplacer les programmes infectés. Si vous n'aviez pas de copies de sauvegarde avant l'infection, créez-les en cas de futures infections.

Il est parfois possible de récupérer des données depuis les disques endommagés par un virus. Sophos peut vous fournir des utilitaires pour réparer les dommages occasionnés par certains virus. Contactez le support technique de Sophos pour obtenir des conseils.

## 11.20 Guérison des effets secondaires des applications

Le nettoyage supprime les applications indésirables mais ne peut pas toujours neutraliser les effets secondaires.

Certaines applications modifient le système d'exploitation, par exemple, en changeant vos paramètres de connexion Internet. Sophos Endpoint Security and Control ne peut pas toujours restaurer tous les paramètres. Par exemple, si une application a modifié la page d'accueil de l'explorateur, Sophos Endpoint Security and Control ne peut pas savoir quelle page d'accueil était utilisée auparavant.

Certaines applications installent des utilitaires, tels que des fichiers .dll ou .ocx sur votre ordinateur. Si un utilitaire est inoffensif (c'est-à-dire qu'il ne possède pas les "qualités" d'une application potentiellement indésirable), par exemple, une bibliothèque de langue, et qu'il ne fait pas partie intégrante de l'application, il se peut que Sophos Endpoint Security and Control ne le détecte pas en tant que partie de l'application. Dans ce cas, le nettoyage n'entraînera pas la suppression du fichier de votre ordinateur.

Parfois une application, telle qu'un adware (logiciel publicitaire), fait partie d'un programme que vous avez installé de manière intentionnelle, et sa présence est requise pour pouvoir exécuter le programme. Si vous supprimez cette application, l'exécution de ce programme peut s'interrompre sur l'ordinateur.

Vous devez :

- Cliquer sur **Informations sur la sécurité** dans le menu **Aide**. Cette opération vous connecte au site Web de Sophos sur lequel vous pouvez consulter l'analyse de l'application.
- Utiliser des sauvegardes pour restaurer les paramètres de votre système ou les programmes que vous désirez utiliser. Si vous n'aviez pas de copies de sauvegarde avant l'incident, créez-les en cas de futurs incidents.

Pour plus d'informations ou de conseils sur la manière de guérir les effets secondaires d'un adware ou d'une application potentiellement indésirable, contactez le support technique Sophos.

## 12 Glossaire

<b>Abonnement logiciels</b>	Ensemble des versions d'un logiciel pour une variété de plates-formes, sélectionnées par l'utilisateur, qu'Update Manager télécharge et maintient à jour. Une version peut être spécifiée pour chaque plate-forme prise en charge (par exemple, "Latest" ou dernière version pour Windows 2000 et supérieur).
<b>Administrateur système</b>	<p>Rôle préconfiguré disposant des droits complets d'administration des logiciels de sécurité Sophos sur le réseau et des rôles dans Enterprise Manager.</p> <p>Le rôle Administrateur système ne peut pas être supprimé ou voir ses droits ou son nom changés et le groupe Sophos Full Administrators Windows ne peut pas être supprimé de ce rôle. Les autres utilisateurs et groupes peuvent être ajoutés ou supprimés du rôle.</p>
<b>Administration déléguée</b>	Fonctionnalité qui vous permet de définir quels ordinateurs sont accessibles à l'utilisateur et quelles tâches il peut effectuer selon son rôle dans l'entreprise.
<b>Application potentiellement indésirable (PUA)</b>	Application non malveillante en soi mais dont la présence est généralement considérée comme inappropriée par la majorité des réseaux professionnels.
<b>Base de données</b>	Composant d'Enterprise Manager qui archive les détails sur les ordinateurs du réseau.
<b>Console d'administration</b>	Composant de Sophos Enterprise Manager qui vous permet de protéger et d'administrer les ordinateurs.
<b>Contrôle des périphériques</b>	Fonction pour réduire la perte accidentelle de données des stations de travail et restreindre l'introduction de logiciels depuis l'extérieur du réseau. Elle prend les mesures appropriées lorsqu'un utilisateur tente d'utiliser sur son poste un périphérique de stockage non autorisé ou un périphérique de réseau.
<b>Droit</b>	Série de permissions pour l'exécution de certaines tâches dans Enterprise Manager.
<b>Détection des comportements suspects</b>	Analyse dynamique du comportement de tous les programmes s'exécutant sur le système afin de détecter et de bloquer toute activité qui semble malveillante.
<b>Événement du tableau de bord</b>	Événement où un indicateur du tableau de bord dépasse le niveau critique. Une alerte par courriel générée lorsqu'un événement se produit sur le tableau de bord.

---

<b>Fichier suspect</b>	Fichier qui présente une combinaison de caractéristiques qui sont généralement, mais pas exclusivement, rencontrées dans les virus.
<b>Gestionnaire d'applications</b>	Boîte de dialogue qui vous permet d'autoriser ou de créer de nouvelles règles pour les applications qui ont été bloquées par le Sophos Client Firewall.
<b>Gestionnaire de mise à jour</b>	Voir <i>Sophos Update Manager</i> .
<b>Groupe</b>	Groupe d'ordinateurs administrés définis dans Sophos Enterprise Manager.
<b>HIPS (système de prévention des intrusions sur l'hôte)</b>	Technologie de sécurité pour assurer la protection contre les fichiers suspects, les virus non identifiés et tout comportement suspect.
<b>Indicateur de bon fonctionnement</b>	Terme générique utilisé pour les icônes décrivant l'état de sécurité d'une section ou d'un élément du tableau de bord, ou l'état global du réseau.
<b>Niveau critique</b>	Valeur qui déclenche le changement de l'état de sécurité d'un élément en Critique.
<b>Niveau d'alerte</b>	Valeur qui déclenche le changement de l'état de sécurité d'un élément en Avertissement.
<b>Niveau seuil</b>	Valeur qui déclenche le changement de l'état de sécurité d'un élément en Avertissement ou Critique.
<b>Nœud racine serveur</b>	Nœud principal de l'arborescence dans le volet <b>Groupes</b> , qui inclut le dossier <b>Non affectés</b> .
<b>Ordinateur administré</b>	Ordinateur sur lequel Remote Management System (RMS) est installé et sur lequel Sophos Enterprise Manager peut installer et mettre à jour les logiciels, et éditer des rapports.
<b>Ordinateur obsolète</b>	Ordinateur ne disposant pas des logiciels Sophos à jour.
<b>Protection antialtération</b>	Fonction qui empêche les programmes malveillants connus et les utilisateurs non autorisés (administrateurs locaux et utilisateurs avec peu d'expérience technique) de désinstaller les logiciels de sécurité de Sophos ou de les désactiver par le biais de l'interface Sophos Endpoint Security and Control.
<b>Protection Live Sophos</b>	Fonction qui utilise la technologie dans-le-nuage pour décider instantanément si un fichier suspect est une menace et prendre les mesures spécifiées dans la configuration du nettoyage antivirus de Sophos.
<b>Périphérique contrôlé</b>	Périphérique sujet au contrôle des périphériques.
<b>Périphérique exempté</b>	Périphérique explicitement exclu du contrôle des périphériques.

<b>Rôle</b>	Série de droits qui déterminent l'accès à Enterprise Manager.
<b>Serveur d'administration</b>	Composant de Sophos Enterprise Manager qui gère la mise à jour et les communications avec les ordinateurs en réseau.
<b>Sophos Update Manager (SUM)</b>	Programme qui télécharge les logiciels et les mises à jour de sécurité Sophos depuis le site Web de Sophos ou depuis un autre serveur de mise à jour dans les emplacements de mise à jour partagés.
<b>Stratégie</b>	Groupe de paramètres, par exemple, pour la mise à jour, appliqué à un groupe ou à des groupes d'ordinateurs.
<b>Tableau de bord</b>	Offre une visibilité immédiate de l'état de sécurité du réseau.
<b>Type de fichier véritable</b>	Type de fichier identifié par l'analyse de la structure d'un fichier par opposition à son extension. Cette méthode est plus fiable.

## 13 Support technique

Le support technique pour les produits Sophos est disponible 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](mailto: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.

## 14 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 la documentation peut être reproduite conformément aux termes de cette licence 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.

### **ACE™, TAO™, CIAO™, and CoSMIC™**

ACE<sup>1</sup>, TAO<sup>2</sup>, CIAO<sup>3</sup>, and CoSMIC<sup>4</sup> (henceforth referred to as “DOC software”) are copyrighted by Douglas C. Schmidt<sup>5</sup> and his research group<sup>6</sup> at Washington University<sup>7</sup>, University of California<sup>8</sup>, Irvine, and Vanderbilt University<sup>9</sup>, Copyright © 1993–2005, all rights reserved.

Since DOC software is open-source, free software, you are free to use, modify, copy, and distribute—perpetually and irrevocably—the DOC software source code and object code produced from the source, as well as copy and distribute modified versions of this software. You must, however, include this copyright statement along with code built using DOC software.

You can use DOC software in commercial and/or binary software releases and are under no obligation to redistribute any of your source code that is built using DOC software. Note, however, that you may not do anything to the DOC software code, such as copyrighting it yourself or claiming authorship of the DOC software code, that will prevent DOC software from being distributed freely using an open-source development model. You needn't inform anyone that you're using DOC software in your software, though we encourage you to let us<sup>10</sup> know so we can promote your project in the DOC software success stories<sup>11</sup>.

DOC software is provided as is with no warranties of any kind, including the warranties of design, merchantability, and fitness for a particular purpose, noninfringement, or arising from a course of dealing, usage or trade practice. Moreover, DOC software is provided with no support and without any obligation on the part of Washington University, UC Irvine, Vanderbilt University, their employees, or students to assist in its use, correction, modification, or enhancement. A number of companies<sup>12</sup> around the world provide commercial support for DOC software, however. DOC software is Y2K-compliant, as long as the underlying OS platform is Y2K-compliant.

Washington University, UC Irvine, Vanderbilt University, their employees, and students shall have no liability with respect to the infringement of copyrights, trade secrets or any patents by DOC software or any part thereof. Moreover, in no event will Washington University, UC Irvine, or Vanderbilt University, their employees, or students be liable for any lost revenue or profits or other special, indirect and consequential damages.

The ACE<sup>13</sup>, TAO<sup>14</sup>, CIAO<sup>15</sup>, and CoSMIC<sup>16</sup> web sites are maintained by the DOC Group<sup>17</sup> at the Institute for Software Integrated Systems (ISIS)<sup>18</sup> and the Center for Distributed Object Computing of Washington University, St. Louis<sup>19</sup> for the development of open-source software as part of the open-source software community<sup>20</sup>. By submitting comments, suggestions, code, code snippets, techniques (including that of usage), and algorithms, submitters acknowledge

that they have the right to do so, that any such submissions are given freely and unreservedly, and that they waive any claims to copyright or ownership. In addition, submitters acknowledge that any such submission might become part of the copyright maintained on the overall body of code, which comprises the DOC software. By making a submission, submitter agree to these terms. Furthermore, submitters acknowledge that the incorporation or modification of such submissions is entirely at the discretion of the moderators of the open-source DOC software projects or their designees.

The names ACE, TAO, CIAO, CoSMIC, Washington University, UC Irvine, and Vanderbilt University, may not be used to endorse or promote products or services derived from this source without express written permission from Washington University, UC Irvine, or Vanderbilt University. Further, products or services derived from this source may not be called ACE, TAO, CIAO, or CoSMIC nor may the name Washington University, UC Irvine, or Vanderbilt University appear in their names, without express written permission from Washington University, UC Irvine, and Vanderbilt University.

If you have any suggestions, additions, comments, or questions, please let me<sup>21</sup> know.

Douglas C. Schmidt<sup>22</sup>

### References

1. <http://www.cs.wustl.edu/~schmidt/ACE.html>
2. <http://www.cs.wustl.edu/~schmidt/TAO.html>
3. <http://www.dre.vanderbilt.edu/CIAO/>
4. <http://www.dre.vanderbilt.edu/cosmic/>
5. <http://www.dre.vanderbilt.edu/~schmidt/>
6. <http://www.cs.wustl.edu/~schmidt/ACE-members.html>
7. <http://www.wustl.edu/>
8. <http://www.uci.edu/>
9. <http://www.vanderbilt.edu/>
10. [mailto:doc\\_group@cs.wustl.edu](mailto:doc_group@cs.wustl.edu)
11. <http://www.cs.wustl.edu/~schmidt/ACE-users.html>
12. <http://www.cs.wustl.edu/~schmidt/commercial-support.html>
13. <http://www.cs.wustl.edu/~schmidt/ACE.html>
14. <http://www.cs.wustl.edu/~schmidt/TAO.html>
15. <http://www.dre.vanderbilt.edu/CIAO/>
16. <http://www.dre.vanderbilt.edu/cosmic/>
17. <http://www.dre.vanderbilt.edu/>
18. <http://www.isis.vanderbilt.edu/>
19. <http://www.cs.wustl.edu/~schmidt/doc-center.html>
20. <http://www.opensource.org/>
21. <mailto:d.schmidt@vanderbilt.edu>
22. <http://www.dre.vanderbilt.edu/~schmidt/>

### Apache

Les logiciels Sophos mentionnés dans le présent document peuvent inclure des programmes logiciels concédés en licence (ou en sous licence) à l'utilisateur selon les termes de la licence

Apache. Une copie du contrat de licence pour chacun des logiciels inclus est disponible sur <http://www.apache.org/licenses/LICENSE-2.0>.

### **Common Public License**

Les logiciels Sophos auxquels le présent document fait référence incluent ou peuvent inclure des programmes logiciels concédés en licence (ou en sous licence) à l'utilisateur selon les termes de la licence Common Public License (CPL), qui, entre autres droits, permettent à l'utilisateur d'avoir accès au code source. La licence CPL exige que pour tout logiciel concédé en licence sous les termes de la licence CPL, qui est distribuée sous un format de code objet, le code source soit aussi mis à disposition de ces utilisateurs sous un format de code objet. Pour chacun de ces logiciels couverts par la licence CPL, le code source est disponible sur commande par courrier postal envoyé à Sophos, par courrier électronique envoyé à [support@sophos.fr](mailto:support@sophos.fr) ou par Internet sur <http://www.sophos.fr/support/queries/enterprise.html>. Une copie du contrat de licence pour chacun des logiciels inclus est disponible sur <http://opensource.org/licenses/cpl1.0.php>

### **iMatix SFL**

This product uses parts of the iMatix SFL, Copyright © 1991-2000 iMatix Corporation <http://www.imatix.com>.

### **OpenSSL cryptographic toolkit**

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact [openssl-core@openssl.org](mailto:openssl-core@openssl.org).

### **OpenSSL license**

Copyright © 1998–2006 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:  

“This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)”
4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact [openssl-core@openssl.org](mailto:openssl-core@openssl.org).
5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

“This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit.

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

### **Original SSLeay license**

Copyright © 1995–1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscape’s SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young’s, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

“This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)”

The word “cryptographic” can be left out if the routines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

“This product includes software written by Tim Hudson (tjh@cryptsoft.com)”

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

## Index

### A

abonnement aux logiciels 55  
 abonnements 54  
   ajout 55  
   sélection 56  
 acceptation d'applications 83, 88, 90  
 accès à la console 19  
 Active Directory  
   importation depuis 28  
 activer  
   protection Web 70  
 adware 68  
 adwares/PUA  
   autoriser 69  
 affectation de stratégies 22, 26  
 ajout d'applications 83, 88  
 ajout d'ordinateurs 28  
 ajout d'ordinateurs dans des groupes 21  
 alertes 39, 121  
   abonnements 121  
   approuver 41  
   courriel 122  
   effacer 41  
   état du réseau 125  
   gestionnaire de mise à jour 42  
   informations sur les éléments détectés 41  
   résolution 40  
   traitement de 40  
 alertes d'abonnement 121  
 alertes de virus  
   courriel 122  
 alertes HIPS  
   courriel 122  
 alertes par courriel  
   antivirus et HIPS 122  
   état du réseau 125  
 alertes sur l'état du réseau 125  
 analyse comportementale runtime 64  
 antivirus 63  
 application de stratégies 22, 26  
 applications  
   acceptation 83, 88, 90  
   ajout 83, 88  
   blocage 91  
 applications potentiellement indésirables 68

approuver les alertes 41  
 approuver les erreurs 41  
 assistant de protection automatique  
   codes d'accès 34  
   sélection des fonctions 34  
 attribution d'un nouveau nom à des groupes 22  
 attribution d'un nouveau nom à des stratégies 26  
 autorisation  
   partage de fichiers et d'imprimantes 84  
   processus cachés 92  
   rawsockets 92  
   trafic du réseau local (LAN) 84  
 autorisation du partage de fichiers et d'imprimantes 84  
 autoriser  
   adwares/PUA 69  
   éléments suspects 66  
   site Web 71

### B

bande passante  
   limitation 57–58  
 blocage  
   applications 91  
   partage de fichiers et d'imprimantes 85  
 boutons de la barre d'outils 5

### C

chevaux de Troie 63  
 comportement suspect  
   blocage 64  
   détection 64  
 configuration 13  
   édition de rapports centralisée 108  
   stratégies 24  
 configuration du gestionnaire de mise à jour 47  
 configuration du pare-feu  
   exportation 110  
   importation 110  
 configuration du Tableau de bord 36  
 configurations secondaire, création 107  
 configurations, application 108  
 connexion intuitive selon l'emplacement  
   à propos de 106  
   configuration 106  
   utilisation de deux adaptateurs réseau 106  
 contrôle  
   exclusions 79

- contrôle (*suite*)
  - planifié 74
- contrôle de la mémoire système 78
- contrôle des ordinateurs 42
  - immédiatement 43
- contrôle des périphériques
  - exemption d'un périphérique d'une stratégie 116
  - sélection des types de périphériques 113
- Contrôle des périphériques
  - aperçu 111
  - blocage des périphériques 115
  - blocage du pont de réseau 112
  - détection des périphériques sans blocage 114
  - détection et blocage des périphériques 115
  - événements 112, 127
  - exemption d'un périphérique de toutes les stratégies 115
  - liste des périphériques exemptés 117
  - messagerie 124
  - périphériques contrôlés 112
- contrôle immédiat 43
- contrôle intégral du système 43
- contrôle planifié 73–74
  - exclusion des éléments de 74
- contrôle sur accès
  - à l'écriture 71
  - à la lecture 71
  - activer 72
  - au moment de renommer 71
  - désactiver 72
  - exclusion des éléments de 72
  - nettoyage 45
- contrôler maintenant 43
- copie
  - détails de l'ordinateur 143
  - données de la liste des ordinateurs 143
- création de groupes 20
- création de rapports 131
- création de stratégies 25

## D

- délai 148
- dépassement de la mémoire tampon 64
- désinfection 43
  - automatique 45
  - manuel 44
- désinfection automatique 45
- désinfection manuelle 44

- détails de l'ordinateur
  - copie 143
  - impression 144
- deux adaptateurs réseau
  - utilisation 106
- distribution des logiciels 49
- droits 16

## E

- échec de l'installation
  - Sophos Endpoint Security and Control 147
- Échec de l'installation de Sophos Endpoint Security and Control 147
- échec du nettoyage 150
- édition de rapports centralisée, configuration 108
- élément partiellement détecté 149
- éléments suspects
  - autoriser 66
  - permettre 66
  - pré-autoriser 66
- emplacement double 80, 106
- emplacements des fichiers d'amorce 35
- emplacements principaux, définition 107
- erreurs
  - approuver 41
  - effacer 41
- état du nettoyage 40
- événements 126
  - Contrôle des périphériques 127
  - exportation dans un fichier 130
  - pare-feu 128
  - protection antialtération 128
- exclusions 79
  - contrôle planifié 74
  - contrôle sur accès 72
- exécution d'un contrôle avec une priorité inférieure 79
- exécution de rapports 140
- exportation de rapports 141
- extensions 75

## F

- fichiers archive 77
- fichiers Macintosh
  - contrôle 76
- fichiers suspects 65
- filtrage des messages ICMP 95

**G**

- gestionnaire de mise à jour 47
  - alertes 42
  - configuration 47
  - conformité à la configuration 53
  - distribution des logiciels 49
  - journalisation 52
  - mise à jour 52
  - mise à jour automatique 52
  - partages réseau pris en charge 50
  - planification 51
  - sélection d'une source de mise 48
  - surveillance 53
  - visualisation de la configuration 47
- glossaire 152
- groupe Non affectés 20, 146
- groupes 19–20
  - ajout d'ordinateurs 21
  - attribution d'un nouveau nom 22
  - création 20
  - groupe Non affectés 20
  - importation depuis Active Directory 28
  - opération de couper-coller 22
  - stratégies utilisées 23
  - suppression 22
  - suppression d'ordinateurs 21

**H**

HIPS 63–64

**I**

- icônes 10
- icônes d'alertes 39
- importation d'ordinateurs
  - depuis le fichier 31
- impression
  - détails de l'ordinateur 144
  - données de la liste des ordinateurs 143
- impression de rapports 141
- interface utilisateur 4–5
  - vue Gestionnaires de mise à jour 11
  - vue Ordinateurs d'extrémité 9
- introduction 13
- itinérance 57

**J**

journalisation des événements 126

**L**

- liste des ordinateurs
  - copie de données depuis 143
  - impression de données depuis 143
- logiciels
  - abonnement à 55
  - sélection 49

**M**

- messagerie 121
  - bureau 124
  - SNMP 123
- messagerie de bureau 124
- messagerie des virus
  - bureau 124
  - SNMP 123
- messagerie HIPS
  - bureau 124
  - SNMP 123
- messagerie SNMP 123
- messages ICMP
  - filtrage 95
  - informations sur 95
- mise à jour
  - automatique 56
  - détails du proxy 57–58
  - immédiate 61
  - itinérance 57
  - journalisation 61
  - limitation de la bande passante 57–58
  - manuel 61
  - ordinateurs non à jour 61
  - planification 60
  - publication des logiciels sur un serveur Web 54
  - serveur principal 57
  - serveur secondaire 57–58
  - source d'installation initiale 60
  - source de mise à jour principale 57
  - source de mise à jour secondaire 57–58
- mise à jour automatique 56
- mise à jour immédiate 61
- mise à jour manuelle 61

- mode de fonctionnement, changement en interactif 87
  - mode interactif, à propos de 87
  - mode interactif, activation 87
  - mode non interactif, passage en 88
  - mode surveillance 82
  - modification des rôles 16
  - modification des stratégies 26
- N**
- nettoyage 40, 43
    - automatique 45
    - échec 150
    - manuel 44
  - nettoyage automatique 45
  - nettoyage manuel 44
  - nouvel utilisateur 19
- O**
- ordinateurs à jour
    - vérification 38
  - ordinateurs administrés 10
  - ordinateurs avec problèmes 38
  - ordinateurs non à jour 147
    - mise à jour 61
    - recherche 38
  - ordinateurs non administrés 146
  - ordinateurs non connectés 10
  - ordinateurs non protégés 38
  - ordinateurs protégés 36–37
  - outil de suppression
    - logiciels de sécurité tiers 33
  - outil de suppression des logiciels de sécurité tiers 33
- P**
- paramétrage d'une règle 101–102
  - paramétrage des règles globales 100, 102, 105
  - pare-feu
    - acceptation d'applications 83, 88, 90
    - activation 86
    - ajout d'applications 83, 88
    - ajout de sommes de contrôle 93
    - autorisation du partage de fichiers et d'imprimantes 84
    - configuration 80
    - configuration avancée 87
    - pare-feu (*suite*)
      - création d'une règle 85, 103
      - désactivation 86
      - événements 128
      - options avancées 87
    - partage d'imprimantes, autorisation 84
    - partage d'imprimantes, blocage 85
    - partage de fichiers et d'imprimantes
      - autorisation 84
    - partage de fichiers et d'imprimantes, autorisation 84
    - partage de fichiers et d'imprimantes, blocage 85
    - partage de fichiers, autorisation 84
    - partage de fichiers, blocage 85
    - partages réseau
      - pris en charge 50
    - partages réseau pris en charge 50
    - planification des mises à jour 51, 60
    - planification des rapports 140
    - pré-autoriser
      - éléments suspects 66
      - site Web 71
    - priorité de règle 97
    - priorité, contrôle 79
    - problèmes de connectivité 148
    - processus cachés, autorisation 92
    - protection antialtération
      - activation 119
      - aperçu 118
      - changement de mot de passe 120
      - désactivation 119
      - événements 118, 128
    - protection des ordinateurs
      - assistant de protection automatique 34
      - codes d'accès 34
      - conditions préalables requises 32
      - préparation de l'installation 32
      - sélection des fonctions 34
    - Protection Live Sophos
      - activation 67
      - aperçu 67
      - désactivation 67
      - technologie dans-le-nuage 67
    - protection Web 70
    - protection, vérifier 36
    - PUA 68
      - alertes régulières 149
      - effets secondaires 151
      - non détectée 149
    - publication des logiciels sur un serveur Web 54

**R**

## rapports

- affichage sous la forme d'un tableau 141
- alertes et événements par emplacement 136
- alertes et événements par heure 135
- alertes et événements par nom d'élément 134
- aperçu 131
- création 131
- événements par utilisateur 138
- exécution 140
- exportation 141
- hiérarchie des mises à jour 140
- historique des alertes et des événements 132
- impression 141
- mise en page 142
- non-conformité à la stratégie des systèmes d'extrémité 137
- non-conformité à la stratégie par heure 137
- planification 140
- protection des ordinateurs d'extrémité administrés 139
- protection des ordinateurs d'extrémité par heure 139
- récapitulatif des alertes 133

## rawsockets, autorisation 92

## recherche d'ordinateurs 28

- Active Directory 28

## recherche des ordinateurs

- avec Active Directory 29
- importation depuis un fichier 31
- par plage IP 30
- sur le réseau 29

## règle

- paramétrer 101–102

## règles globales

- paramètre 100, 102, 105

## règles globales par défaut

- information supplémentaires 98

## réseau protégé 36

## résolution des alertes

- état du nettoyage 40
- informations sur les éléments détectés 41
- mesures à prendre 40–41

## résolution des problèmes

- alertes à traiter 146
- contrôle sur accès 145
- délai 148

résolution des problèmes (*suite*)

- Échec de l'installation de Sophos Endpoint Security and Control 147
- élément partiellement détecté 149
- groupe Non affectés 146
- impossible de créer une nouvelle stratégie 147
- Linux 148
- Mac 147
- nettoyage 150
- option Créer une stratégie désactivée 147
- option Créer une stratégie grisée 147
- option Dupliquer une stratégie désactivée 147
- option Dupliquer une stratégie grisée 147
- ordinateurs non à jour 147
- ordinateurs non administrés 146
- pare-feu désactivé 145
- pare-feu non installé 145
- problèmes de connectivité 148
- PUA, alertes régulières 149
- PUA, effets secondaires 151
- PUA, non détectée 149
- virus, effets secondaires 150
- Windows 2000 ou supérieur 148

## rôles 15

- ajout d'utilisateurs et de groupes aux 16
- modification 16
- préconfigurés 15

## rôles d'utilisateur

- affichage 16

## rôles préconfigurés 15

## rootkits

- rechercher 77

**S**

## sélection d'abonnements 56

## sélection des logiciels 49

## serveur de mise à jour 47

## serveur principal 57

- changement des codes d'accès 58

## serveur secondaire 57–58

## signaux d'avertissement 10

## site Web

- autoriser 71
- permettre 71
- pré-autoriser 71

## sommes de contrôle 93

## Sophos Enterprise Manager 3

## Sophos Update Manager 47

## source d'installation initiale 60

source de mise à jour 48  
  alternative 57  
  principal 57  
  secondaire 57–58  
  serveur Web 54  
source de mise à jour alternative 57  
spywares 63  
stratégie antivirus et HIPS 63  
stratégies  
  affectation 22, 26  
  antivirus et HIPS 63  
  aperçu 23  
  application 22, 26–27  
  attribution d'un nouveau nom 26  
  configuration 24  
  création 25  
  modification 26  
  par défaut 23  
  quels groupes utilisent 27  
  suppression 27  
  vérification 27  
suppression d'ordinateurs depuis des groupes 21  
suppression d'un groupe 22  
suppression de stratégies 27  
système de prévention des intrusions sur l'hôte 64

## T

Tableau de bord  
  configuration 36

Tableau de bord (*suite*)  
  icônes d'état de la sécurité 8  
  volets 7  
technologie dans-le-nuage 67  
trafic du réseau local (LAN), autorisation 84  
traitement des alertes 40  
tri de la liste des ordinateurs  
  ordinateurs avec problèmes 38  
  ordinateurs non protégés 38  
types de fichiers contrôlés 75

## U

utilisation des abonnements 56

## V

vers 63  
virus 63  
Virus  
  effets secondaires 150  
virus Mac 76  
virus Macintosh 76  
vue Gestionnaires de mise à jour 11  
vue Ordinateurs d'extrémité 9  
  copie de données depuis 143  
  impression de données depuis 143