

# SOPHOS

## Sophos Endpoint Security and Control Aide

Version du produit : 9.0

Date du document : octobre 2009



## Table des matières

1 A propos de Sophos Endpoint Security and Control.....	3
2 A propos de la page d'accueil.....	4
3 Groupes Sophos.....	5
4 Utilisation de Sophos Anti-Virus.....	8
5 Utilisation de Sophos Device Control.....	41
6 Utilisation de Sophos Data Control.....	43
7 Utilisation de Sophos Client Firewall.....	45
8 Utilisation de Sophos AutoUpdate.....	71
9 Résolution des problèmes.....	74
10 Glossaire.....	81
11 Support technique.....	86
12 Copyright.....	87

# 1 A propos de Sophos Endpoint Security and Control

Sophos Endpoint Security and Control 9.0 est une suite intégrée de logiciels de sécurité.

**Sophos Anti-Virus** détecte et nettoie les virus, chevaux de Troie, vers et spywares, ainsi que les adwares et toutes autres applications potentiellement indésirables. La technologie HIPS (Host Intrusion Prevention System) protège votre ordinateur contre les fichiers suspects, les rootkits, les virus non identifiés et les comportements suspects.

**Sophos Application Control** bloque les applications non autorisées tels que les Voix sur IP, les messageries instantanées, les partages de fichiers et les logiciels de jeux.

**Sophos Device Control** bloque les périphériques de stockage externe non autorisés et les technologies de connexion sans fil.

**Sophos Data Control** empêche toute fuite accidentelle d'informations d'identification personnelles depuis les ordinateurs administrés.

**Sophos Client Firewall** empêche les vers, les chevaux de Troie et les spywares de dérober et de communiquer des informations sensibles et empêche également toute intrusion de pirates informatiques.

**Sophos AutoUpdate** vous offre la mise à jour en mode sans échec et régule la bande passante lors de la mise à jour avec des connexions réseau lentes.

## 2 A propos de la page d'accueil

La page d'**Accueil** apparaît dans le volet droit lorsque vous ouvrez la fenêtre **Sophos Endpoint Security and Control**. Elle vous permet de configurer et d'utiliser les logiciels.

Au cours de votre utilisation de Sophos Endpoint Security and Control, le contenu du volet de droite change. Pour retourner à la page d'**Accueil**, cliquez sur le bouton **Accueil** de la barre d'outils.

## 3 Groupes Sophos

### 3.1 A propos des groupes Sophos

Sophos Endpoint Security and Control restreint l'accès à certaines parties du logiciel aux membres de certains groupes Sophos.

Lorsque Sophos Endpoint Security and Control est installé, chaque utilisateur sur cet ordinateur est d'abord affecté à un groupe Sophos selon son groupe Windows.

Groupe Windows	Groupe Sophos
Administrateurs	SophosAdministrator
Super Utilisateurs	SophosPowerUser
Utilisateurs	SophosUser

Les utilisateurs qui ne sont pas affectés à un groupe Sophos, y compris les utilisateurs invités, peuvent uniquement effectuer les tâches suivantes :

- Contrôle sur accès
- Contrôle par clic droit

#### **SophosUsers**

Les SophosUsers peuvent effectuer les tâches ci-dessus et également les tâches suivantes :

- Ouvrir la fenêtre Sophos Endpoint Security and Control
- Paramétrer et exécuter des contrôles à la demande
- Configurer le contrôle par clic droit
- Gérer avec des droits limités, les éléments placés en quarantaine.
- Créer et configurer les règles du pare-feu

#### **SophosPowerUsers**

Les SophosPowerUsers ont les mêmes droits que les SophosUsers et disposent en plus des droits suivants :

- Privilèges plus étendus dans le Gestionnaire de quarantaine
- Accès au Gestionnaire d'autorisation

#### **SophosAdministrators**

Les SophosAdministrators peuvent utiliser et configurer toutes les parties de Sophos Endpoint Security and Control.

## 3.2 Ajout d'un utilisateur au groupe Sophos

Si vous êtes un administrateur de domaine ou un membre du groupe Administrateurs Windows sur cet ordinateur, vous pouvez changer le groupe Sophos auquel appartient un utilisateur. Généralement, cette opération a pour but de changer les droits d'accès de l'utilisateur à Sophos Endpoint Security and Control.

Pour ajouter un utilisateur au groupe Sophos :

1. Sous Windows, ouvrez Gestion de l'ordinateur.
2. Dans l'arborescence de la console, cliquez sur **Utilisateurs**.
3. Cliquez avec le bouton droit de la souris sur le compte de l'utilisateur et cliquez sur **Propriétés**.
4. Dans l'onglet **Membre de**, cliquez sur **Ajouter**.
5. Dans le champ **Entrez des noms séparés par des points-virgules ou choisissez à partir de la liste**, saisissez les noms de groupes Sophos :
  - SophosAdministrator
  - SophosPowerUser
  - SophosUser
6. Si vous souhaitez valider le nom du groupe Sophos, cliquez sur **Vérifier les noms**.

Lorsque l'utilisateur ouvrira une session sur l'ordinateur, ses droits d'accès à Sophos Endpoint Security and Control auront été modifiés.

### Remarques

- Pour ouvrir la fenêtre Gestion de l'ordinateur, cliquez sur **Démarrer** et cliquez ensuite sur **Panneau de configuration**. Cliquez deux fois sur **Outils d'administration** et cliquez deux fois sur **Gestion de l'ordinateur**.
- Pour supprimer l'utilisateur d'un groupe d'utilisateurs Sophos, dans l'onglet **Membre de**, sélectionnez le groupe dans **Membre de** et cliquez ensuite sur **Supprimer**.

## 3.3 Configuration des droits utilisateur pour le Gestionnaire de quarantaine

Si vous êtes un membre du groupe SophosAdministrator, vous pouvez configurer les droits utilisateur pour le Gestionnaire de quarantaine.

1. Dans le menu **Configurer**, pointez votre curseur sur **Antivirus** et cliquez sur **Droits utilisateur pour le gestionnaire de quarantaine**.

2. Sélectionnez le type d'utilisateurs qui va effectuer chaque type d'actions.

**Remarque :** à l'exception de l'option **Autoriser**, les droits que vous avez définis ici s'appliquent uniquement au **Gestionnaire de quarantaine**.

Option	Description
<b>Nettoyer les secteurs</b>	L'utilisateur peut nettoyer les secteurs de démarrage de disquette.
<b>Nettoyer les fichiers</b>	L'utilisateur peut nettoyer les documents et les programmes.
<b>Supprimer les fichiers</b>	L'utilisateur peut supprimer les fichiers infectés.
<b>Déplacer les fichiers</b>	L'utilisateur peut déplacer les fichiers infectés dans un autre dossier.
<b>Autoriser</b>	L'utilisateur autorise l'exécution d'éléments suspects, d'adwares et de PUA sur l'ordinateur.  Cette option s'applique au <b>Gestionnaire d'autorisation</b> et au <b>Gestionnaire de quarantaine</b> .

## 4 Utilisation de Sophos Anti-Virus

### 4.1 Différences entre le contrôle sur accès et le contrôle à la demande

Le **contrôle sur accès** est votre méthode principale de protection contre les virus et toutes autres menaces.

A chaque fois que vous accédez (copiez, enregistrez, déplacez, ou ouvrez) un fichier, Sophos Anti-Virus contrôle le fichier et lui accorde l'accès uniquement s'il ne représente aucune menace pour votre ordinateur ou si son utilisation a été autorisée.

En plus du contrôle sur accès, Sophos Anti-Virus vous propose différents types de **contrôle à la demande** pour vous assurer une protection renforcée.

Un contrôle à la demande est un contrôle que vous lancez. Vous pouvez contrôler tout ce que vous voulez que ce soit un seul fichier ou tout un ordinateur.

### 4.2 Contrôle sur accès

#### 4.2.1 Désactivation temporaire du contrôle sur accès

Si vous êtes un membre du groupe SophosAdministrator, vous pouvez avoir temporairement besoin, pour des raisons de maintenance ou de résolution des problèmes, de désactiver le pare-feu, puis de le réactiver. Vous pouvez désactiver la protection sur accès tout en continuant à exécuter des contrôles à la demande sur votre ordinateur.

Sophos Endpoint Security and Control conserve les paramètres que vous choisissez ici, même après le redémarrage de l'ordinateur. Si vous désactivez le contrôle sur accès, votre ordinateur reste sans protection jusqu'à ce vous réactiviez le contrôle sur accès.

1. Dans le menu **Configurer**, pointez votre curseur sur **Antivirus** et cliquez sur **Contrôle sur accès**.
2. Deselectionnez la case **Activer le contrôle sur accès pour cet ordinateur**.

#### 4.2.2 Spécification des extensions de fichier pour le contrôle sur accès

**Important :** si une console d'administration est utilisée pour administrer Sophos Endpoint Security and Control sur cet ordinateur, il se peut que vous perdiez tous les changements que vous avez effectués.

Vous pouvez spécifier les extensions de fichier à contrôler au cours du contrôle sur accès.

1. Dans le menu **Configurer**, pointez votre curseur sur **Antivirus** et cliquez sur **Contrôle sur accès**.

2. Cliquez sur l'onglet **Extensions** et paramétrez les options comme décrit ci-dessous.

#### **Contrôle de tous les fichiers**

Cliquez sur cette option pour activer le contrôle de tous les fichiers, quelles que soient leurs extensions.

#### **Me permettre de gérer exactement ce qui est contrôlé**

Cliquez sur cette option pour restreindre le contrôle aux fichiers ayant une extension particulière spécifiée dans la liste des extensions.



**Avertissement :** la liste des extensions inclut les types de fichiers que nous recommandons de contrôler. Comme expliqué ci-dessous, méfiez-vous lorsque vous modifiez la liste.

Pour ajouter une extension de nom de fichier dans la liste, cliquez sur **Ajouter**. Vous pouvez utiliser le caractère joker ? pour remplacer un caractère quelconque.

Pour supprimer une extension de la liste, sélectionnez l'extension et cliquez sur **Supprimer**.

Pour changer l'extension d'un fichier dans la liste, sélectionnez l'extension et cliquez sur **Modifier**.

Lorsque vous sélectionnez **Me permettre de gérer exactement ce qui est contrôlé**, l'option **Contrôler les fichiers sans extension** est sélectionnée par défaut. Pour désactiver le contrôle des fichiers sans extension, désélectionnez **Contrôler les fichiers sans extension**.

### 4.2.3 Configuration du contrôle sur accès

Pour ouvrir la boîte de dialogue des paramètres du contrôle sur accès :

- ❖ Dans le menu **Configurer**, pointez votre curseur sur **Antivirus** et cliquez sur **Contrôle sur accès**.
- [Contrôle dans les fichiers archive](#) à la page 21
- [Recherche des virus Mac](#) à la page 22
- [Contrôle de tous les fichiers](#) à la page 22
- [Recherche d'adwares et de PUA](#) à la page 22
- [Recherche des fichiers suspects](#) à la page 22
- [Réinitialisation des sommes de contrôle des fichiers contrôlés](#) à la page 23

### 4.2.4 Exclusion de fichiers, de dossiers ou de lecteurs du contrôle sur accès

**Important :** si une console d'administration est utilisée pour administrer Sophos Endpoint Security and Control sur cet ordinateur, il se peut que vous perdiez tous les changements que vous avez effectués.

Vous pouvez exclure des fichiers, des dossiers et des lecteurs du contrôle sur accès.

1. Dans le menu **Configurer**, pointez votre curseur sur **Antivirus** et cliquez sur **Contrôle sur accès**.

2. Cliquez sur l'onglet **Exclusions** et paramétrez les options comme décrit ci-dessous.

#### **Élément exclu**

Pour spécifier des éléments devant être exclus du contrôle, cliquez sur **Ajouter**. Dans la boîte de dialogue **Exclusion d'un élément**, spécifiez le type et le nom de l'élément à exclure. Reportez-vous à la section *Spécification des éléments exclus*.

Pour supprimer des éléments de la liste des éléments exclus, cliquez sur **Supprimer**.

Pour changer des éléments dans la liste des éléments exclus, cliquez sur **Modifier**.

#### **Spécification des éléments exclus**

Dans la boîte de dialogue **Exclusion d'un élément**, sélectionnez le **Type d'élément**.

Spécifiez le **Nom de l'élément** à l'aide du bouton **Parcourir** ou en saisissant dans la zone de texte.

**Remarque :** si vous travaillez sur une plate-forme 64 bits, le bouton **Parcourir** ne sera pas visible dans la boîte de dialogue **Élément exclu**.

D'autres détails sur la spécification des noms des éléments sont donnés ci-dessous.

##### ■ **Nom de fichier**

Si vous spécifiez seulement le nom d'un fichier, Sophos Anti-Virus exclut tous les fichiers portant ce nom, quelle que soit leur emplacement. Par exemple,

`fred.bmp`

entraîne l'exclusion par Sophos Anti-Virus de tous les fichiers appelés fred.bmp, quel que soit leur emplacement.

##### ■ **Chemin intégral**

Vous pouvez spécifier l'emplacement exact et le nom d'un fichier et Sophos Anti-Virus exclura seulement ce fichier-là. Le chemin peut inclure un lecteur ou un partage. Par exemple,

`C:\Divers\fred.bmp`

entraîne l'exclusion par Sophos Anti-Virus du fichier fred.bmp dans le dossier Divers présent sur le lecteur C:.

`\\Serveur1\Utilisateurs\Fred\Lettre.rtf`

entraîne l'exclusion par Sophos Anti-Virus du fichier Lettre.rtf présent dans le dossier Fred du partage Utilisateurs sur Serveur1.

Si vous ne spécifiez ni lecteur ni partage, Sophos Anti-Virus prend le chemin situé à la racine d'un lecteur ou d'un partage quelconque.

##### ■ **Chemin partiel**

Vous pouvez spécifier un lecteur ou un partage et Sophos Anti-Virus exclura l'intégralité de ce lecteur ou de ce partage ainsi que tout ce qui est situé au-dessous. Par exemple,

`A:`

entraîne l'exclusion par Sophos Anti-Virus de tout ce qui est présent sur le lecteur A:.

Vous pouvez spécifier un dossier et Sophos Anti-Virus exclura l'intégralité de ce dossier ainsi que tout ce qui est situé au-dessous. Par exemple,

```
D:\Outils\
```

entraîne l'exclusion par Sophos Anti-Virus de tout ce qui est présent dans le dossier Outils sur le lecteur D: et dans tous les sous-dossiers.

Vous pouvez spécifier un dossier et un nom de fichier et Sophos Anti-Virus exclura le dossier et le nom de fichier correspondants. Par exemple,

```
logs\log.txt
```

entraîne l'exclusion par Sophos Anti-Virus du fichier log.txt dans tout dossier appelés logs présent sur un lecteur ou sur un partage quelconque.

### Caractères joker

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.

### Plusieurs extensions de fichiers

Les noms de fichiers avec plusieurs extensions sont traités comme si la dernière extension était la véritable extension et le reste faisait partie du nom du fichier. Par exemple,

[nomfichier].[extension1].[extension2] signifie que le nom du fichier est [nomfichier].[extension1] et que l'extension est [extension2].

### Conventions d'appellation standard

Le nom de fichier ou le chemin est validé selon les conventions d'appellation standard (par exemple, un nom de dossier peut contenir des espaces mais ne peut pas contenir seulement des espaces).

## 4.2.5 Modification de la fréquence du contrôle sur accès

**Important :** si une console d'administration est utilisée pour administrer Sophos Endpoint Security and Control sur cet ordinateur, il se peut que vous perdiez tous les changements que vous avez effectués.

Vous pouvez préciser si Sophos Anti-Virus contrôle des fichiers lorsqu'ils sont ouverts, lorsqu'ils sont enregistrés ou lorsqu'ils sont renommés.

1. Dans le menu **Configurer**, pointez votre curseur sur **Antivirus** et cliquez sur **Contrôle sur accès**.

2. Cliquez sur l'onglet **Contrôle** et paramétrez les options comme décrit ci-dessous.

Pour spécifier que les fichiers doivent être contrôlés lorsqu'ils sont ouverts, sélectionnez **A la lecture**. Cette option est vivement recommandée.

Pour spécifier que les fichiers doivent être contrôlés lorsqu'ils sont enregistrés, sélectionnez **A l'écriture**.

Pour spécifier que les fichiers doivent être contrôlés lorsqu'ils sont renommés, sélectionnez **Au moment de renommer**.

## 4.2.6 Détection des comportements suspects et des dépassements de la mémoire tampon

**Important :** si une console d'administration est utilisée pour administrer Sophos Endpoint Security and Control sur cet ordinateur, il se peut que vous perdiez tous les changements que vous avez effectués.

Si vous êtes un membre du groupe SophosAdministrator, vous pouvez modifier les paramètres de détection des comportements suspects et des dépassements de la mémoire tampon :

1. Dans le menu **Configurer**, choisissez **Antivirus**, puis cliquez sur **Analyse comportementale runtime HIPS** pour afficher la boîte de dialogue **Analyse comportementale runtime HIPS**.
2. Pour activer ou désactiver la détection du comportement suspect, sélectionnez ou dessélectionnez **Détecter tout comportement suspect**, respectivement.

Pour activer ou désactiver la détection des dépassements de la mémoire tampon, sélectionnez ou dessélectionnez **Détecter tout dépassement de la mémoire tampon**, respectivement.

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

3. S'il s'agit d'une nouvelle installation de Sophos Anti-Virus sur cet ordinateur, les comportements suspects et dépassements de mémoire tampon sont *détectés* par défaut mais pas *bloqués*. S'il s'agit d'une mise à niveau, les comportements suspects et dépassements de mémoire tampon ne sont pas détectés par défaut.



**Avertissement :** nous vous recommandons d'exécuter Sophos Anti-Virus en mode détection seule pendant un moment et d'autoriser les programmes dont vous avez besoin avant d'activer le blocage automatique des comportements suspects et des dépassements de mémoire tampon. Cette approche vous évite de bloquer des programmes nécessaires à vos utilisateurs.

Pour activer le *blocage* des comportements suspects et des dépassements de la mémoire tampon ainsi que la *détection*, dessélectionnez la case **Alerter uniquement**.

## 4.2.7 A propos de la recherche des applications contrôlées

Une *application contrôlée* est une application interdite d'exécution sur votre ordinateur par la stratégie de sécurité de votre entreprise.

La recherche des applications contrôlées est activée ou désactivée par une console d'administration conformément à la stratégie de contrôle des applications et elle est incluse dans le cadre du contrôle à la demande.

Pour plus d'informations sur le contrôle sur accès, reportez-vous à la section [Différences entre le contrôle sur accès et le contrôle à la demande](#) à la page 8.

## 4.2.8 Désactivation de la recherche des applications contrôlées

**Important :** si une console d'administration est utilisée pour administrer Sophos Endpoint Security and Control sur cet ordinateur, il se peut que vous perdiez tous les changements que vous avez effectués.

Si la recherche des applications contrôlées est activée sur votre ordinateur, elle peut vous empêcher de désinstaller certaines applications. Si vous êtes un membre du groupe SophosAdministrator, vous pouvez désactiver temporairement la recherche des applications contrôlées sur cet ordinateur.

Pour désactiver la recherche des applications contrôlées :

1. Dans le menu **Configurer**, cliquez sur **Contrôle des applications**.
2. Dessélectionnez la case **Activer le contrôle sur accès**.

## 4.3 Contrôle à la demande

### 4.3.1 Types de contrôle à la demande

Un contrôle à la demande est un contrôle que vous lancez. Vous pouvez contrôler tout ce que vous voulez que ce soit un seul fichier ou tout un ordinateur.

Les types de contrôle à la demande suivants sont fournis avec Sophos Anti-Virus :

- Contrôle intégral de l'ordinateur
- Contrôle par clic droit
- Contrôle personnalisé

#### Contrôle intégral de l'ordinateur

Contrôle de tout votre ordinateur, y compris le secteur de démarrage et la mémoire système, à tout moment de votre choix.

- [Exécution d'un contrôle intégral de l'ordinateur](#) à la page 17

### Contrôle par clic droit

Contrôle d'un fichier, d'un dossier ou d'un lecteur dans Windows Explorer à tout moment de votre choix.

- [Exécution d'un contrôle par clic droit](#) à la page 17

### Contrôle personnalisé

Contrôle d'une série spécifique de fichiers ou de dossiers. Vous pouvez soit exécuter manuellement un contrôle personnalisé, soit le planifier pour qu'il s'exécute tout seul.

- [Exécution d'un contrôle personnalisé](#) à la page 20
- [Planification d'un contrôle personnalisé](#) à la page 19

## 4.3.2 Spécification des extensions de fichier pour le contrôle à la demande

**Important :** si une console d'administration est utilisée pour administrer Sophos Endpoint Security and Control sur cet ordinateur, il se peut que vous perdiez tous les changements que vous avez effectués.

Vous pouvez spécifier les extensions de fichier à contrôler au cours du contrôle à la demande.

1. Dans le menu **Configurer**, cliquez sur **Extensions et exclusions à la demande**.
2. Cliquez sur l'onglet **Extensions** et paramétrez les options comme décrit ci-dessous.

#### Contrôle de tous les fichiers

Cliquez sur cette option pour activer le contrôle de tous les fichiers, quelles que soient leurs extensions.

#### Me permettre de gérer exactement ce qui est contrôlé

Cliquez sur cette option pour restreindre le contrôle aux fichiers ayant une extension particulière spécifiée dans la liste des extensions.



**Avertissement :** la liste des extensions inclut les types de fichiers que nous conseillons de contrôler. Comme expliqué ci-dessous, méfiez-vous lorsque vous modifiez la liste.

Pour ajouter une extension de nom de fichier dans la liste, cliquez sur **Ajouter**. Vous pouvez utiliser le caractère joker ? pour remplacer un caractère quelconque.

Pour supprimer une extension de la liste, sélectionnez l'extension et cliquez sur **Supprimer**.

Pour changer l'extension d'un fichier dans la liste, sélectionnez l'extension et cliquez sur **Modifier**.

Lorsque vous sélectionnez **Me permettre de gérer exactement ce qui est contrôlé**, l'option **Contrôler les fichiers sans extension** est sélectionnée par défaut. Pour désactiver le contrôle des fichiers sans extension, désélectionnez **Contrôler les fichiers sans extension**.

### 4.3.3 Exclusion de fichiers, de dossiers ou de lecteurs du contrôle à la demande

**Important :** si une console d'administration est utilisée pour administrer Sophos Endpoint Security and Control sur cet ordinateur, il se peut que vous perdiez tous les changements que vous avez effectués.

Vous pouvez exclure des fichiers, des dossiers et des lecteurs du contrôle à la demande.

**Remarque :** la procédure décrite ci-dessous s'applique à *tous* les contrôles à la demande. Pour exclure des éléments d'un contrôle à la demande *particulier*, reportez-vous à la section [Création d'un contrôle personnalisé](#) à la page 18.

1. Dans le menu **Configurer**, pointez votre curseur sur **Antivirus** et cliquez sur **Extensions et exclusions à la demande**.
2. Cliquez sur l'onglet **Exclusions**. Paramétrez les options comme décrit ci-dessous.

#### Élément exclu

Pour spécifier des éléments devant être exclus du contrôle, cliquez sur **Ajouter**. Dans la boîte de dialogue **Exclusion d'un élément**, spécifiez le type et le nom de l'élément à exclure. Reportez-vous à la section *Spécification des éléments exclus*.

Pour supprimer des éléments de la liste des éléments exclus, cliquez sur **Supprimer**.

Pour changer des éléments dans la liste des éléments exclus, cliquez sur **Modifier**.

#### Spécification des éléments exclus

Dans la boîte de dialogue **Exclusion d'un élément**, sélectionnez le **Type d'élément**.

Spécifiez le **Nom de l'élément** à l'aide du bouton **Parcourir** ou en saisissant dans la zone de texte.

**Remarque :** si vous travaillez sur une plate-forme 64 bits, le bouton **Parcourir** ne sera pas visible dans la boîte de dialogue **Élément exclu**.

D'autres détails sur la spécification des noms des éléments sont donnés ci-dessous.

##### ■ Nom de fichier

Si vous spécifiez seulement le nom d'un fichier, Sophos Anti-Virus exclut tous les fichiers portant ce nom, quelle que soit leur emplacement. Par exemple,

`fred.bmp`

entraîne l'exclusion par Sophos Anti-Virus de tous les fichiers appelés fred.bmp, quel que soit leur emplacement.

##### ■ Chemin intégral

Vous pouvez spécifier l'emplacement exact et le nom d'un fichier et Sophos Anti-Virus exclura seulement ce fichier-là. Le chemin peut inclure un lecteur ou un partage. Par exemple,

`C:\Divers\fred.bmp`

entraîne l'exclusion par Sophos Anti-Virus du fichier fred.bmp dans le dossier Divers présent sur le lecteur C: .

```
\\Serveur1\Utilisateurs\Fred\Lettre.rtf
```

entraîne l'exclusion par Sophos Anti-Virus du fichier Lettre.rtf présent dans le dossier Fred du partage Utilisateurs sur Serveur1.

Si vous ne spécifiez ni lecteur ni partage, Sophos Anti-Virus prend le chemin situé à la racine d'un lecteur ou d'un partage quelconque.

### ■ Chemin partiel

Vous pouvez spécifier un lecteur ou un partage et Sophos Anti-Virus exclura l'intégralité de ce lecteur ou de ce partage ainsi que tout ce qui est situé au-dessous. Par exemple,

A :

entraîne l'exclusion par Sophos Anti-Virus de tout ce qui est présent sur le lecteur A: .

Vous pouvez spécifier un dossier et Sophos Anti-Virus exclura l'intégralité de ce dossier ainsi que tout ce qui est situé au-dessous. Par exemple,

```
D:\Outils\
```

entraîne l'exclusion par Sophos Anti-Virus de tout ce qui est présent dans le dossier Outils sur le lecteur D: et dans tous les sous-dossiers.

Vous pouvez spécifier un dossier et un nom de fichier et Sophos Anti-Virus exclura le dossier et le nom de fichier correspondants. Par exemple,

```
logs\log.txt
```

entraîne l'exclusion par Sophos Anti-Virus du fichier log.txt dans tout dossier appelés logs présent sur un lecteur ou sur un partage quelconque.

### Caractères joker

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.

### Plusieurs extensions de fichiers

Les noms de fichiers avec plusieurs extensions sont traités comme si la dernière extension était la véritable extension et le reste faisait partie du nom du fichier. Par exemple,

```
[nomfichier].[extension1].[extension2] signifie que le nom du fichier est [nomfichier].[extension1] et que l'extension est [extension2].
```

### Conventions d'appellation standard

Le nom de fichier ou le chemin est validé selon les conventions d'appellation standard (par exemple, un nom de dossier peut contenir des espaces mais ne peut pas contenir seulement des espaces).

#### 4.3.4 Exécution d'un contrôle intégral de l'ordinateur

**Remarque :** l'option **Contrôler cet ordinateur** ne contrôle pas les fichiers Mac stockés sur les ordinateurs Windows. Si vous souhaitez que Sophos Anti-Virus contrôle les fichiers exécutables Mac, vous devez paramétrer un contrôle à la demande personnalisé et activer le contrôle des fichiers Mac pour ce contrôle.

Pour plus d'informations sur les contrôles à la demande personnalisés, reportez-vous à la section [Création d'un contrôle personnalisé](#) à la page 18.

Pour plus d'informations sur le contrôle des fichiers Mac, reportez-vous à la section [Recherche des virus Mac](#) à la page 22.

Pour contrôler tout votre ordinateur, y compris le secteur de démarrage et la mémoire système :

- ❖ Sur la page d'**Accueil**, sous **Antivirus et HIPS**, cliquez sur **Contrôler cet ordinateur**.  
Pour plus d'informations sur la page d'**Accueil**, reportez-vous à la section [A propos de la page d'accueil](#) à la page 4.

Une boîte de dialogue de progression ainsi que le **Récapitulatif d'activité** apparaissent dans la fenêtre **Sophos Endpoint Security and Control**.

Si des menaces ou des applications contrôlées sont trouvées, cliquez sur **Plus** et reportez-vous à la section *Gestion des éléments en quarantaine*.

#### 4.3.5 Configurer le contrôle par clic droit

**Important :** si une console d'administration est utilisée pour administrer Sophos Endpoint Security and Control sur cet ordinateur, vous ne perdrez *aucun* changement que vous avez effectué.

- ❖ Dans le menu **Configurer**, pointez votre curseur sur **Antivirus** et cliquez sur **Contrôle par clic droit**.
  - [Contrôle dans les fichiers archive](#) à la page 21
  - [Recherche des virus Mac](#) à la page 22
  - [Contrôle de tous les fichiers](#) à la page 22
  - [Recherche d'adwares et de PUA](#) à la page 22
  - [Recherche des fichiers suspects](#) à la page 22

#### 4.3.6 Exécution d'un contrôle par clic droit

Vous pouvez contrôler les fichiers, les dossiers et les lecteurs depuis l'Explorateur Windows ou du bureau en exécutant un contrôle par clic droit.

1. A l'aide de l'Explorateur Windows, ou sur le bureau, sélectionnez le fichier, le dossier ou le lecteur de disque dur que vous voulez contrôler.  
Vous pouvez sélectionner plusieurs fichiers et dossiers.
2. Cliquez avec le bouton droit de la souris sur la sélection et cliquez sur **Contrôler avec Sophos Anti-Virus**.

Si des menaces ou des applications contrôlées sont trouvées, cliquez sur **Plus** et reportez-vous à la section *Gestion des éléments en quarantaine* de ce fichier d'Aide.

## 4.4 Contrôles personnalisés





### 4.4.1 Création d'un contrôle personnalisé

1. Sur la page d'**Accueil**, sous **Antivirus et HIPS**, cliquez sur **Contrôles**.  
Pour plus d'informations sur la page d'**Accueil**, reportez-vous à la section [A propos de la page d'accueil](#) à la page 4.
2. Cliquez sur **Paramétrer un nouveau contrôle**.
3. Dans la zone de texte **Nom du contrôle**, saisissez un nom de contrôle.
4. Dans le volet **Éléments à contrôler**, sélectionnez les lecteurs et les dossiers que vous souhaitez contrôler. Pour cela, sélectionnez la case à cocher située à gauche de chaque lecteur ou dossier. Pour en savoir plus sur les icônes qui apparaissent dans les cases à cocher, reportez-vous à la section [Représentation des éléments à contrôler](#) à la page 18.  
**Remarque :** les lecteurs ou dossiers non disponibles (parce qu'ils sont hors connexion ou supprimés) sont affichés avec une police de caractères barrés. Ils sont supprimés du volet **Éléments à contrôler** lorsqu'ils sont désélectionnés ou si la sélection de leur lecteur ou dossier(s) parent a été modifiée.
5. Pour configurer davantage le contrôle, cliquez sur **Configurer ce contrôle** (pour plus d'informations, reportez-vous à la section [Configuration d'un contrôle personnalisé](#) à la page 19.)
6. Cliquez sur **Enregistrer** pour enregistrer le contrôle ou sur **Enregistrer et démarrer** pour enregistrer et exécuter le contrôle.

### 4.4.2 Représentation des éléments à contrôler

Dans le volet **Éléments à contrôler**, différentes icônes apparaissent dans la case à cocher près de chaque élément (unité ou dossier), en fonction des éléments qui seront contrôlés. Ces icônes apparaissent ci-dessous avec des explications.

Icône	Explication
<input type="checkbox"/>	L'élément et tous les sous-éléments <i>ne sont pas</i> sélectionnés pour le contrôle.
<input checked="" type="checkbox"/>	L'élément et tous les sous-éléments <i>sont</i> sélectionnés pour le contrôle.

Icône	Explication
	L'élément est partiellement sélectionné : l'élément n'est pas sélectionné, mais certains sous-éléments sont sélectionnés pour le contrôle.
	L'élément et tous les sous-éléments sont exclus de ce contrôle donné.
	L'élément est partiellement exclu : l'élément n'est pas sélectionné, mais certains sous-éléments sont exclus de ce contrôle particulier.
	L'élément et tous les sous-éléments sont exclus de tous les contrôles à la demande à cause d'une exclusion à la demande qui a été paramétrée. Pour plus d'informations, reportez-vous à la section <a href="#">Exclusion de fichiers, de dossiers ou de lecteurs du contrôle sur accès</a> à la page 9.

### 4.4.3 Configuration d'un contrôle personnalisé

1. Sur la page d'**Accueil**, sous **Antivirus et HIPS**, cliquez sur **Contrôles**.  
Pour plus d'informations sur la page d'**Accueil**, reportez-vous à la section [A propos de la page d'accueil](#) à la page 4.
2. Dans la liste des **Contrôles disponibles**, sélectionnez le contrôle que vous souhaitez modifier et cliquez sur **Modifier**.
3. Cliquez sur **Configurer ce contrôle**.
  - [Contrôle dans les fichiers archive](#) à la page 21
  - [Recherche des virus Mac](#) à la page 22
  - [Contrôle de tous les fichiers](#) à la page 22
  - [Recherche d'adwares et de PUA](#) à la page 22
  - [Recherche des fichiers suspects](#) à la page 22
  - [Contrôle à la recherche des rootkits](#) à la page 23

### 4.4.4 Planification d'un contrôle personnalisé

Si vous êtes un membre du groupe SophosAdministrator, vous pouvez planifier un contrôle personnalisé ou consulter et modifier les contrôles planifiés créés par d'autres utilisateurs.

1. Sur la page d'**Accueil**, sous **Antivirus et HIPS**, cliquez sur **Contrôles**.  
Pour plus d'informations sur la page d'**Accueil**, reportez-vous à la section [A propos de la page d'accueil](#) à la page 4.
2. Dans la liste des **Contrôles disponibles**, sélectionnez le contrôle que vous souhaitez modifier et cliquez sur **Modifier**.
3. Cliquez sur **Planifier ce contrôle**.

4. Dans la boîte de dialogue **Planification du contrôle**, sélectionnez **Activer la planification**.  
Sélectionnez le(s) jour(s) d'exécution du contrôle.  
Ajoutez la ou les heures en cliquant sur **Ajouter**.  
Si nécessaire, supprimez ou modifiez une heure en la sélectionnant et en cliquant respectivement sur **Supprimer** ou **Modifier**.
5. Saisissez le *nom utilisateur* et le *mot de passe*. Assurez-vous que le mot de passe soit bien rempli.  
Le contrôle planifié s'exécute avec les droits d'accès de cet utilisateur.

#### 4.4.5 Exécution d'un contrôle personnalisé

**Remarque :** vous pouvez exécuter manuellement des contrôles personnalisés planifiés. Les contrôles planifiés apparaissent dans la liste **Contrôles disponibles** avec l'icône d'une horloge.

1. Sur la page d'**Accueil**, sous **Antivirus et HIPS**, cliquez sur **Contrôles**.  
Pour plus d'informations sur la page d'**Accueil**, reportez-vous à la section [A propos de la page d'accueil](#) à la page 4.
2. Dans la liste des **Contrôles disponibles**, sélectionnez le contrôle que vous souhaitez exécuter et cliquez sur **Démarrer**.  
Une boîte de dialogue de progression ainsi que le **Récapitulatif d'activité** apparaissent dans la fenêtre Sophos Endpoint Security and Control.

Si des menaces ou des applications contrôlées sont trouvées, cliquez sur **Plus** et reportez-vous à la section *Gestion des éléments en quarantaine*.

#### 4.4.6 Attribution d'un nouveau nom à un contrôle personnalisé

1. Sur la page d'**Accueil**, sous **Antivirus et HIPS**, cliquez sur **Contrôles**.  
Pour plus d'informations sur la page d'**Accueil**, reportez-vous à la section [A propos de la page d'accueil](#) à la page 4.
2. Dans la liste des **Contrôles disponibles**, sélectionnez le contrôle que vous souhaitez modifier et cliquez sur **Modifier**.
3. Dans la zone de texte **Nom du contrôle**, saisissez le nouveau nom du contrôle.

#### 4.4.7 Suppression d'un contrôle personnalisé

1. Sur la page d'**Accueil**, sous **Antivirus et HIPS**, cliquez sur **Contrôles**.  
Pour plus d'informations sur la page d'**Accueil**, reportez-vous à la section [A propos de la page d'accueil](#) à la page 4.
2. Dans la liste des **Contrôles disponibles**, sélectionnez le contrôle que vous souhaitez supprimer, puis cliquez sur **Supprimer**.

## 4.4.8 Visualisation du journal du contrôle personnalisé

1. Sur la page d'**Accueil**, sous **Antivirus et HIPS**, cliquez sur **Contrôles**.  
Pour plus d'informations sur la page d'**Accueil**, reportez-vous à la section [A propos de la page d'accueil](#) à la page 4.
2. Dans la liste des **Contrôles disponibles**, cliquez sur **Récapitulatif** pour ce contrôle personnalisé.
3. Dans la boîte de dialogue **Récapitulatif**, cliquez sur le lien présent en bas.

Depuis la page du journal, vous pouvez copier le journal dans le Presse-papiers, l'envoyer par courriel ou l'imprimer.

Pour rechercher un texte spécifique dans le journal, cliquez sur **Rechercher** et saisissez le texte que vous souhaitez rechercher.

## 4.5 Options de contrôle supplémentaires

### 4.5.1 Contrôle dans les fichiers archive

**Important :** si une console d'administration est utilisée pour administrer Sophos Endpoint Security and Control sur cet ordinateur, il se peut que vous perdiez tous les changements que vous avez effectués.

**Remarque :** nous vous recommandons de ne pas activer cette option, pour les raisons suivantes :

- Le contrôle dans les fichiers archive ralentit énormément le contrôle.
- Que vous activiez cette option ou non, lorsque vous ouvrez un fichier extrait du fichier archive, le fichier extrait est contrôlé.
- Que vous activiez cette option ou non, les fichiers compressés avec des utilitaires de compression dynamique (PKLite, LZEXE et Diet) sont aussi contrôlés.

Vous pouvez, par contre, activer l'option afin que le contenu d'une archive ou d'un fichier compressé soit contrôlé avant qu'il ne soit téléchargé ou envoyé par courriel depuis votre ordinateur.

Pour contrôler dans les fichiers archive :

1. Ouvrez la boîte de dialogue des paramètres de contrôle pour le type de contrôle que vous voulez configurer. (reportez-vous à la section [Ouverture de la boîte de dialogue des paramètres de contrôle](#) à la page 28).
2. Sur l'onglet **Options**, sélectionnez la case à cocher **Contrôler dans les fichiers archive**.

## 4.5.2 Recherche des virus Mac

**Important :** si une console d'administration est utilisée pour administrer Sophos Endpoint Security and Control sur cet ordinateur, il se peut que vous perdiez tous les changements que vous avez effectués.

Vous pouvez permettre à Sophos Anti-Virus de contrôler les fichiers Mac stockés sur les ordinateurs Windows.

1. Ouvrez la boîte de dialogue des paramètres de contrôle pour le type de contrôle que vous voulez configurer (reportez-vous à la section [Ouverture de la boîte de dialogue des paramètres de contrôle](#) à la page 28).
2. Sur l'onglet **Options**, sélectionnez la case à cocher **Rechercher les virus Macintosh**.

## 4.5.3 Contrôle de tous les fichiers

**Important :** si une console d'administration est utilisée pour administrer Sophos Endpoint Security and Control sur cet ordinateur, il se peut que vous perdiez tous les changements que vous avez effectués.

Vous pouvez permettre à Sophos Anti-Virus de contrôler tous les fichiers, toutefois, ceci affectera les performances de l'ordinateur.

1. Ouvrez la boîte de dialogue des paramètres de contrôle pour le type de contrôle que vous voulez configurer (reportez-vous à la section [Ouverture de la boîte de dialogue des paramètres de contrôle](#) à la page 28).
2. Sur l'onglet **Options**, sélectionnez la case à cocher **Contrôler tous les fichiers**.

## 4.5.4 Recherche d'adwares et de PUA

**Important :** si une console d'administration est utilisée pour administrer Sophos Endpoint Security and Control sur cet ordinateur, il se peut que vous perdiez tous les changements que vous avez effectués.

1. Ouvrez la boîte de dialogue des paramètres de contrôle pour le type de contrôle que vous voulez configurer (reportez-vous à la section [Ouverture de la boîte de dialogue des paramètres de contrôle](#) à la page 28).
2. Sur l'onglet **Options**, sélectionnez la case à cocher **Rechercher les adwares et PUA**.

## 4.5.5 Recherche des fichiers suspects

**Important :** si une console d'administration est utilisée pour administrer Sophos Endpoint Security and Control sur cet ordinateur, il se peut que vous perdiez tous les changements que vous avez effectués.

Un *fichier suspect* est un fichier qui comporte une combinaison de caractéristiques généralement, mais pas exclusivement, trouvées dans les virus.

Pour rechercher les fichiers suspects :

1. Ouvrez la boîte de dialogue des paramètres de contrôle pour le type de contrôle que vous voulez configurer. (reportez-vous à la section [Ouverture de la boîte de dialogue des paramètres de contrôle](#) à la page 28).
2. Sur l'onglet **Options**, sélectionnez la case à cocher **Rechercher les fichiers suspects (HIPS)**.

#### 4.5.6 Contrôle à la recherche des rootkits

**Important :** si une console d'administration est utilisée pour administrer Sophos Endpoint Security and Control sur cet ordinateur, il se peut que vous perdiez tous les changements que vous avez effectués.

Si vous êtes membre du groupe SophosAdministrator, le contrôle à la recherche des rootkits est toujours exécuté lorsque vous effectuez un contrôle intégral de l'ordinateur.

Vous pouvez aussi effectuer un contrôle à la recherche des rootkits dans le cadre d'un contrôle personnalisé.

Pour effectuer un contrôle à la recherche des rootkits :

1. Sur la page d'**Accueil**, sous **Antivirus et HIPS**, cliquez sur **Contrôles**.  
Pour plus d'informations sur la page d'**Accueil**, reportez-vous à la section [A propos de la page d'accueil](#) à la page 4.
2. Dans la liste des **Contrôles disponibles**, sélectionnez le contrôle que vous souhaitez modifier et cliquez sur **Modifier**.
3. Cliquez sur **Configurer ce contrôle**.
4. Sur l'onglet **Options**, sélectionnez la case à cocher **Rechercher les rootkits**.

#### 4.5.7 Réinitialisation des sommes de contrôle des fichiers contrôlés

La liste des sommes de contrôle des fichiers contrôlés est réinitialisée lorsqu'une mise à jour de Sophos Anti-Virus se produit ou lorsque vous redémarrez votre ordinateur. La liste est alors reconstruite avec de nouvelles données à mesure que les fichiers sont contrôlés par Sophos Anti-Virus.

Vous pouvez réinitialiser la liste des sommes de contrôle des fichiers contrôlés depuis Sophos Endpoint Security and Control si vous ne voulez pas redémarrer votre ordinateur.

Pour réinitialiser les sommes de contrôle des fichiers contrôlés :

1. Dans le menu **Configurer**, pointez votre curseur sur **Antivirus** et cliquez sur **Contrôle sur accès**.
2. Sur l'onglet **Options**, cliquez sur **Vider la mémoire cache**.

## 4.6 Configuration des alertes

### 4.6.1 Configuration de la messagerie de bureau pour l'antivirus

**Important :** si une console d'administration est utilisée pour administrer Sophos Endpoint Security and Control sur cet ordinateur, il se peut que vous perdiez tous les changements que vous avez effectués.

Pour permettre à Sophos Anti-Virus d'afficher les messages sur le bureau à la découverte d'une menace, procédez ainsi. Ceci s'applique seulement au contrôle sur accès.

1. Dans le menu **Configurer**, pointez votre curseur sur **Antivirus** et cliquez sur **Messagerie**.
2. Dans la boîte de dialogue **Messagerie**, cliquez sur l'onglet **Messagerie de bureau**. Paramétrez les options comme décrit ci-dessous.

#### Activer la messagerie de bureau

Sélectionnez cette option pour permettre à Sophos Anti-Virus d'afficher les messages sur le bureau à la découverte d'une menace.

#### Messages à envoyer

Sélectionnez les événements pour lesquels vous souhaitez que Sophos Anti-Virus envoie des messages sur le bureau.

#### Message défini par l'utilisateur

Dans cette zone de texte, vous pouvez saisir un message qui sera ajouté à la fin du message standard.

### 4.6.2 Configuration de l'alerte par courriel pour l'antivirus

**Important :** si une console d'administration est utilisée pour administrer Sophos Endpoint Security and Control sur cet ordinateur, il se peut que vous perdiez tous les changements que vous avez effectués.

Pour permettre à Sophos Anti-Virus d'envoyer des alertes par courriel en cas de découverte d'une menace ou d'erreur, procédez ainsi : Cette opération s'applique aux contrôles sur accès, à la demande et par clic droit.

1. Dans le menu **Configurer**, pointez votre curseur sur **Antivirus** et cliquez sur **Messagerie**.

2. Dans la boîte de dialogue **Messagerie**, cliquez sur l'onglet **Alertes par courriel**. Paramétrez les options comme décrit ci-dessous.

#### Activer les alertes par courriel

Sélectionnez cette option pour permettre à Sophos Anti-Virus d'envoyer des alertes par courriel.

#### Messages à envoyer

Sélectionnez les événements pour lesquels vous souhaitez que Sophos Anti-Virus envoie des alertes par courriel. Les **erreurs de contrôle** incluent des instances lorsque l'accès à un élément que Sophos Anti-Virus tente de contrôler lui est refusé.

Sophos Anti-Virus n'envoie pas d'alertes par courriel pour les menaces détectées par le contrôle des pages web car les menaces ne sont pas téléchargées sur votre ordinateur. C'est la raison pour laquelle aucune mesure n'est nécessaire.

#### 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 **Modifier** pour changer l'adresse électronique que vous avez ajoutée.

#### Configurer SMTP

Cliquez sur cette option pour changer les paramètres du serveur SMTP et la langue des alertes par courriel (reportez-vous au tableau ci-dessous).

Configuration des paramètres SMTP	
<b>Serveur SMTP</b>	Dans la zone de texte, saisissez le nom de l'hôte ou l'adresse IP du serveur SMTP. Cliquez sur <b>Tester</b> pour tester si la connexion au serveur SMTP peut être effectuée (ceci n'envoie <i>pas</i> de courriel de test).
<b>Adresse 'expéditeur' SMTP</b>	Dans la zone de texte, saisissez une adresse électronique à laquelle les messages renvoyés et les rapports de non-distribution peuvent être envoyés.
<b>Adresse 'réponse' SMTP</b>	Lorsque les alertes par courriel sont envoyées depuis une boîte aux lettres automatique, vous pouvez saisir dans la zone de texte une adresse électronique à laquelle les réponses aux alertes par courriel peuvent être envoyées.
<b>Langue</b>	Cliquez sur la flèche du menu déroulant et sélectionnez la langue dans laquelle les alertes par courriel doivent être envoyées.

### 4.6.3 Configuration de la messagerie SNMP pour l'antivirus

**Important :** si une console d'administration est utilisée pour administrer Sophos Endpoint Security and Control sur cet ordinateur, il se peut que vous perdiez tous les changements que vous avez effectués.

Pour permettre à Sophos Anti-Virus d'envoyer des messages SNMP en cas de découverte d'une menace ou d'erreur, procédez ainsi : Cette opération s'applique aux contrôles sur accès, à la demande et par clic droit.

1. Dans le menu **Configurer**, pointez votre curseur sur **Antivirus** et cliquez sur **Messagerie**.
2. Dans la boîte de dialogue **Messagerie**, cliquez sur l'onglet **Messagerie SNMP**. Paramétrez les options comme décrit ci-dessous.

#### **Activer la messagerie SNMP**

Sélectionnez cette option pour permettre à Sophos Anti-Virus d'envoyer des messages SNMP.

#### **Messages à envoyer**

Sélectionnez les événements pour lesquels vous souhaitez que Sophos Anti-Virus envoie des messages SNMP. Les **erreurs de contrôle** incluent des instances lorsque l'accès à un élément que Sophos Anti-Virus tente de contrôler lui est refusé.

Sophos Anti-Virus n'envoie pas de messages SNMP pour les menaces détectées par le contrôle des pages web car les menaces ne sont pas téléchargées sur votre ordinateur. C'est la raison pour laquelle aucune mesure n'est nécessaire.

#### **Destination de déroutement SNMP**

Dans la zone de texte, saisissez l'adresse IP ou le nom de l'ordinateur auquel les alertes sont envoyées.

#### **Nom de la communauté SNMP**

Dans la zone de texte, saisissez le nom de la communauté SNMP.

#### **Tester**

Cliquez sur cette option pour envoyer un message SNMP test à la destination de déroutement SNMP que vous avez spécifiée.

### 4.6.4 Configuration de la journalisation des événements antivirus

Pour permettre à Sophos Anti-Virus d'ajouter des alertes dans le journal des événements Windows 2000 ou supérieur lors de la découverte d'une menace ou en cas d'erreur, procédez ainsi : Cette opération s'applique aux contrôles sur accès, à la demande et par clic droit.

1. Dans le menu **Configurer**, pointez votre curseur sur **Antivirus** et cliquez sur **Messagerie**.

2. Dans la boîte de dialogue **Messagerie**, cliquez sur l'onglet **Journal des événements**. Paramétrez les options comme décrit ci-dessous.

#### **Activer la journalisation des événements**

Sélectionnez cette option pour permettre à Sophos Anti-Virus d'envoyer des messages dans le journal des événements Windows.

#### **Messages à envoyer**

Sélectionnez les événements pour lesquels vous souhaitez que Sophos Anti-Virus envoie des messages. Les **erreurs de contrôle** incluent des instances lorsque l'accès à un élément que Sophos Anti-Virus tente de contrôler lui est refusé.

Sophos Anti-Virus n'envoie pas de messages pour les menaces détectées par le contrôle des pages web car les menaces ne sont pas téléchargées sur votre ordinateur. C'est la raison pour laquelle aucune mesure n'est nécessaire.

## **4.7 Journal du contrôle**

### **4.7.1 Configuration du journal du contrôle**

Le journal du contrôle de cet ordinateur est archivé à l'emplacement suivant :

```
C:\Documents and Settings\All Users\Application  
Data\Sophos\Sophos  
Anti-Virus\logs\SAV.txt
```

1. Dans le menu **Configurer**, pointez votre curseur sur **Antivirus** et cliquez sur **Journalisation**.
2. Dans la boîte de dialogue **Configuration de la journalisation pour cet ordinateur**, définissez les options comme décrit ci-dessous.

#### **Niveau de journalisation**

Pour empêcher toute journalisation, cliquez sur **Aucun**. Pour journaliser un résumé des informations, les messages d'erreur et ainsi de suite, cliquez sur **Normal**. Pour journaliser la plupart des informations, y compris les fichiers contrôlés, les principales étapes d'un contrôle, et ainsi de suite, cliquez sur **Détaillé**.

#### **Journalisation de l'archivage**

Pour activer l'archivage mensuel du fichier journal, sélectionnez **Activer l'archivage**. Les fichiers archive sont stockés dans le même dossier que le fichier journal. Sélectionnez le **Nombre de fichiers archive** à stocker avant que le plus ancien ne soit supprimé. Sélectionnez **Compresser le journal** pour réduire la taille du fichier journal.

### **4.7.2 Visualisation du journal du contrôle**

- ❖ Sur la page d'Accueil, sous **Antivirus et HIPS**, cliquez sur **Voir le journal de l'antivirus et HIPS**.

Pour plus d'informations sur la page d'**Accueil**, reportez-vous à la section [A propos de la page d'accueil](#) à la page 4.

Depuis la page du journal, vous pouvez copier le journal dans le Presse-papiers, l'envoyer par courriel ou l'imprimer.

Pour rechercher un texte spécifique dans le journal, cliquez sur **Rechercher** et saisissez le texte que vous souhaitez rechercher.

## 4.8 Nettoyage

### 4.8.1 A propos du nettoyage

Le nettoyage élimine les menaces présentes sur votre ordinateur en effectuant l'une des opérations suivantes :

- Suppression d'un virus dans un fichier ou dans un secteur de démarrage.
- Déplacement ou suppression d'un fichier suspect
- Suppression d'un élément d'adware ou de PUA

Le nettoyage n'annule pas les actions que la menace a déjà exécutées.

Le nettoyage des documents ne répare pas les modifications que le virus a apportées au document.

Le nettoyage des programmes doit uniquement être utilisé en guise de mesure provisoire. Remplacez ensuite les programmes nettoyés à l'aide des disques originaux ou d'une sauvegarde saine.

Le nettoyage n'est pas disponible pour les menaces détectées par le contrôle des pages web car ces menaces ne sont pas téléchargées sur votre ordinateur. Dans ce cas, aucune mesure n'est nécessaire.

### 4.8.2 Ouverture de la boîte de dialogue des paramètres de contrôle

Pour ouvrir la boîte de dialogue des paramètres du **contrôle par clic droit** :

- Dans le menu **Configurer**, pointez votre curseur sur **Antivirus** et cliquez sur **Contrôle par clic droit**.

Pour ouvrir la boîte de dialogue des paramètres du **contrôle personnalisé** :

1. Sur la page d'**Accueil**, sous **Antivirus et HIPS**, cliquez sur **Contrôles**.

Pour plus d'informations sur la page d'**Accueil**, reportez-vous à la section [A propos de la page d'accueil](#) à la page 4.

2. Dans la liste des **Contrôles disponibles**, sélectionnez le contrôle que vous souhaitez modifier et cliquez sur **Modifier**.
3. Cliquez sur **Configurer ce contrôle**.

Pour ouvrir la boîte de dialogue des paramètres du **contrôle sur accès** :

- Dans le menu **Configurer**, pointez votre curseur sur **Antivirus** et cliquez sur **Contrôle sur accès**.

### 4.8.3 Paramétrage du nettoyage automatique des virus/spywares

**Important :** si une console d'administration est utilisée pour administrer Sophos Endpoint Security and Control sur cet ordinateur, il se peut que vous perdiez tous les changements que vous avez effectués.

Lorsque le contrôle sur accès est activé, ou lorsque vous exécutez un contrôle à la demande ou par clic droit, Sophos Anti-Virus peut automatiquement effectuer les opérations suivantes :


- Nettoyage de la majorité des éléments infectés
- Assainissement des éléments infectés en utilisant d'autres moyens que le nettoyage.

**Remarque :** le nettoyage automatique des infections à plusieurs composants n'est pas disponible pour le contrôle sur accès. Pour nettoyer les infections à plusieurs composants de votre ordinateur, utilisez la section Gestionnaire de quarantaine. Pour plus d'informations sur le Gestionnaire de quarantaine, reportez-vous à la section [Traitement des adwares et des PUA en quarantaine](#) à la page 34.

Toutes les mesures que Sophos Anti-Virus prend contre les éléments infectés sont consignées dans le journal pour cet ordinateur ou journalisées pour le contrôle à la demande. Pour plus d'informations, reportez-vous aux sections [Visualisation du journal du contrôle](#) à la page 27 ou [Visualisation du journal du contrôle personnalisé](#) à la page 21.

Pour supprimer totalement certaines infections à plusieurs composants de votre ordinateur, vous devez redémarrer l'ordinateur. Si c'est le cas, vous aurez la possibilité de redémarrer votre ordinateur immédiatement ou ultérieurement. Les étapes finales de nettoyage seront exécutées après le redémarrage de l'ordinateur.

1. Ouvrez la boîte de dialogue des paramètres de contrôle pour le type de contrôle que vous voulez configurer (reportez-vous à la section [Ouverture de la boîte de dialogue des paramètres de contrôle](#) à la page 28).

2. Dans la boîte de dialogue des paramètres de contrôle, cliquez sur l'onglet **Nettoyage**. Paramétrez les options comme décrit ci-dessous.
  - Sélectionnez **Nettoyer automatiquement les éléments contenant des virus/spywares** pour permettre à Sophos Anti-Virus de désinfecter les secteurs de démarrage de disquettes, les documents, les programmes et tout ce qui est sélectionné pour un contrôle. Le nettoyage des documents ne répare en aucune façon les effets secondaires du virus dans le document (reportez-vous à la section [Obtention d'informations sur le nettoyage](#) à la page 32 pour savoir comment obtenir plus de détails à propos des effets secondaires des virus sur le site Web de Sophos).
  - Sophos Anti-Virus peut assainir un fichier infecté par d'autres moyens que le nettoyage. Vous pouvez sélectionner d'autres mesures que vous souhaitez voir prendre par Sophos Anti-Virus contre les fichiers infectés si vous n'utilisez pas le nettoyage automatique, ou si le nettoyage échoue. En revanche,  
 **Avertissement :** utilisez ces options seulement si le support technique de Sophos vous l'a conseillé. Sinon, utilisez le Gestionnaire de quarantaine pour nettoyer votre ordinateur des virus/spywares trouvés par Sophos Anti-Virus. Pour plus d'informations sur le Gestionnaire de quarantaine, reportez-vous à la section [Traitement des adwares et des PUA en quarantaine](#) à la page 34.

Cliquez sur **Supprimer** pour vous débarrasser du fichier. Cliquez sur **Déplacer dans** pour déplacer le fichier dans un autre dossier que vous pouvez sélectionner en utilisant **Parcourir**. Le déplacement d'un fichier exécutable réduit la probabilité de son exécution.

Vous ne pouvez pas automatiquement déplacer une infection à plusieurs composants.

**Remarque :** pour apprendre à nettoyer votre ordinateur des virus/spywares à l'aide du gestionnaire de quarantaine, reportez-vous à la section [Traitement des virus/spywares en quarantaine](#) à la page 33.

#### 4.8.4 Paramétrage du nettoyage automatique des adwares et des PUA

Lorsque vous exécutez un contrôle à la demande ou par clic droit, Sophos Anti-Virus peut automatiquement nettoyer les adwares et les PUA de votre ordinateur.

**Remarque :** le nettoyage automatique des adwares et des PUA n'est pas disponible pour le contrôle sur accès. Pour nettoyer les adwares et les PUA indésirables de votre ordinateur, utilisez le Gestionnaire de quarantaine. Pour plus d'informations sur le Gestionnaire de quarantaine, reportez-vous à la section [Traitement des adwares et des PUA en quarantaine](#) à la page 34.

Toutes les mesures que Sophos Anti-Virus prend contre les adwares et les PUA sont consignées dans le journal pour cet ordinateur ou dans le journal du contrôle à la demande. Pour plus d'informations, reportez-vous aux sections [Visualisation du journal du contrôle](#) à la page 27 ou [Visualisation du journal du contrôle personnalisé](#) à la page 21.

Pour supprimer totalement de votre ordinateur certains adwares et PUA constitués de plusieurs composants, vous devez redémarrer l'ordinateur. Si c'est le cas, vous aurez la possibilité de redémarrer votre ordinateur immédiatement ou ultérieurement. Les étapes finales de nettoyage seront exécutées après le redémarrage de l'ordinateur.

1. Ouvrez la boîte de dialogue des paramètres de contrôle pour le type de contrôle que vous voulez configurer (reportez-vous à la section [Ouverture de la boîte de dialogue des paramètres de contrôle](#) à la page 28).
2. Dans la boîte de dialogue des paramètres de contrôle, cliquez sur l'onglet **Nettoyage**.
3. Sélectionnez **Nettoyer automatiquement les adwares/PUA** pour permettre à Sophos Anti-Virus de supprimer de l'ordinateur pour tous les utilisateurs tous les composants connus des adwares et des PUA. Le nettoyage ne répare pas tous les changements que l'adware ou la PUA a déjà faits (reportez-vous à la section [Obtention d'informations sur le nettoyage](#) à la page 32 pour savoir comment voir sur le site Web de Sophos les détails sur les effets secondaires d'un adware ou d'un PUA).

**Remarque :** pour apprendre à nettoyer votre ordinateur des adwares et des PUA à l'aide du gestionnaire de quarantaine, reportez-vous à la section [Traitement des adwares et des PUA en quarantaine](#) à la page 34.

#### 4.8.5 Paramétrage du nettoyage automatique des fichiers suspects

**Important :** si une console d'administration est utilisée pour administrer Sophos Endpoint Security and Control sur cet ordinateur, il se peut que vous perdiez tous les changements que vous avez effectués.

Lorsque le contrôle sur accès est activé, ou lorsque vous exécutez un contrôle à la demande ou par clic droit, Sophos Anti-Virus peut automatiquement supprimer ou déplacer les fichiers suspects.

Un *fichier suspect* est un fichier qui comporte une combinaison de caractéristiques généralement, mais pas exclusivement, trouvées dans les virus.

1. Ouvrez la boîte de dialogue des paramètres de contrôle pour le type de contrôle que vous voulez configurer (reportez-vous à la section [Ouverture de la boîte de dialogue des paramètres de contrôle](#) à la page 28).
2. Dans la boîte de dialogue des paramètres de contrôle, cliquez sur l'onglet **Nettoyage**. Dans le volet **Fichiers suspects**, paramétrez les options comme décrit ci-dessous.



**Avertissement :** utilisez ces options seulement si le support technique de Sophos vous l'a conseillé. Sinon, utilisez le Gestionnaire de quarantaine pour nettoyer votre ordinateur des virus/spywares trouvés par Sophos Anti-Virus. Pour plus d'informations sur le Gestionnaire de quarantaine, reportez-vous à la section [Traitement des fichiers suspects en quarantaine](#) à la page 36.

Cliquez sur **Supprimer** pour vous débarrasser du fichier. Cliquez sur **Déplacer dans** pour déplacer le fichier dans un autre dossier que vous pouvez sélectionner en utilisant **Parcourir**. Le déplacement d'un fichier exécutable réduit la probabilité de son exécution.

**Remarque :** pour apprendre à nettoyer votre ordinateur des fichiers suspects à l'aide du gestionnaire de quarantaine, reportez-vous à la section [Traitement des fichiers suspects en quarantaine](#) à la page 36.

## 4.8.6 Obtention d'informations sur le nettoyage

Lorsqu'une menace est trouvée sur votre ordinateur, il est très important que vous vérifiez son analyse correspondante sur le site Web de Sophos pour avoir plus d'informations sur la menace ainsi que des conseils de nettoyage. Vous pouvez procéder depuis les deux emplacements suivants :

- L'alerte sur le bureau (contrôle sur accès)
- La boîte de dialogue de progression du contrôle (contrôle à la demande et par clic droit)
- Le gestionnaire de quarantaine (tous les types de contrôles)

### Informations via l'alerte sur le bureau

Si le contrôle sur accès est activé sur votre ordinateur, Sophos Anti-Virus affiche une alerte sur le bureau lorsqu'une menace est trouvée. Dans la boîte de message, cliquez sur le nom de la menace sur laquelle vous souhaitez en savoir plus.

Sophos Anti-Virus vous connecte à l'analyse de la menace sur le site Web de Sophos.

### Informations via la boîte de dialogue de progression du contrôle

Pour un contrôle à la demande et un contrôle exécuté par clic droit, dans le journal qui apparaît dans la boîte de dialogue de progression du contrôle (ou dans la boîte de dialogue de récapitulatif du contrôle, affichée une fois que le contrôle est terminé), cliquez sur le nom de la menace sur laquelle vous souhaitez en savoir plus.

Sophos Anti-Virus vous connecte à l'analyse de la menace sur le site Web de Sophos.

### Informations via le Gestionnaire de quarantaine

1. Sur la page d'**Accueil**, sous **Antivirus et HIPS**, cliquez sur **Gérer les éléments en quarantaine**. Pour plus d'informations sur la page d'**Accueil**, reportez-vous à la section [A propos de la page d'accueil](#) à la page 4.
2. Dans la colonne **Nom**, cliquez sur le nom de la menace sur laquelle vous souhaitez en savoir plus.

Sophos Anti-Virus vous connecte à l'analyse de la menace sur le site Web de Sophos.

## 4.9 Gestion des éléments en quarantaine

### 4.9.1 A propos du Gestionnaire de quarantaine

Le Gestionnaire de quarantaine vous permet de traiter les éléments trouvés par le contrôle non éliminés automatiquement lors du contrôle. Chaque élément est présent ici pour l'une des raisons suivantes :

- Aucune option de nettoyage (nettoyer, supprimer, déplacer) n'a été choisie pour le type de contrôle qui a détecté l'élément.
- Une option de nettoyage a été choisie pour le type de contrôle qui a détecté l'élément mais l'option a échoué.

- L'élément a plusieurs infections et contient encore des menaces supplémentaires.
- La menace a seulement été partiellement détectée et un contrôle intégral de l'ordinateur est nécessaire pour la détecter totalement. Pour savoir comment procéder, reportez-vous à la section [Exécution d'un contrôle intégral de l'ordinateur](#) à la page 17.
- L'élément affiche un comportement suspect.
- L'élément est une application contrôlée.

**Remarque :** les adwares, les PUA et les infections à plusieurs composants détectés lors du contrôle sur accès sont toujours énumérés dans le gestionnaire de quarantaine. Le nettoyage automatique des adwares, PUA et des infections à plusieurs composants n'est pas disponible pour le contrôle sur accès.

Une option de nettoyage peut avoir échoué à cause de droits d'accès insuffisants. Si vous avez des droits plus importants, vous pouvez utiliser le gestionnaire de quarantaine pour traiter le ou les élément(s).

Les menaces détectées lors du contrôle des pages web ne figurent pas dans le Gestionnaire de quarantaine car elles ne sont pas téléchargées sur votre ordinateur. C'est la raison pour laquelle aucune mesure n'est nécessaire.

## 4.9.2 Traitement des virus/spywares en quarantaine

**Remarque :** le terme *virus* est ici utilisé pour désigner un virus, un ver, un cheval de Troie ou tout autre logiciel malveillant.

1. Sur la page d'**Accueil**, sous **Antivirus et HIPS**, cliquez sur **Gérer les éléments en quarantaine**.  
Pour plus d'informations sur la page d'**Accueil**, reportez-vous à la section [A propos de la page d'accueil](#) à la page 4.
2. Dans la liste **Afficher**, cliquez sur **Virus/spywares**.

Les informations concernant chaque élément apparaissent dans les colonnes.

**Nom** affiche l'identité que Sophos Anti-Virus a détectée. Pour en savoir plus sur le virus/spyware, cliquez sur son identité et Sophos Anti-Virus vous connecte à l'analyse du virus/spyware sur le site Web de Sophos.

**Détails** affiche le nom et l'emplacement de l'élément. Si l'élément est associé à un rootkit, il apparaît comme "Caché". Si un lien **plus** apparaît près du nom de fichier, cela signifie que l'élément est infecté par une infection à plusieurs composants. Cliquez sur le lien pour voir la liste des autres composants faisant partie de l'infection. Si l'un des composants est associé à un rootkit, la boîte de dialogue indique que certains composants sont cachés.

**Actions disponibles** affiche les actions que vous pouvez effectuer sur l'élément. A moins que l'élément soit caché, trois actions sont disponibles : Nettoyer, Supprimer et Déplacer, décrites ci-dessous. Si vous cliquez sur l'une des actions, celle-ci est effectuée sur l'élément, attendant la confirmation. Les fichiers cachés peuvent seulement être nettoyés.

### Traitement des éléments infectés

Pour traiter les virus/spywares, utilisez les boutons décrits ci-dessous.

### Sélectionner tout/Dessélectionner tout

Cliquez sur ces boutons pour sélectionner ou dessélectionner tous les éléments. Ceci vous permet d'effectuer la même action sur un groupe d'éléments. Pour sélectionner ou dessélectionner un élément donné, sélectionnez la case à cocher située près de son nom.

### Effacer de la liste

Cliquez sur cette option pour supprimer des éléments sélectionnés de la liste, si vous êtes sûr qu'ils ne contiennent ni virus ni spyware. Par contre, ceci ne supprime pas les éléments du disque.

### Lancer une action

Cliquez sur cette option pour afficher une liste d'actions que vous pouvez effectuer sur les éléments sélectionnés.

- Cliquez sur **Nettoyer** pour supprimer un virus ou un élément de spyware des éléments sélectionnés. Le nettoyage des documents ne répare en aucune façon les effets secondaires du virus dans le document.

**Remarque :** pour supprimer totalement de votre ordinateur certains virus/spywares constitués de plusieurs composants ou pour nettoyer des fichiers cachés, vous devez redémarrer l'ordinateur. Si c'est le cas, vous aurez la possibilité de redémarrer votre ordinateur immédiatement ou ultérieurement. Les étapes finales de nettoyage seront exécutées après le redémarrage de l'ordinateur.

- Cliquez sur **Supprimer** pour supprimer les éléments sélectionnés de votre ordinateur. Utilisez cette fonction avec précaution.
- Cliquez sur **Déplacer** pour déplacer les éléments sélectionnés dans un autre dossier. Les éléments sont déplacés dans le dossier qui a été spécifié lorsque le nettoyage a été paramétré. Le déplacement d'un fichier exécutable réduit la probabilité de son exécution. Utilisez cette fonction avec précaution.



**Avertissement :** parfois, si vous supprimez ou déplacez un fichier infecté, il est possible que votre ordinateur ne fonctionne plus correctement parce qu'il ne parvient pas à trouver le fichier. Aussi, un fichier infecté peut seulement faire partie d'une infection multiple, auquel cas la suppression ou le déplacement de ce fichier en particulier ne nettoiera pas votre ordinateur de l'infection. Dans ce cas, contactez le support technique de Sophos pour obtenir de l'assistance dans le traitement des éléments.

Pour plus d'informations sur comment contacter le support technique, reportez-vous à la section [Support technique](#) à la page 86.

Pour configurer l'action que vous pouvez réaliser, reportez-vous à la section [Configuration des droits utilisateur pour le Gestionnaire de quarantaine](#) à la page 6.

## 4.9.3 Traitement des adwares et des PUA en quarantaine

1. Sur la page d'**Accueil**, sous **Antivirus et HIPS**, cliquez sur **Gérer les éléments en quarantaine**.

Pour plus d'informations sur la page d'**Accueil**, reportez-vous à la section [A propos de la page d'accueil](#) à la page 4.

2. Dans la liste **Afficher**, cliquez sur **Adwares ou PUA**.

Les informations concernant chaque élément apparaissent dans les colonnes.

**Nom** affiche l'identité que Sophos Anti-Virus a détectée. Pour en savoir plus sur l'adware ou la PUA, cliquez sur son identité et Sophos Anti-Virus vous connecte à son analyse sur le site Web de Sophos.

**Détails** affiche le sous-type de l'adware ou de la PUA. Si l'élément est associé à un rootkit, il apparaît comme "Caché". Si un lien **plus** apparaît près du sous-type, cela signifie que l'élément est un élément d'adware ou de PUA à plusieurs composants. Cliquez sur le lien pour voir la liste des autres composants faisant partie de l'adware ou de la PUA. Si l'un des composants est associé à un rootkit, la boîte de dialogue indique que certains composants sont cachés.

**Actions disponibles** affiche les actions que vous pouvez effectuer sur l'élément. Vous avez le choix entre deux options : Autoriser et Nettoyer, décrites ci-dessous. Si vous cliquez sur l'une des actions, celle-ci est effectuée sur l'élément, attendant la confirmation.

### Traitement des adwares et des PUA

Pour traiter les adwares et les PUA, utilisez les boutons décrits ci-dessous.

#### Sélectionner tout/Dessélectionner tout

Cliquez sur ces boutons pour sélectionner ou dessélectionner tous les éléments. Ceci vous permet d'effectuer la même action sur un groupe d'éléments. Pour sélectionner ou dessélectionner un élément donné, sélectionnez la case à cocher située près de son nom.

#### Effacer de la liste

Cliquez sur cette option pour supprimer les éléments sélectionnés de la liste, si vous leur faites confiance. Par contre, ceci ne supprime pas les éléments du disque.

#### Lancer une action

Cliquez sur cette option pour afficher une liste d'actions que vous pouvez effectuer sur les éléments sélectionnés.

- Cliquez sur **Autoriser** pour autoriser les éléments sélectionnés sur l'ordinateur, si vous leur faites confiance. Ceci ajoute les éléments à la liste des adwares et des PUA autorisés de manière à ce que Sophos Anti-Virus n'empêche pas leur exécution sur votre ordinateur.
- Cliquez sur **Nettoyer** pour supprimer de l'ordinateur tous les composants connus des éléments sélectionnés pour tous les utilisateurs. Pour nettoyer les adwares et les PUA de l'ordinateur, vous devez être membre des deux groupes Administrateurs Windows et SophosAdministrator.

**Remarque :** pour supprimer totalement de votre ordinateur certains adwares et PUA constitués de plusieurs composants ou pour nettoyer des fichiers cachés, vous devez redémarrer l'ordinateur. Si c'est le cas, vous aurez la possibilité de redémarrer votre ordinateur immédiatement ou ultérieurement. Les étapes finales de nettoyage seront exécutées après le redémarrage de l'ordinateur.

Pour configurer les actions que vous pouvez réaliser, reportez-vous à la section [Configuration des droits utilisateur pour le Gestionnaire de quarantaine](#) à la page 6.

Pour voir les listes des adwares et des PUA connus et autorisés, cliquez sur **Configurer l'autorisation**.

## 4.9.4 Traitement des fichiers suspects en quarantaine

Un *fichier suspect* est un fichier qui comporte une combinaison de caractéristiques généralement, mais pas exclusivement, trouvées dans les virus.

1. Sur la page d'**Accueil**, sous **Antivirus et HIPS**, cliquez sur **Gérer les éléments en quarantaine**.

Pour plus d'informations sur la page d'**Accueil**, reportez-vous à la section [A propos de la page d'accueil](#) à la page 4.

2. Dans la liste **Afficher**, cliquez sur **Fichiers suspects**.

Les informations concernant chaque élément apparaissent dans les colonnes.

**Nom** affiche l'identité que Sophos Anti-Virus a détectée. Pour en savoir plus sur le fichier suspect, cliquez sur son identité et Sophos Anti-Virus vous connecte à son analyse sur le site Web de Sophos.

**Détails** affiche le nom et l'emplacement de l'élément. Si l'élément est associé à un rootkit, il apparaît comme "Caché".

**Actions disponibles** affiche les actions que vous pouvez effectuer sur l'élément. A moins que l'élément soit caché, trois actions sont disponibles : Autoriser, Supprimer et Déplacer, décrites ci-dessous. Si vous cliquez sur l'une des actions, celle-ci est effectuée sur l'élément, attendant la confirmation. Les fichiers cachés peuvent seulement être autorisés.

### Traitement des fichiers suspects

Pour traiter les fichiers suspects, utilisez les boutons décrits ci-dessous.

#### Sélectionner tout/Dessélectionner tout

Cliquez sur ces boutons pour sélectionner ou dessélectionner tous les éléments. Ceci vous permet d'effectuer la même action sur un groupe d'éléments. Pour sélectionner ou dessélectionner un élément donné, sélectionnez la case à cocher située près de son nom.

#### Effacer de la liste

Cliquez sur cette option pour supprimer les éléments sélectionnés de la liste, si vous leur faites confiance. Par contre, ceci ne supprime pas les éléments du disque.

#### Lancer une action

Cliquez sur cette option pour afficher une liste d'actions que vous pouvez effectuer sur les éléments sélectionnés.

- Cliquez sur **Autoriser** pour autoriser les éléments sélectionnés sur l'ordinateur, si vous leur faites confiance. Ceci ajoute les éléments à la liste des éléments suspects autorisés de manière à ce que Sophos Anti-Virus n'empêche pas leur accès.
- Cliquez sur **Supprimer** pour supprimer les éléments sélectionnés de votre ordinateur. Utilisez cette fonction avec précaution.
- Cliquez sur **Déplacer** pour déplacer les éléments sélectionnés dans un autre dossier. Les éléments sont déplacés dans le dossier qui a été spécifié lorsque le nettoyage a été paramétré.

Le déplacement d'un fichier exécutable réduit la probabilité de son exécution. Utilisez cette fonction avec précaution.



**Avertissement :** parfois, si vous supprimez ou déplacez un fichier infecté, il est possible que votre ordinateur ne fonctionne plus correctement parce qu'il ne parvient pas à trouver le fichier.

Pour configurer les actions que vous pouvez réaliser, reportez-vous à la section [Configuration des droits utilisateur pour le Gestionnaire de quarantaine](#) à la page 6.

Pour voir la liste des fichiers suspects autorisés, cliquez sur **Configurer l'autorisation**.

## 4.9.5 Traitement des comportements suspects en quarantaine

*Le comportement suspect* est une activité qui semble malveillante.

1. Sur la page d'**Accueil**, sous **Antivirus et HIPS**, cliquez sur **Gérer les éléments en quarantaine**.

Pour plus d'informations sur la page d'**Accueil**, reportez-vous à la section [A propos de la page d'accueil](#) à la page 4.

2. Dans la liste **Afficher**, cliquez sur **Comportements suspects**.

Les informations concernant chaque élément apparaissent dans les colonnes.

**Nom** affiche l'identité que Sophos Anti-Virus a détectée. Pour en savoir plus sur le comportement, cliquez sur l'identité et Sophos Anti-Virus vous connecte à l'analyse du comportement sur le site Web de Sophos.

**Détails** affiche le nom et l'emplacement de l'élément.

**Actions disponibles** affiche les actions que vous pouvez effectuer sur l'élément. Si vous avez activé le blocage de tout comportement suspect, il n'y a qu'une seule opération disponible : Autoriser, décrite ci-dessous. Si vous cliquez sur l'action, celle-ci est effectuée sur l'élément, attendant la confirmation.

### Traitement du comportement suspect

Pour traiter le comportement suspect, utilisez les boutons décrits ci-dessous.

#### Sélectionner tout/Dessélectionner tout

Cliquez sur ces boutons pour sélectionner ou dessélectionner tous les éléments. Ceci vous permet d'effectuer la même action sur un groupe d'éléments. Pour sélectionner ou dessélectionner un élément donné, sélectionnez la case à cocher située près de son nom.

#### Effacer de la liste

Cliquez sur cette option pour supprimer les éléments sélectionnés de la liste, si vous leur faites confiance. Par contre, ceci ne supprime pas les éléments du disque.

#### Lancer une action

Cliquez sur cette option pour afficher une liste d'actions que vous pouvez effectuer sur les éléments sélectionnés.

- Cliquez sur **Autoriser** pour autoriser les éléments sélectionnés sur l'ordinateur, si vous leur faites confiance. Ceci ajoute les éléments à la liste des éléments suspects autorisés de manière à ce que Sophos Anti-Virus n'empêche pas le comportement.

Pour configurer les actions que vous pouvez réaliser, reportez-vous à la section [Configuration des droits utilisateur pour le Gestionnaire de quarantaine](#) à la page 6.

Pour voir la liste des comportements suspects autorisés, cliquez sur **Configurer l'autorisation**.

## 4.9.6 Traitement des applications contrôlées en quarantaine

Une *application contrôlée* est une application interdite d'exécution sur votre ordinateur par la stratégie de sécurité de votre entreprise.

1. Sur la page d'**Accueil**, sous **Antivirus et HIPS**, cliquez sur **Gérer les éléments en quarantaine**.

Pour plus d'informations sur la page d'**Accueil**, reportez-vous à la section [A propos de la page d'accueil](#) à la page 4.

2. Dans la liste **Afficher**, cliquez sur **Applications contrôlées**.

Les informations concernant chaque élément apparaissent dans les colonnes.

**Nom** affiche l'identité que Sophos Anti-Virus a détectée. Pour en savoir plus sur l'application contrôlée, cliquez sur son identité et Sophos Anti-Virus vous connecte à son analyse sur le site Web de Sophos.

**Détails** affiche le sous-type de l'application contrôlée. Si un lien **plus** apparaît près du sous-type, cliquez dessus pour voir la liste des autres composants faisant partie de l'application contrôlée.

**Actions disponibles** affiche les actions que vous pouvez effectuer sur l'élément. En revanche, aucune action n'est disponible pour les applications contrôlées à part l'effacement de l'élément de la liste, décrit ci-dessous.

### Traitement des applications contrôlées

Pour traiter les applications contrôlées, utilisez les boutons décrits ci-dessous.

#### Sélectionner tout/Dessélectionner tout

Cliquez sur ces boutons pour sélectionner ou dessélectionner tous les éléments. Ceci vous permet d'effectuer la même action sur un groupe d'éléments. Pour sélectionner ou dessélectionner un élément donné, sélectionnez la case à cocher située près de son nom.

#### Effacer de la liste

Cliquez sur cette option pour supprimer les éléments sélectionnés de la liste. Par contre, ceci ne supprime pas les éléments du disque. Avant que vous ne les utilisiez, les applications contrôlées doivent être autorisées par la console centrale.

## 4.10 Autorisation d'utilisation d'éléments

### 4.10.1 Autorisation d'utilisation d'adwares et de PUA

**Important :** si une console d'administration est utilisée pour administrer Sophos Endpoint Security and Control sur cet ordinateur, il se peut que vous perdiez tous les changements que vous avez effectués.

Si vous voulez exécuter un adware ou une application que Sophos Anti-Virus a classé comme potentiellement indésirable, vous pouvez l'autoriser.

Pour autoriser l'utilisation d'adwares et de PUA :

1. Dans le menu **Configurer**, pointez votre curseur sur **Antivirus** et cliquez sur **Autorisation**.
2. Sur l'onglet **Adwares ou PUA**, dans la liste **Adwares ou PUA connus**, sélectionnez l'adware ou la PUA.
3. Cliquez sur **Ajouter**.

L'adware ou la PUA apparaît maintenant dans la zone de liste **Adwares ou PUA autorisés**.

**Remarque :** vous pouvez aussi autoriser des adwares et des PUA dans le Gestionnaire de quarantaine. Pour plus d'instructions sur la manière de procéder, reportez-vous à la section [Traitement des adwares et des PUA en quarantaine](#) à la page 34.

### 4.10.2 Blocage des adwares et des PUA autorisés

Pour empêcher l'exécution des adwares et des PUA actuellement autorisés sur votre ordinateur :

1. Dans le menu **Configurer**, pointez votre curseur sur **Antivirus** et cliquez sur **Autorisation**.
2. Sur l'onglet **Adwares ou PUA**, dans la liste **Adwares ou PUA connus**, sélectionnez l'adware ou la PUA que vous souhaitez bloquer.
3. Cliquez sur **Supprimer**.

### 4.10.3 Autorisation d'utilisation d'éléments suspects

**Important :** si une console d'administration est utilisée pour administrer Sophos Endpoint Security and Control sur cet ordinateur, il se peut que vous perdiez tous les changements que vous avez effectués.

Si vous voulez autoriser un élément que Sophos Anti-Virus a classé comme suspect, autorisez-le comme suit :

1. Dans le menu **Configurer**, pointez votre curseur sur **Antivirus** et cliquez sur **Autorisation**.
2. Cliquez sur l'onglet correspondant au type d'élément qui a été détecté (par exemple, **Dépassement de la mémoire tampon**).
3. Dans la liste **Connus**, sélectionnez l'élément suspect.
4. Cliquez sur **Ajouter**.

L'élément suspect apparaît dans la liste **Autorisés**.

**Remarque :** vous pouvez aussi autoriser des éléments suspects dans le gestionnaire de quarantaine. Pour de plus amples informations sur la manière de procéder, consultez les sujets suivants :

- [Traitement des fichiers suspects en quarantaine](#) à la page 36
- [Traitement des comportements suspects en quarantaine](#) à la page 37

#### 4.10.4 Préautorisation d'éléments suspects

Si vous voulez autoriser un élément que Sophos Endpoint Security and Control n'a pas encore classé comme suspect, vous pouvez le préautoriser.

Pour préautoriser un élément suspect :

1. Dans le menu **Configurer**, pointez votre curseur sur **Antivirus** et cliquez sur **Autorisation**.
2. Cliquez sur l'onglet correspondant au type d'élément qui a été détecté (par exemple, **Dépassement de la mémoire tampon**).
3. Cliquez sur **Nouveau**.
4. Recherchez l'élément suspect et cliquez deux fois dessus.

L'élément suspect apparaît dans la liste **Autorisés**.

## 5 Utilisation de Sophos Device Control

### 5.1 A propos du contrôle des périphériques sur cet ordinateur

Si une console d'administration n'est pas utilisée pour administrer Sophos Endpoint Security and Control sur cet ordinateur, la fonctionnalité de contrôle des périphériques n'est *pas* incluse.

Le contrôle des périphériques est activé ou désactivé par une console d'administration. Lorsque le contrôle des périphériques est activé, il peut empêcher toute connexion d'un périphérique à cet ordinateur que vous souhaiteriez utiliser pour effectuer des opérations de maintenance ou de résolutions des problèmes. Dans ce cas, vous pouvez temporairement désactiver le contrôle des périphériques sur cet ordinateur. Pour plus d'informations, reportez-vous à la section [Désactivation temporaire du contrôle des périphériques](#) à la page 41.

### 5.2 Quels types de périphériques peuvent être contrôlés ?

Le contrôle des périphériques bloque ou autorise trois types de périphériques sur cet ordinateur : *stockage, réseau et courte portée*.

#### Stockage

- Périphériques de stockage amovibles (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 disquettes

#### Réseau

- Modems
- Sans fil (interfaces Wi-Fi, norme 802.11)

La stratégie de contrôle des périphériques de cet ordinateur peut être en mode **Bloquer le pont**, ce qui désactive les adaptateurs réseau sans fil ou modem lorsque l'ordinateur 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)

### 5.3 Désactivation temporaire du contrôle des périphériques

**Important :** si une console d'administration est utilisée pour administrer Sophos Endpoint Security and Control sur cet ordinateur, il se peut que vous perdiez tous les changements que vous avez effectués.

Si vous êtes un membre du groupe SophosAdministrator et si vous souhaitez connecter un périphérique à cet ordinateur pour des raisons de maintenance ou de résolution de problèmes (par exemple, pour installer un logiciel depuis un CD-ROM), vous pouvez temporairement désactiver le contrôle des périphériques.

Pour désactiver le contrôle des périphériques sur cet ordinateur :

1. Dans le menu **Configurer**, cliquez sur **Contrôle des périphériques**.
2. Dessélectionnez la case **Activer Sophos Device Control**.

## 5.4 Configuration du journal du contrôle des périphériques

1. Dans le menu **Configurer**, cliquez sur **Contrôle des périphériques**.
2. Sous **Niveau de journalisation**, sélectionnez l'une des options suivantes :
  - Cliquez sur **Aucun** pour ne pas effectuer la journalisation.
  - Cliquez sur **Normal** pour journaliser un résumé des informations, les messages d'erreur et ainsi de suite.
  - Cliquez sur **Détaillé** pour fournir des informations sur beaucoup plus d'activités que celles du journal normal. Utilisez uniquement ce paramètre lorsque vous avez besoin d'une journalisation détaillée pour résoudre les problèmes, car ce paramètre entraîne l'augmentation rapide du volume du journal.
3. Sous **Journalisation de l'archivage**, suivez les instructions à l'écran.

## 5.5 Visualisation du journal du contrôle des périphériques

- ❖ Sur la page d'**Accueil**, sous **Contrôle des périphériques**, cliquez sur **Voir le journal du contrôle des périphériques**.

Pour plus d'informations sur la page d'**Accueil**, reportez-vous à la section [A propos de la page d'accueil](#) à la page 4.

Depuis la page du journal, vous pouvez copier le journal dans le Presse-papiers, l'envoyer par courriel ou l'imprimer.

Pour rechercher un texte spécifique dans le journal, cliquez sur **Rechercher** et saisissez le texte que vous souhaitez rechercher.

## 6 Utilisation de Sophos Data Control

### 6.1 A propos du contrôle des données sur cet ordinateur

Si une console d'administration n'est pas utilisée pour administrer Sophos Endpoint Security and Control sur cet ordinateur, la fonctionnalité de contrôle des données n'est *pas* incluse.

Le contrôle des données est activé ou désactivé par une stratégie émise par une console d'administration. En revanche, si vous êtes un membre du groupe SophosAdministrator, vous pouvez désactiver temporairement le contrôle des données sur cet ordinateur pour la maintenance et la résolution des problèmes. Pour plus d'informations, reportez-vous à la section [Désactivation temporaire du contrôle des données](#) à la page 43.

### 6.2 Désactivation temporaire du contrôle des données

**Important :** si une console d'administration est utilisée pour administrer Sophos Endpoint Security and Control sur cet ordinateur, il se peut que vous perdiez tous les changements que vous avez effectués.

Si vous êtes un membre du groupe SophosAdministrator, vous pouvez désactiver temporairement le contrôle des données sur cet ordinateur pour la maintenance et la résolution des problèmes :

1. Dans le menu **Configurer**, cliquez sur **Contrôle des données**.
2. Dessélectionnez la case **Activer Sophos Data Control**.

### 6.3 Comment ajouter un fichier dans un périphérique de stockage ?

Si le contrôle des données est activé sur cet ordinateur, la stratégie de contrôle des données peut bloquer toute tentative d'ajout d'un fichier dans un périphérique de stockage surveillé à l'aide des méthodes suivantes :

- Enregistrement des données depuis un programme
- Utilisation de la commande de copie sous DOS
- Création d'un nouveau fichier sur le périphérique à l'aide de Windows Explorer

Si vous voyez une alerte de bureau qui vous avertit à ce propos, enregistrez le fichier sur votre disque dur ou sur un lecteur réseau, puis utilisez l'Explorateur Windows pour le copier sur le périphérique de stockage.

### 6.4 Configuration du journal du contrôle des données

1. Dans le menu **Configurer**, cliquez sur **Contrôle des données**.

2. Sous **Niveau de journalisation**, sélectionnez l'une des options suivantes :
  - Cliquez sur **Aucun** pour ne pas effectuer la journalisation.
  - Cliquez sur **Normal** pour journaliser un résumé des informations, les messages d'erreur et ainsi de suite.
  - Cliquez sur **Détaillé** pour fournir des informations sur beaucoup plus d'activités que celles du journal normal. Utilisez uniquement ce paramètre lorsque vous avez besoin de tester les nouvelles règles du contrôle des données, car ce paramètre entraîne l'augmentation rapide du volume du journal.
3. Sous **Journalisation de l'archivage**, suivez les instructions à l'écran.

## 6.5 Visualisation du journal du contrôle des données

- ❖ Sur la page d'**Accueil**, sous **Contrôle des données**, cliquez sur **Voir le journal du contrôle des données**.

Pour plus d'informations sur la page d'**Accueil**, reportez-vous à la section [A propos de la page d'accueil](#) à la page 4.

Depuis la page du journal, vous pouvez copier le journal dans le Presse-papiers, l'envoyer par courriel ou l'imprimer.

Pour rechercher un texte spécifique dans le journal, cliquez sur **Rechercher** et saisissez le texte que vous souhaitez rechercher.

## 7 Utilisation de Sophos Client Firewall

### 7.1 Introduction au pare-feu

Lorsque le pare-feu est installé pour la première fois, il se peut que vous ayez à le configurer. Ceci dépend de la manière dont il a été installé. Il existe deux types d'installation :

- Installé sur un ordinateur en réseau et administré depuis la console d'administration
- Installé sur un ordinateur autonome et administré depuis l'ordinateur

#### **Pare-feu administré depuis une console d'administration**

Si le pare-feu est installé et administré depuis une console d'administration, il autorise ou bloque les applications et le trafic conformément aux règles définies par la stratégie.

Vous ne recevez aucun message et n'avez pas besoin de configurer le pare-feu sauf si la stratégie a mis le pare-feu en mode interactif (voir ci-dessous).

#### **Pare-feu administré depuis cet ordinateur**

Si le pare-feu est administré sur cet ordinateur, nous vous recommandons de commencer par créer des règles pour autoriser l'accès au réseau à des applications et services usuels tels que les navigateurs Web et les clients de messagerie.

Pour plus d'informations sur la création des règles, reportez-vous à la section [A propos de la configuration du pare-feu](#) à la page 45.

Le pare-feu est par défaut en mode interactif (voir ci-dessous). Maintenez le pare-feu en mode interactif afin de vous laisser le temps d'autoriser ou de bloquer d'autres applications et services que vous utilisez.

Dès que le pare-feu est configuré et qu'il reconnaît les applications que vous utilisez le plus, nous vous recommandons de passer à l'un des modes non interactif.

Pour plus d'informations, reportez-vous à la section [Passage en mode non interactif](#) à la page 51.

#### **Qu'est ce que le mode interactif ?**

En mode interactif, le pare-feu vous demande d'autoriser ou de bloquer toutes les applications et tout le trafic pour lesquels ne s'appliquent aucune règle.

Pour plus d'informations sur le traitement des messages depuis le pare-feu, reportez-vous à la section [A propos du mode interactif](#) à la page 51.

### 7.2 Configuration du pare-feu

#### 7.2.1 A propos de la configuration du pare-feu

Vous pouvez configurer le pare-feu de plusieurs façons différentes puis l'activer. Toutefois, si une console d'administration est utilisée pour administrer Sophos Endpoint Security and

Control sur cet ordinateur, il se peut que vous perdiez tous les changements que vous avez effectués.

Retrouvez ci-dessous quelques-unes des fonctions les plus communes :

- [Activation du mode interactif](#) à la page 51
- [Filtrage des messages ICMP](#) à la page 49
- [Autorisation du trafic sur le réseau local \(LAN\)](#) à la page 48
- [Autorisation des téléchargements FTP](#) à la page 47
- [Création d'une règle globale](#) à la page 56
- [Autorisation d'une application](#) à la page 49
- [Autorisation de lancement des processus cachés aux applications](#) à la page 61
- [Autorisation d'utilisation des rawsockets aux applications](#) à la page 61
- [Utilisation des sommes de contrôle pour authentifier les applications](#) à la page 62

## 7.2.2 Désactivation temporaire du pare-feu

Si vous êtes un membre du groupe SophosAdministrator, vous pouvez avoir temporairement besoin, pour des raisons de maintenance ou de résolution des problèmes, de désactiver le pare-feu, puis de le réactiver.

Sophos Endpoint Security and Control conserve les paramètres que vous choisissez ici, même après le redémarrage de l'ordinateur. Si vous désactivez le pare-feu, votre ordinateur reste sans protection jusqu'à ce vous le réactiviez.

1. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Configurer le pare-feu**.  
Pour plus d'informations sur la page d'**Accueil**, reportez-vous à la section [A propos de la page d'accueil](#) à la page 4.
2. Sous **Configurations**, sélectionnez la case **Autoriser tout le trafic** pour l'emplacement principal ou l'emplacement secondaire.

## 7.2.3 Autorisation des courriels

**Important :** si une console d'administration est utilisée pour administrer Sophos Endpoint Security and Control sur cet ordinateur, il se peut que vous perdiez tous les changements que vous avez effectués.

1. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Configurer le pare-feu**.  
Pour plus d'informations sur la page d'**Accueil**, reportez-vous à la section [A propos de la page d'accueil](#) à la page 4.
2. Sous **Configurations**, cliquez sur le bouton **Configurer** correspondant à l'emplacement que vous souhaitez configurer.
3. Cliquez sur l'onglet **Applications**
4. Cliquez sur **Ajouter**, recherchez l'application de messagerie et cliquez deux fois dessus.

L'application de messagerie est autorisée en tant qu'application fiable.

Les applications fiables reçoivent un accès intégral et inconditionnel au réseau, y compris l'accès à Internet. Pour une sécurité renforcée, vous pouvez appliquer les règles prédéterminées fournies par Sophos :

1. Dans la liste des applications autorisées, cliquez sur l'application de messagerie.
2. Cliquez sur **Personnaliser** > **Ajouter des règles prédéterminées** > **Client de messagerie**.

## 7.2.4 Autorisation d'utilisation d'un navigateur Web

**Remarque :** si vous autorisez l'utilisation d'un navigateur Web, vous autorisez également l'accès FTP.

1. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Configurer le pare-feu**.  
Pour plus d'informations sur la page d'**Accueil**, reportez-vous à la section [A propos de la page d'accueil](#) à la page 4.
2. Sous **Configurations**, cliquez sur le bouton **Configurer** correspondant à l'emplacement que vous souhaitez configurer.
3. Cliquez sur l'onglet **Applications**
4. Cliquez sur **Ajouter**, recherchez l'application de navigateur Web et cliquez deux fois dessus.

L'application de navigateur Web est autorisée en tant qu'application fiable.

Les applications fiables reçoivent un accès intégral et inconditionnel au réseau, y compris l'accès à Internet. Pour une sécurité renforcée, vous pouvez appliquer les règles prédéterminées fournies par Sophos :

1. Dans la liste des applications autorisées, cliquez sur l'application de navigateur Web.
2. Cliquez sur **Personnaliser** > **Ajouter des règles prédéterminées** > **Navigateur**.

## 7.2.5 Autorisation des téléchargements FTP

**Remarque :** si vous avez autorisé l'utilisation d'un navigateur Web qui peut accéder aux serveurs FTP, vous n'avez pas besoin d'autoriser les téléchargements FTP.

1. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Configurer le pare-feu**.  
Pour plus d'informations sur la page d'**Accueil**, reportez-vous à la section [A propos de la page d'accueil](#) à la page 4.
2. Sous **Configurations**, cliquez sur le bouton **Configurer** correspondant à l'emplacement que vous souhaitez configurer.
3. Cliquez sur l'onglet **Applications**
4. Cliquez sur **Ajouter**, recherchez l'application FTP et cliquez deux fois dessus.

L'application FTP est autorisée en tant qu'application fiable.

Les applications fiables reçoivent un accès intégral et inconditionnel au réseau, y compris l'accès à Internet. Pour une sécurité renforcée, vous pouvez appliquer les règles prédéterminées fournies par Sophos :

1. Dans la liste des applications autorisées, cliquez sur l'application FTP.
2. Cliquez sur **Personnaliser > Ajouter des règles prédéterminées > Client FTP**.

## 7.2.6 Autorisation du trafic sur le réseau local (LAN)

**Remarque :** si vous autorisez le trafic sur un un réseau local (LAN), vous autorisez également le partage de fichiers et d'imprimantes.

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

1. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Configurer le pare-feu**.  
Pour plus d'informations sur la page d'**Accueil**, reportez-vous à la section [A propos de la page d'accueil](#) à la page 4.
2. Sous **Configurations**, cliquez sur le bouton **Configurer** correspondant à l'emplacement que vous souhaitez configurer.
3. Sur l'onglet **Réseau local**, procédez de l'une des manières suivantes :
  - Cliquez sur **Détecter** pour détecter le réseau local sur lequel se trouve votre ordinateur et ajoutez-le à la liste des adresses réseau.
  - Cliquez sur **Ajouter**. Dans la boîte de dialogue **Sélection de l'adresse**, sélectionnez le **Format de l'adresse**, saisissez le nom de domaine ou l'adresse IP et cliquez sur **Ajouter**.
4. Cliquez sur **OK** pour fermer la boîte de dialogue **Sélection de l'adresse**.
5. Dans la liste des adresses réseau, sélectionnez la case **Fiable** pour autoriser le trafic sur un réseau local.

## 7.2.7 Autorisation du partage des fichiers et des imprimantes sur un réseau local (LAN)

**Remarque :** si vous avez autorisé le trafic sur un réseau local (LAN), vous n'avez pas besoin d'autoriser le partage de fichiers et d'imprimantes.

1. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Configurer le pare-feu**.  
Pour plus d'informations sur la page d'**Accueil**, reportez-vous à la section [A propos de la page d'accueil](#) à la page 4.
2. Sous **Configurations**, cliquez sur le bouton **Configurer** correspondant à l'emplacement que vous souhaitez configurer.
3. Sur l'onglet **Réseau local**, procédez de l'une des manières suivantes :
  - Cliquez sur **Détecter** pour détecter le réseau local sur lequel se trouve votre ordinateur et ajoutez-le à la liste des adresses réseau.
  - Cliquez sur **Ajouter**. Dans la boîte de dialogue **Sélection de l'adresse**, sélectionnez le **Format de l'adresse**, saisissez le nom de domaine ou l'adresse IP et cliquez sur **Ajouter**.
4. Cliquez sur **OK** pour fermer la boîte de dialogue **Sélection de l'adresse**.
5. Dans la liste des adresses réseau, sélectionnez la case **NetBIOS** pour autoriser le partage des fichiers et des imprimantes sur un réseau local.

## 7.2.8 Autorisation d'une application

1. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Configurer le pare-feu**.  
Pour plus d'informations sur la page d'**Accueil**, reportez-vous à la section [A propos de la page d'accueil](#) à la page 4.
2. Sous **Configurations**, cliquez sur le bouton **Configurer** correspondant à l'emplacement que vous souhaitez configurer.
3. Cliquez sur l'onglet **Applications**
4. Cliquez sur **Ajouter**, recherchez l'application et cliquez deux fois dessus.

L'application est autorisée et considérée comme fiable.

Les applications fiables 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 59
- [Application de règles d'applications prédéterminées](#) à la page 58

## 7.2.9 Blocage d'une application

1. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Configurer le pare-feu**.  
Pour plus d'informations sur la page d'**Accueil**, reportez-vous à la section [A propos de la page d'accueil](#) à la page 4.
2. Sous **Configurations**, cliquez sur le bouton **Configurer** correspondant à l'emplacement que vous souhaitez configurer.
3. Cliquez sur l'onglet **Applications**
4. Si l'application ne figure pas dans la liste, cliquez sur **Ajouter**, recherchez l'application et cliquez deux fois dessus.
5. Sélectionnez l'application dans la liste et cliquez sur **Bloquer**.

## 7.2.10 Filtrage des messages ICMP

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 50.

Pour filtrer les messages ICMP :

1. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Configurer le pare-feu**.  
Pour plus d'informations sur la page d'**Accueil**, reportez-vous à la section [A propos de la page d'accueil](#) à la page 4.

2. Sous **Configurations**, cliquez sur le bouton **Configurer** correspondant à l'emplacement que vous souhaitez configurer.
3. Sur l'onglet **ICMP**, sélectionnez la case **Entrant** ou **Sortant** pour autoriser les types de messages entrants ou sortants spécifiés.

### 7.2.11 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 <code>ping</code> .
<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 répondra 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 interréseau mais sont désormais caducs 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.

## 7.2.12 Restauration des paramètres par défaut du pare-feu

1. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Configurer le pare-feu**.  
Pour plus d'informations sur la page d'**Accueil**, reportez-vous à la section [A propos de la page d'accueil](#) à la page 4.
2. Sous **Gestion de la configuration**, cliquez sur **Valeurs par défaut**.

## 7.3 Fonctionnement en mode interactif

### 7.3.1 A 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 vous demande si vous voulez autoriser le trafic cette fois-ci seulement, le bloquer cette fois-ci seulement ou si vous voulez créer une règle pour ce type de trafic.

En mode interactif, vous allez voir apparaître les types de boîte de dialogue d'apprentissage suivants :

- [Boîtes de dialogue d'apprentissage des processus cachés](#) à la page 52
- [Boîtes de dialogue d'apprentissage des protocoles](#) à la page 52
- [Boîtes de dialogue d'apprentissage des applications](#) à la page 53
- [Boîtes de dialogue d'apprentissage des rawsockets](#) à la page 53
- [Boîtes de dialogue d'apprentissage des sommes de contrôle](#) à la page 53

### 7.3.2 Activation du mode interactif

1. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Configurer le pare-feu**.  
Pour plus d'informations sur la page d'**Accueil**, reportez-vous à la section [A propos de la page d'accueil](#) à la page 4.
2. Sous **Configurations**, cliquez sur le bouton **Configurer** correspondant à l'emplacement que vous souhaitez configurer.
3. Sur l'onglet **Général**, sous **Mode de fonctionnement**, cliquez sur **Interactif**.

### 7.3.3 Passage en mode non interactif

Il existe deux modes non interactif :

- Autoriser par défaut
- Bloquer par défaut

En modes non interactif, le pare-feu traite le trafic réseau automatiquement en utilisant vos règles. Le trafic réseau sans règle de correspondance est soit autorisé, soit bloqué.

Pour passer en mode non interactif :

1. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Configurer le pare-feu**.  
Pour plus d'informations sur la page d'**Accueil**, reportez-vous à la section [A propos de la page d'accueil](#) à la page 4.
2. Sous **Configurations**, cliquez sur le bouton **Configurer** correspondant à l'emplacement que vous souhaitez configurer.
3. Sur l'onglet **Général**, sous **Mode de fonctionnement**, cliquez sur **Autoriser par défaut** ou sur **Bloquer par défaut**.

### 7.3.4 Boîtes de dialogue d'apprentissage des processus cachés

On parle de processus caché lorsqu'une application en lance une autre afin qu'elle lui trouve un accès au réseau. Certaines applications malveillantes utilisent parfois cette technique pour échapper aux pare-feu : elles lancent une application fiable pour accéder au réseau plutôt que de le faire elles-mêmes.

La boîte de dialogue d'apprentissage des processus cachés vous donne des informations sur le processus caché et sur l'application qui l'a lancé.

- [Activation des boîtes de dialogue d'apprentissage des processus cachés](#) à la page 52

### 7.3.5 Activation des boîtes de dialogue d'apprentissage des processus cachés

Si vous utilisez le mode interactif, le pare-feu peut afficher une boîte de dialogue d'apprentissage lorsqu'il détecte un nouveau lanceur de programme.

Si vous utilisez le mode interactif et si cette option n'est pas sélectionnée, les nouveaux lanceurs de programme sont bloqués et ne peuvent pas lancer les processus cachés.

Pour activer les boîtes de dialogue de processus cachés :

1. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Configurer le pare-feu**.  
Pour plus d'informations sur la page d'**Accueil**, reportez-vous à la section [A propos de la page d'accueil](#) à la page 4.
2. Sous **Configurations**, cliquez sur le bouton **Configurer** correspondant à l'emplacement que vous souhaitez configurer.
3. Cliquez sur l'onglet **Processus**.
4. Sélectionnez la case **Avertir à propos des nouveaux lanceurs de programme**.

### 7.3.6 Boîtes de dialogue d'apprentissage des protocoles

Si le pare-feu détecte une activité réseau du système qu'il ne peut relier à aucune application spécifique, il demande la création d'une règle de protocole.

La boîte de dialogue d'apprentissage des protocoles donne des informations sur l'activité réseau non reconnue, c'est-à-dire, le protocole et l'adresse distante.

### 7.3.7 Boîtes de dialogue d'apprentissage des applications

Si le pare-feu détecte qu'une application tente d'accéder au réseau sans respecter de règles existantes, il demande la création d'une règle d'application.

La boîte de dialogue d'apprentissage des applications donne des informations sur l'activité réseau non reconnue, c'est-à-dire, le service distant et l'adresse distante.

### 7.3.8 Boîtes de dialogue d'apprentissage des rawsockets

Les rawsockets permettent aux processus de contrôler tous les aspects des données qu'ils envoient sur le réseau et peuvent être utilisées à des fins malveillantes.

Si le pare-feu détecte qu'une rawsocket tente d'accéder au réseau sans respecter de règles existantes, il demande la création d'une règle de rawsocket.

La boîte de dialogue d'apprentissage des rawsockets donne des informations sur la rawsocket.

- [Activation des boîtes de dialogue d'apprentissage des rawsockets](#) à la page 53

### 7.3.9 Activation des boîtes de dialogue d'apprentissage des rawsockets

Si vous utilisez le mode interactif, le pare-feu peut afficher une boîte de dialogue d'apprentissage lorsqu'il détecte qu'une rawsocket tente d'accéder au réseau sans respecter de règles existantes.

Si vous utilisez le mode interactif et si cette option n'est pas sélectionnée, les rawsockets sont bloquées et ne peuvent accéder au réseau.

Pour activer les boîtes de dialogue des rawsockets :

1. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Configurer le pare-feu**.  
Pour plus d'informations sur la page d'**Accueil**, reportez-vous à la section [A propos de la page d'accueil](#) à la page 4.
2. Sous **Configurations**, cliquez sur le bouton **Configurer** correspondant à l'emplacement que vous souhaitez configurer.
3. Cliquez sur l'onglet **Processus**.
4. Sélectionnez la case **Avertir à propos de l'utilisation des rawsockets**.

### 7.3.10 Boîtes de dialogue d'apprentissage des sommes de contrôle

Si le pare-feu détecte une application (nouvelle ou modifiée), il affiche une boîte de dialogue d'apprentissage des sommes de contrôle.

Si vous souhaitez autoriser l'accès au réseau, vous devez ajouter sa somme de contrôle (son identifiant exclusif) à la liste des sommes de contrôle reconnues.

Sélectionnez l'une des options suivantes :

- **Ajouter la somme de contrôle à celles existantes pour cette application** autorise plusieurs versions de cette application.

- **Remplacer toutes les sommes de contrôle existantes pour cette application** remplace toutes les sommes de contrôle existantes pour cette application par celle demandant l'accès et par conséquent, autorise uniquement la version la plus récente de cette application.
- **Bloquer cette application jusqu'à son redémarrage** bloque l'application juste pour cette occasion.

### 7.3.11 Activation des boîtes de dialogue d'apprentissage des sommes de contrôle

Si vous utilisez le mode interactif, le pare-feu peut afficher une boîte de dialogue d'apprentissage lorsqu'il détecte une application, qu'elle soit nouvelle ou modifiée.

Si vous utilisez le mode interactif et que cette option n'est pas sélectionnée, les applications sont bloquées et ne peuvent accéder au réseau.

Pour activer les boîtes de dialogue des sommes de contrôle :

1. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Configurer le pare-feu**.  
Pour plus d'informations sur la page d'**Accueil**, reportez-vous à la section [A propos de la page d'accueil](#) à la page 4.
2. Sous **Configurations**, cliquez sur le bouton **Configurer** correspondant à l'emplacement que vous souhaitez configurer.
3. Sélectionnez la case **Utiliser les sommes de contrôle pour authentifier les applications**.

## 7.4 Fichiers de configuration du pare-feu

### 7.4.1 A propos des fichiers de configuration du pare-feu

Sophos Client Firewall vous permet d'exporter les paramètres généraux ainsi que les règles du pare-feu sous un fichier de configuration. Vous pouvez utiliser cette fonction pour effectuer les opérations suivantes :

- Faire une copie de sauvegarde et restaurer l'intégralité de la configuration de votre pare-feu.
- Enregistrer une configuration des paramètres généraux et l'installer sur plusieurs ordinateurs.
- Créer des règles pour les applications sur un ordinateur et les exporter pour une utilisation sur d'autres ordinateurs exécutant les mêmes applications.
- Utiliser la console d'administration pour fusionner les configurations créées sur plusieurs ordinateurs différents afin de créer une stratégie qui soit valide sur tous les ordinateurs du réseau.

### 7.4.2 Exportation d'un fichier de configuration du pare-feu

1. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Configurer le pare-feu**.  
Pour plus d'informations sur la page d'**Accueil**, reportez-vous à la section [A propos de la page d'accueil](#) à la page 4.

2. Cliquez sur **Exporter**.
3. Nommez votre fichier de configuration, mettez-le à l'emplacement de votre choix, et cliquez sur **Enregistrer**.

### 7.4.3 Importation d'un fichier de configuration du pare-feu

1. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Configurer le pare-feu**.  
Pour plus d'informations sur la page d'**Accueil**, reportez-vous à la section [A propos de la page d'accueil](#) à la page 4.
2. Cliquez sur **Importer**.
3. Sélectionnez un fichier de configuration et cliquez sur **Ouvrir**.
4. Suivez les instructions à l'écran.

## 7.5 Règles de pare-feu

### 7.5.1 A 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.

### 7.5.2 A 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 dans l'ordre suivant.

1. Si la connexion se fait sur une adresse faisant partie des plages spécifiées sur l'onglet **Réseau local**, et si l'adresse a été marquée comme fiable, la connexion est autorisée sans aucune vérification supplémentaire.
2. Si le réseau autorise uniquement NetBIOS, toute connexion répondant aux critères suivant est autorisée :
  - Toute connexion TCP où le port distant est dans la plage 137-139 ou 445.
  - Toute connexion TCP où le port local est dans la plage 137-139 ou 445.
  - Toute connexion UDP où le port distant est dans la plage 137 ou 138.
  - Toute connexion UDP où le port local est dans la plage 137 ou 138.

3. Tout trafic NetBIOS n'ayant pas été autorisé à l'aide de l'onglet **LAN** est bloqué. Pour plus d'informations sur la manière d'autoriser le trafic NetBIOS, reportez-vous à la section [Autorisation du partage des fichiers et des imprimantes sur un réseau local \(LAN\)](#) à la page 48.
4. Les règles globales à priorité élevée sont vérifiées dans l'ordre où elles apparaissent dans la liste.
5. Si aucune règle n'a encore été appliquée à la connexion, le pare-feu vérifie les règles d'applications.
6. Si la connexion n'a pas encore été traitée, le pare-feu applique les règles globales à priorité normale dans l'ordre où elles apparaissent dans la liste.
7. Si aucune règle n'a été trouvée pour traiter la connexion :
  - En mode **Autoriser par défaut**, le trafic est autorisé.
  - En mode **Bloquer par défaut**, le trafic est bloqué.
  - En mode **Interactif**, l'utilisateur décide de l'action à mener.

## 7.5.3 Règles globales

### 7.5.3.1 Création d'une règle globale

**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. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Configurer le pare-feu**.  
Pour plus d'informations sur la page d'**Accueil**, reportez-vous à la section [A propos de la page d'accueil](#) à la page 4.
2. Sous **Configurations**, cliquez sur le bouton **Configurer** correspondant à l'emplacement que vous souhaitez configurer.
3. Cliquez sur l'onglet **Règles globales**.
4. Cliquez sur **Ajouter**.
5. 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.
6. 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 [A propos de l'ordre dans lequel les règles sont appliquées](#) à la page 55.
7. Sous **Sélectionner les événements que la règle traitera**, sélectionnez les conditions auxquelles la connexion doit correspondre pour que la règle s'applique.
8. Sous **Sélectionner les actions avec lesquelles la règle répondra**, sélectionnez soit **Autoriser** soit **Bloquer**.

9. Pour autoriser les réponses depuis l'ordinateur distant qui seront basées sur la connexion initiale, sélectionnez **Inspection "stateful"**.
10. 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.

### 7.5.3.2 Modification d'une règle globale

**Important :** nous vous recommandons de modifier les règles globales uniquement si vous êtes familier avec les protocoles réseau.

Pour modifier une règle globale :

1. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Configurer le pare-feu**.  
Pour plus d'informations sur la page d'**Accueil**, reportez-vous à la section [A propos de la page d'accueil](#) à la page 4.
2. Sous **Configurations**, cliquez sur le bouton **Configurer** correspondant à l'emplacement que vous souhaitez configurer.
3. Cliquez sur l'onglet **Règles globales**.
4. Dans la liste **Règle**, sélectionnez la règle que vous souhaitez modifier.
5. Cliquez sur **Modifier**.
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 [A propos de l'ordre dans lequel les règles sont appliquées](#) à la page 55.
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 "stateful"**.
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.

### 7.5.3.3 Copie d'une règle globale

Pour copier une règle globale et l'ajouter à la liste des règles :

1. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Configurer le pare-feu**.  
Pour plus d'informations sur la page d'**Accueil**, reportez-vous à la section [A propos de la page d'accueil](#) à la page 4.
2. Sous **Configurations**, cliquez sur le bouton **Configurer** correspondant à l'emplacement que vous souhaitez configurer.
3. Cliquez sur l'onglet **Règles globales**.

4. Dans la liste **Règle**, sélectionnez la règle que vous souhaitez copier.
5. Cliquez sur **Copier**.

#### 7.5.3.4 Modification de l'ordre dans lequel les règles sont appliquées

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. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Configurer le pare-feu**.  
Pour plus d'informations sur la page d'**Accueil**, reportez-vous à la section [A propos de la page d'accueil](#) à la page 4.
2. Sous **Configurations**, cliquez sur le bouton **Configurer** correspondant à l'emplacement que vous souhaitez configurer.
3. Cliquez sur l'onglet **Règles globales**.
4. Dans la liste **Règle**, cliquez sur la règle que vous souhaitez faire monter ou descendre dans la liste.
5. Cliquez sur **Monter** ou **Descendre**.

#### 7.5.3.5 Suppression d'une règle globale

1. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Configurer le pare-feu**.  
Pour plus d'informations sur la page d'**Accueil**, reportez-vous à la section [A propos de la page d'accueil](#) à la page 4.
2. Sous **Configurations**, cliquez sur le bouton **Configurer** correspondant à l'emplacement que vous souhaitez configurer.
3. Cliquez sur l'onglet **Règles globales**.
4. Dans la liste **Règle**, sélectionnez la règle que vous souhaitez supprimer.
5. Cliquez sur **Supprimer**.

### 7.5.4 Règles d'applications

#### 7.5.4.1 Application de règles d'applications prédéterminées

Une prédétermination est une série de règles d'applications créées par Sophos. Pour ajouter des règles prédéterminées à la fin de la liste des règles pour une application :

1. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Configurer le pare-feu**.  
Pour plus d'informations sur la page d'**Accueil**, reportez-vous à la section [A propos de la page d'accueil](#) à la page 4.
2. Sous **Configurations**, cliquez sur le bouton **Configurer** correspondant à l'emplacement que vous souhaitez configurer.
3. Cliquez sur l'onglet **Applications**
4. Sélectionnez l'application dans la liste et cliquez sur la flèche près du bouton **Personnaliser**.

5. Pointez votre curseur sur **Ajouter des règles prédéterminées** et cliquez sur une prédétermination.

#### 7.5.4.2 Création d'une règle d'applications

Pour créer une règle personnalisée qui vous permettra d'ajuster avec précision l'accès autorisé pour une application :

1. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Configurer le pare-feu**.  
Pour plus d'informations sur la page d'**Accueil**, reportez-vous à la section [A propos de la page d'accueil](#) à la page 4.
2. Sous **Configurations**, cliquez sur le bouton **Configurer** correspondant à l'emplacement que vous souhaitez configurer.
3. Cliquez sur l'onglet **Applications**
4. Sélectionnez l'application dans la liste et cliquez sur **Personnaliser**.  
Vous pouvez aussi cliquer deux fois sur l'application dans la liste.
5. Dans la boîte de dialogue **Règles d'applications**, 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 d'applications ne peuvent pas avoir le même nom, en revanche, deux applications peuvent chacune avoir une règle portant le même nom.
7. Sous **Sélectionner les événements que la règle traitera**, sélectionnez les conditions auxquelles la connexion doit correspondre pour que la règle s'applique.
8. Sous **Sélectionner les actions avec lesquelles la règle répondra**, sélectionnez soit **Autoriser** soit **Bloquer**.
9. Pour autoriser les réponses depuis l'ordinateur distant qui seront basées sur la connexion initiale, sélectionnez **Inspection "stateful"**.
10. 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.

#### 7.5.4.3 Modification d'une règle d'applications

1. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Configurer le pare-feu**.  
Pour plus d'informations sur la page d'**Accueil**, reportez-vous à la section [A propos de la page d'accueil](#) à la page 4.
2. Sous **Configurations**, cliquez sur le bouton **Configurer** correspondant à l'emplacement que vous souhaitez configurer.
3. Cliquez sur l'onglet **Applications**
4. Sélectionnez l'application dans la liste et cliquez sur **Personnaliser**.  
Vous pouvez aussi cliquer deux fois sur l'application dans la liste.
5. Dans la boîte de dialogue **Règles d'applications**, cliquez sur **Modifier**.

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 d'applications ne peuvent pas avoir le même nom, en revanche, deux applications peuvent chacune avoir une règle portant le même nom.
7. Sous **Sélectionner les événements que la règle traitera**, sélectionnez les conditions auxquelles la connexion doit correspondre pour que la règle s'applique.
8. Sous **Sélectionner les actions avec lesquelles la règle répondra**, sélectionnez soit **Autoriser** soit **Bloquer**.
9. Pour autoriser les réponses depuis l'ordinateur distant qui seront basées sur la connexion initiale, sélectionnez **Inspection "stateful"**.
10. 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.

#### 7.5.4.4 Copie d'une règle d'applications

Pour copier une règle d'applications et l'ajouter à la liste des règles :

1. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Configurer le pare-feu**.  
Pour plus d'informations sur la page d'**Accueil**, reportez-vous à la section [A propos de la page d'accueil](#) à la page 4.
2. Sous **Configurations**, cliquez sur le bouton **Configurer** correspondant à l'emplacement que vous souhaitez configurer.
3. Cliquez sur l'onglet **Applications**
4. Sélectionnez l'application dans la liste et cliquez sur **Personnaliser**.  
Vous pouvez aussi cliquer deux fois sur l'application dans la liste.
5. Dans la boîte de dialogue **Règles d'applications**, cliquez sur **Copier**.

#### 7.5.4.5 Modification de l'ordre dans lequel les règles d'applications sont appliquées

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. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Configurer le pare-feu**.  
Pour plus d'informations sur la page d'**Accueil**, reportez-vous à la section [A propos de la page d'accueil](#) à la page 4.
2. Sous **Configurations**, cliquez sur le bouton **Configurer** correspondant à l'emplacement que vous souhaitez configurer.
3. Cliquez sur l'onglet **Applications**
4. Sélectionnez l'application dans la liste et cliquez sur **Personnaliser**.  
Vous pouvez aussi cliquer deux fois sur l'application dans la liste.
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**.

#### 7.5.4.6 Suppression d'une règle d'applications

1. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Configurer le pare-feu**.  
Pour plus d'informations sur la page d'**Accueil**, reportez-vous à la section [A propos de la page d'accueil](#) à la page 4.
2. Sous **Configurations**, cliquez sur le bouton **Configurer** correspondant à l'emplacement que vous souhaitez configurer.
3. Cliquez sur l'onglet **Applications**
4. Sélectionnez l'application dans la liste et cliquez sur **Personnaliser**.
5. Dans la boîte de dialogue **Règles d'applications**, cliquez sur **Supprimer**.

#### 7.5.4.7 Autorisation de lancement des processus cachés aux applications

Une application lance parfois un autre processus caché afin qu'il lui trouve un accès au réseau.

Certaines applications malveillantes peuvent utiliser cette technique pour échapper aux pare-feu : elles lancent une application fiable pour accéder au réseau plutôt que de le faire elles-mêmes.

Le pare-feu envoie une alerte à la console d'administration, si elle est utilisée, la première fois qu'un processus caché est détecté.

Pour autoriser des applications à lancer des processus cachés :

1. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Configurer le pare-feu**.  
Pour plus d'informations sur la page d'**Accueil**, reportez-vous à la section [A propos de la page d'accueil](#) à la page 4.
2. Sous **Configurations**, cliquez sur le bouton **Configurer** correspondant à l'emplacement que vous souhaitez configurer.
3. Cliquez sur l'onglet **Processus**.
4. Dans la zone supérieure, cliquez sur le bouton **Ajouter**.
5. Recherchez l'application et cliquez deux fois dessus.

Si vous utilisez le mode interactif, le pare-feu peut afficher une boîte de dialogue d'apprentissage lorsqu'il détecte un nouveau lanceur de programme.

■ [Activation du mode interactif](#) à la page 51

■ [Activation des boîtes de dialogue d'apprentissage des processus cachés](#) à la page 52

#### 7.5.4.8 Autorisation d'utilisation des rawsockets aux applications

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.

Le pare-feu envoie une alerte à la console d'administration, si elle est utilisée, la première fois qu'une rawsocket est détectée.

Pour autoriser les applications à accéder au réseau par le biais des rawsockets :

1. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Configurer le pare-feu**.  
Pour plus d'informations sur la page d'**Accueil**, reportez-vous à la section [A propos de la page d'accueil](#) à la page 4.
2. Sous **Configurations**, cliquez sur le bouton **Configurer** correspondant à l'emplacement que vous souhaitez configurer.
3. Cliquez sur l'onglet **Processus**.
4. Dans la zone inférieure, cliquez sur le bouton **Ajouter**.
5. Recherchez l'application et cliquez deux fois dessus.

Si vous utilisez le mode interactif, le pare-feu peut afficher une boîte de dialogue d'apprentissage lorsqu'il détecte une rawsocket.

- [Activation du mode interactif](#) à la page 51
- [Activation des boîtes de dialogue d'apprentissage des rawsockets](#) à la page 53

#### 7.5.4.9 Utilisation des sommes de contrôle pour authentifier les applications

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 ou (en mode interactif) demande à l'utilisateur ce qu'il doit faire.

Le pare-feu envoie également une alerte à la console d'administration, si elle est utilisée, la première fois qu'une application (qu'elle soit nouvelle ou modifiée) est détectée.

Pour ajouter une somme de contrôle à la liste des sommes de contrôle autorisées :

1. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Configurer le pare-feu**.  
Pour plus d'informations sur la page d'**Accueil**, reportez-vous à la section [A propos de la page d'accueil](#) à la page 4.
2. Sous **Configurations**, cliquez sur le bouton **Configurer** correspondant à l'emplacement que vous souhaitez configurer.
3. Cliquez sur l'onglet **Sommes de contrôle**.
4. Cliquez sur **Ajouter**.
5. Recherchez l'application et cliquez deux fois dessus.

Si vous utilisez le mode interactif, le pare-feu peut afficher une boîte de dialogue d'apprentissage lorsqu'il détecte une application, qu'elle soit nouvelle ou modifiée.

- [Activation du mode interactif](#) à la page 51
- [Activation des boîtes de dialogue d'apprentissage des processus cachés](#) à la page 52

## 7.6 Connexion intuitive selon l'emplacement

### 7.6.1 A propos de la connexion intuitive selon l'emplacement

La connexion intuitive selon l'emplacement est une fonction de Sophos Client Firewall qui assigne une série de règles selon l'emplacement de l'ordinateur.

Un ordinateur portable peut, par exemple, se voir assigner une série de règles de pare-feu plus restrictives lorsqu'il est utilisé en dehors des locaux de l'entreprise car il ne bénéficiera pas de la protection du pare-feu réseau.

Pour utiliser la connexion intuitive selon l'emplacement, commencez par définir une liste d'emplacements principaux (par exemple, vos différents réseaux d'entreprise). Lorsque le pare-feu détecte votre connexion à l'un des réseaux principaux, il utilise votre configuration principale.

- [Définition des emplacements principaux](#) à la page 63

Ensuite, créez une configuration secondaire. Si le pare-feu détecte que vous n'êtes **pas** connecté à l'un de vos emplacements principaux, il utilise votre configuration secondaire.

- [Création d'une configuration secondaire](#) à la page 64

### 7.6.2 Définition des emplacements principaux

Le pare-feu utilise votre configuration principal lorsqu'il détecte que vous êtes dans l'un de vos emplacements principaux.

1. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Configurer le pare-feu**.  
Pour plus d'informations sur la page d'**Accueil**, reportez-vous à la section [A propos de la page d'accueil](#) à la page 4.
2. Cliquez sur l'onglet **Détection de l'emplacement**.
3. 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.

Dans les deux cas, le pare-feu examine ou résout votre liste d'emplacements principaux. Lorsqu'il trouve une correspondance, votre ordinateur est placé dans l'un de vos emplacements principaux.

4. Suivez les instructions à l'écran.

### 7.6.3 Création d'une configuration secondaire

Le pare-feu utilise votre configuration secondaire lorsqu'il détecte que vous n'êtes pas connecté à votre emplacement principal.

1. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Configurer le pare-feu**.  
Pour plus d'informations sur la page d'**Accueil**, reportez-vous à la section [A propos de la page d'accueil](#) à la page 4.
2. Sélectionnez la case à cocher **Ajout d'une configuration pour un second emplacement**.

Paramétrez maintenant votre configuration secondaire. Pour plus d'informations, reportez-vous à la section *Configuration du pare-feu*.

## 7.7 Rapport du pare-feu

### 7.7.1 A propos des rapports du pare-feu

Par défaut, les rapports du pare-feu signale les modifications d'état, les événements et les erreurs à la console d'administration.

#### 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 la console d'administration. Dans ce cas, vous pouvez décider de ne **pas** envoyer d'alertes "Diffère de la stratégie" à la console d'administration 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 65.

#### Événements du pare-feu

Un *événement* a lieu lorsqu'une application sur votre ordinateur ou lorsque le système d'exploitation de votre ordinateur essaye de communiquer avec un autre ordinateur par le biais d'une connexion réseau.

Vous pouvez empêcher le pare-feu de signaler les événements à la console d'administration.

Pour plus d'informations, reportez-vous à la section [Désactivation du signalement du trafic réseau inconnu](#) à la page 65.

## 7.7.2 Activation ou désactivation du signalement des modifications locales

Si la configuration de votre pare-feu 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 la console d'administration concernant les modifications apportées aux règles globales, aux applications, aux processus ou aux sommes de contrôle. Vous pouvez vouloir faire ceci, par exemple, lorsque vous travaillez 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 cet ordinateur est prévue pour être conforme à la stratégie, **activez le signalement des modifications locales**.

Pour désactiver le signalement des modifications locales :

1. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Configurer le pare-feu**.  
Pour plus d'informations sur la page d'**Accueil**, reportez-vous à la section [A propos de la page d'accueil](#) à la page 4.
2. Sous **Configurations**, cliquez sur le bouton **Configurer** correspondant à l'emplacement que vous souhaitez configurer.
3. Dans l'onglet **Général**, sous **Signalement**, effacez 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.

Pour activer le signalement des modifications locales, sélectionnez la case à cocher.

## 7.7.3 Désactivation du signalement du trafic réseau inconnu

Vous pouvez empêcher le pare-feu de signaler le trafic réseau inconnu à la console d'administration. Le pare-feu considère le trafic comme inconnu s'il n'a pas de règle.

Pour empêcher le pare-feu de signaler le trafic réseau inconnu à la console d'administration :

1. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Configurer le pare-feu**.  
Pour plus d'informations sur la page d'**Accueil**, reportez-vous à la section [A propos de la page d'accueil](#) à la page 4.
2. Sous **Configurations**, cliquez sur le bouton **Configurer** correspondant à l'emplacement que vous souhaitez configurer.
3. Dans l'onglet **Général**, sous **Blocage**, sélectionnez la case à cocher **Utiliser les sommes de contrôle pour authentifier les applications**.
4. Sous **Signalement**, désélectionnez la case à cocher **Signaler les applications et le trafic inconnus à la console d'administration**.

## 7.7.4 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 de signaler les erreurs à la console d'administration :

1. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Configurer le pare-feu**.  
Pour plus d'informations sur la page d'**Accueil**, reportez-vous à la section [A propos de la page d'accueil](#) à la page 4.
2. Sous **Configurations**, cliquez sur le bouton **Configurer** correspondant à l'emplacement que vous souhaitez configurer.
3. Dans l'onglet **Général**, sous **Signalement**, désélectionnez la case à cocher **Signaler les erreurs à la console d'administration**.

## 7.7.5 Configuration de la messagerie de bureau

Vous pouvez contrôler à l'aide d'infobulles les messages que le pare-feu affiche sur le bureau.

En mode interactif, les infobulles sur les applications et le trafic inconnus n'apparaissent pas car les mêmes informations figurent dans les boîtes de dialogue d'apprentissage.

1. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Configurer le pare-feu**.  
Pour plus d'informations sur la page d'**Accueil**, reportez-vous à la section [A propos de la page d'accueil](#) à la page 4.
2. Sous **Configurations**, cliquez sur le bouton **Configurer** correspondant à l'emplacement que vous souhaitez configurer.
3. Dans l'onglet **Général**, sous **Messagerie de bureau**, procédez ainsi :
  - Pour afficher les infobulles sur les alertes et les erreurs du pare-feu, sélectionnez la case à cocher **Afficher les alertes et les erreurs**.
  - Pour afficher les infobulles sur les applications et le trafic inconnus, sélectionnez la case à cocher **Afficher les applications et le trafic inconnus**.

## 7.8 Journalisation du pare-feu

### 7.8.1 A propos du visualiseur de journaux du pare-feu

Le visualiseur de journaux de Sophos Client Firewall vous permet de visualiser, de filtrer et d'enregistrer des informations suivantes :

- Toutes les connexions
- Les connexions qui ont été autorisées ou bloquées
- Événements du pare-feu
- Le journal système

### 7.8.2 Ouverture du visualiseur de journaux du pare-feu

- ❖ Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Voir le journal du pare-feu**.

Pour plus d'informations sur la page d'**Accueil**, reportez-vous à la section [A propos de la page d'accueil](#) à la page 4.

### 7.8.3 Configuration de la journalisation du pare-feu

Pour gérer la taille et le contenu de la base de données du journal des événements du pare-feu :

1. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Configurer le pare-feu**.  
Pour plus d'informations sur la page d'**Accueil**, reportez-vous à la section [A propos de la page d'accueil](#) à la page 4.
2. Cliquez sur l'onglet **Journal**.
3. Pour gérer la taille de la base de données du journal des événements du pare-feu, sélectionnez l'une des options suivantes :

Option	Description
<b>Permettre à la base de données de croître sans limites</b>	Cliquez sur <b>Conserver tous les enregistrements</b> .
<b>Effacer les anciens enregistrements</b>	Cliquez sur <b>Supprimer les anciens enregistrements</b> , puis configurez les <b>Paramètres de nettoyage du journal</b> .

4. Sous **Paramètres de nettoyage du journal**, sélectionnez une ou plusieurs des options suivantes :
  - Cliquez sur la case à cocher **Supprimer les enregistrements après** et saisissez ou sélectionnez un chiffre dans la zone **Jours**.
  - Cliquez sur la case à cocher **Ne pas garder plus de** et saisissez ou sélectionnez un chiffre dans la zone **Enregistrements**.
  - Cliquez sur la case à cocher **Conserver la taille sous** et saisissez ou sélectionnez un chiffre dans la zone **Mo**.

### 7.8.4 Changement de l'aspect du visualiseur de journaux du pare-feu

1. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Voir le journal du pare-feu**.  
Pour plus d'informations sur la page d'**Accueil**, reportez-vous à la section [A propos de la page d'accueil](#) à la page 4.
2. Dans le menu **Affichage**, cliquez sur **Disposition**.
3. Dans la boîte de dialogue **Personnalisation de la vue**, sélectionnez les éléments à cacher ou à afficher :
  - L'**Arborescence** apparaît dans le volet gauche.
  - La **Barre d'outils** apparaît en haut du visualiseur de journaux du pare-feu.
  - La **Barre de description** apparaît au-dessus des données dans le volet droit.
  - La **Barre d'état** apparaît au bas du visualiseur de journaux du pare-feu.

## 7.8.5 Personnalisation du format des données

Vous pouvez changer le format utilisé pour afficher les éléments de données suivants dans les journaux du pare-feu :

- Afficher les ports sous la forme d'un nombre ou d'un nom, par exemple **HTTP** ou **80**.
- Afficher les applications sous la forme d'icônes, de chemins de fichiers ou les deux.
- Spécifier la taille de l'unité utilisée pour afficher la vitesse de transfert des données, par exemple **Koctets** ou **Moctets**.
- Cacher ou afficher la grille.

Pour personnaliser le format des données :

1. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Voir le journal du pare-feu**.  
Pour plus d'informations sur la page d'**Accueil**, reportez-vous à la section [A propos de la page d'accueil](#) à la page 4.
2. Dans le menu **Affichage**, cliquez sur **Personnaliser**.
3. Sélectionnez les options souhaitées.

## 7.8.6 Affichage ou masquage des colonnes dans le visualiseur de journaux du pare-feu

1. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Voir le journal du pare-feu**.  
Pour plus d'informations sur la page d'**Accueil**, reportez-vous à la section [A propos de la page d'accueil](#) à la page 4.
2. Cliquez sur un élément dans l'arborescence pour afficher des colonnes dans le volet des détails.
3. Dans le menu **Affichage**, sélectionnez **Ajouter/Supprimer des colonnes**.  
Vous pouvez aussi cliquer avec le bouton droit de la souris sur l'un des en-têtes de colonnes.
4. Dans la boîte de dialogue **Colonnes**, procédez ainsi :

Option	Description
Masquer une colonne	Dessélectionnez sa case à cocher.
Afficher une colonne	Sélectionnez sa case à cocher.

## 7.8.7 Réorganisation des colonnes dans le visualiseur de journaux du pare-feu

1. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Voir le journal du pare-feu**.  
Pour plus d'informations sur la page d'**Accueil**, reportez-vous à la section [A propos de la page d'accueil](#) à la page 4.

2. Cliquez sur un élément dans l'arborescence pour afficher des colonnes dans le volet des détails.
3. Dans le menu **Affichage**, sélectionnez **Ajouter/Supprimer des colonnes**.  
Vous pouvez aussi cliquer avec le bouton droit de la souris sur l'un des en-têtes de colonnes.
4. Dans la boîte de dialogue **Colonnes**, cliquez sur un nom de colonne, puis cliquez sur **Vers le haut** ou **Vers le bas** pour changer la position de la colonne.

### Remarques

- Vous pouvez aussi réorganiser les colonnes dans le volet des détails en utilisant la souris pour déplacer un en-tête de colonne à gauche ou à droite de sa position d'origine. Au moment du déplacement de la colonne, une surbrillance entre les en-têtes de colonnes indique la nouvelle position de la colonne.
- Vous pouvez redimensionner les colonnes en utilisant la souris pour déplacer les en-têtes de colonnes.

## 7.8.8 Filtrage des enregistrements dans un journal de pare-feu

Vous pouvez trier les enregistrements du journal du pare-feu en créant un filtre.

Pour filtrer les enregistrements du journal du pare-feu :

1. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Voir le journal du pare-feu**.  
Pour plus d'informations sur la page d'**Accueil**, reportez-vous à la section [A propos de la page d'accueil](#) à la page 4.
2. Dans l'arborescence, sélectionnez un journal.
3. Dans le menu **Action**, cliquez sur **Ajouter un filtre**.
4. Suivez le reste des instructions dans l'assistant **Règles**.

Le filtre apparaît dans l'arborescence immédiatement au-dessous du noeud du journal que vous voulez filtrer.

## 7.8.9 Exportation de tous les enregistrements depuis un journal de pare-feu

Pour exporter tous les enregistrements depuis le journal de pare-feu dans un fichier texte ou CSV :

1. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Voir le journal du pare-feu**.  
Pour plus d'informations sur la page d'**Accueil**, reportez-vous à la section [A propos de la page d'accueil](#) à la page 4.
2. Dans l'arborescence, sélectionnez un journal.
3. Cliquez avec le bouton droit de la souris sur la liste des enregistrements, puis cliquez sur **Exporter tous les enregistrements**.
4. Dans la zone **Nom du fichier**, saisissez un nom de fichier.
5. Dans la liste **Type de fichier**, cliquez sur le type de fichier désiré.

### 7.8.10 Exportation d'une sélection d'enregistrements depuis un journal de pare-feu

Pour exporter une sélection d'enregistrements depuis un journal de pare-feu dans un fichier texte ou CSV :

1. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Voir le journal du pare-feu**.  
Pour plus d'informations sur la page d'**Accueil**, reportez-vous à la section [A propos de la page d'accueil](#) à la page 4.
2. Dans l'arborescence, sélectionnez un journal.
3. Sélectionnez les enregistrements que vous voulez exporter.  
Si les enregistrements se mettent à jour rapidement, dans le menu **Affichage**, désélectionnez la case à cocher **Rafraîchir automatiquement**.
4. Dans le menu **Action**, cliquez sur **Exporter les enregistrements sélectionnés**.
5. Dans la zone **Nom du fichier**, saisissez un nom de fichier.
6. Dans la liste **Type de fichier**, cliquez sur le type de fichier désiré.

## 8 Utilisation de Sophos AutoUpdate

### 8.1 Mise à jour immédiate

Par défaut, Sophos AutoUpdate est prévu pour effectuer une mise à jour toutes les 60 minutes si vous êtes connecté en permanence à Internet ou à votre réseau.

Si vous avez une connexion par modem, Sophos AutoUpdate est prévu pour effectuer une mise à jour lorsque vous vous connectez à Internet ou à votre réseau, puis toutes les 60 minutes.

Pour une mise à jour immédiate :

- ❖ Cliquez avec le bouton droit de la souris sur l'icône Sophos Endpoint Security and Control de la zone de notification, puis cliquez sur **Mettre à jour maintenant**.

### 8.2 Planification des mises à jour

**Important :** si une console d'administration est utilisée pour administrer Sophos Endpoint Security and Control sur cet ordinateur, il se peut que vous perdiez tous les changements que vous avez effectués.

Vous pouvez spécifier quand ou à quelle fréquence Sophos AutoUpdate se met à jour.

1. Dans le menu **Configurer**, cliquez sur **Mise à jour**.
2. Cliquez sur l'onglet **Planifier**.
3. Sélectionnez **Activer les mises à jour automatiques**, puis saisissez la fréquence (en minutes) avec laquelle Sophos AutoUpdate se mettra à jour.  
si les mises à jour sont téléchargées directement depuis le serveur Sophos, Sophos AutoUpdate ne peut pas se mettre à jour plus fréquemment que toutes les 60 minutes. Sur un réseau, les mises à jour sont toutes les 5 minutes par défaut.

### 8.3 Choix d'une source pour les mises à jour

Si vous souhaitez que Sophos AutoUpdate se mette à jour automatiquement, vous devez spécifier d'où il télécharge les mises à jour.

1. Dans le menu **Configurer**, cliquez sur **Mise à jour**.
2. Cliquez sur l'onglet **Emplacement principal**.
3. Dans la liste **Adresse**, saisissez le chemin UNC ou l'adresse web du serveur de mise à jour.

Pour télécharger les mises à jour directement depuis Sophos via Internet, sélectionnez **Sophos** dans la liste **Adresse**.

4. Dans la zone **Nom utilisateur**, tapez le **Nom utilisateur** du compte qui sera utilisé pour accéder au serveur de mise à jour.  
Si le **Nom utilisateur** doit avoir une qualification pour indiquer le domaine, utilisez la forme *domaine\nomutilisateur*.
5. Dans la zone **Mot de passe**, tapez et confirmez le **Mot de passe**.

## 8.4 Choix d'une source alternative pour les mises à jour

Vous pouvez définir une source alternative pour les mises à jour. Si Sophos AutoUpdate ne peut pas mettre à jour depuis sa source habituelle, il tente de mettre à jour à partir de cette source alternative.

1. Dans le menu **Configurer**, cliquez sur **Mise à jour**.
2. Cliquez sur l'onglet **Emplacement secondaire**.
3. Dans la liste **Adresse**, saisissez le chemin UNC ou l'adresse web du serveur de mise à jour.

Pour télécharger les mises à jour directement depuis Sophos via Internet, sélectionnez **Sophos** dans la liste **Adresse**.

4. Dans la zone **Nom utilisateur**, tapez le **Nom utilisateur** du compte qui sera utilisé pour accéder au serveur de mise à jour.

Si le **Nom utilisateur** doit avoir une qualification pour indiquer le domaine, utilisez la forme *domaine\nomutilisateur*.

5. Dans la zone **Mot de passe**, tapez et confirmez le **Mot de passe**.

## 8.5 Mise à jour via un serveur proxy

Si Sophos AutoUpdate met à jour via Internet, vous devez saisir les détails de tout serveur proxy qu'il doit utiliser pour se connecter à Internet.

1. Dans le menu **Configurer**, cliquez sur **Mise à jour**.
2. Cliquez sur l'onglet **Emplacement principal** ou **Emplacement secondaire**.
3. Cliquez sur **Détails du proxy**.
4. Sélectionnez la case à cocher **Accéder à l'emplacement via un proxy**.
5. Saisissez l'**Adresse** et le numéro du **Port** du serveur proxy.
6. 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*.

## 8.6 Mise à jour via une connexion par modem

Pour mettre à jour via une connexion par modem à Internet :

1. Dans le menu **Configurer**, cliquez sur **Mise à jour**.
2. Cliquez sur l'onglet **Planifier**.
3. Sélectionnez **Vérifier les mises à jour à la connexion**.

Sophos AutoUpdate se mettra à jour chaque fois que vous vous connecterez à Internet.

## 8.7 Limitation de la bande passante utilisée pour la mise à jour

Pour empêcher Sophos AutoUpdate d'utiliser toute votre bande passante lorsque vous en avez besoin pour d'autres opérations (comme le téléchargement de votre courrier), vous pouvez limiter la quantité de bande passante utilisée.

1. Dans le menu **Configurer**, cliquez sur **Mise à jour**.
2. Cliquez sur l'onglet **Emplacement principal** ou **Emplacement secondaire**.
3. Cliquez sur **Avancés**.
4. Sélectionnez la case à cocher **Limiter la quantité de bande passante utilisée** et déplacez le curseur pour spécifier la quantité de bande passante utilisée par Sophos AutoUpdate.

**Remarque :** si vous spécifiez plus de bande passante qu'il n'y en a de disponible, Sophos AutoUpdate utilise toute la bande passante.

## 8.8 Journalisation de l'activité de mise à jour

Vous pouvez configurer Sophos AutoUpdate pour qu'il enregistre l'activité de mise à jour dans un fichier journal.

1. Dans le menu **Configurer**, cliquez sur **Mise à jour**.
2. Cliquez sur l'onglet **Journalisation**.
3. Sélectionnez la case à cocher **Enregistrer l'activité de Sophos AutoUpdate**.
4. Dans la zone **Taille maximale du journal**, tapez ou sélectionnez la taille maximale en Mo pour le journal.
5. Dans la liste **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 cette option seulement lorsque vous avez besoin d'un journal détaillé pour la résolution des problèmes.

## 8.9 Consultation du fichier journal de mise à jour

1. Dans le menu **Configurer**, cliquez sur **Mise à jour**.
2. Cliquez sur l'onglet **Journalisation**.
3. Cliquez sur **Consulter le fichier journal**.

## 9 Résolution des problèmes

### 9.1 Echec de la mise à jour

#### 9.1.1 A propos des échecs de mise à jour

Pour en savoir plus sur un échec de mise à jour, examinez le journal de mise à jour : pour plus d'instructions sur la manière de procéder, reportez-vous à la section [Consultation du fichier journal de mise à jour](#) à la page 73.

Les sections ci-dessous expliquent pourquoi la mise à jour peut avoir échoué et comment vous pouvez changer les paramètres pour corriger le problème.

- [Sophos Endpoint Security and Control contacte une source incorrecte pour les mises à jour](#) à la page 74
- [Sophos Endpoint Security and Control ne peut pas utiliser votre serveur proxy](#) à la page 74
- [La mise à jour automatique n'est pas correctement planifiée](#) à la page 75
- [La source des mises à jour n'est pas gérée](#) à la page 75

#### 9.1.2 Sophos Endpoint Security and Control contacte une source incorrecte pour les mises à jour

1. Dans le menu **Configurer**, cliquez sur **Mise à jour**.
2. Sur l'onglet **Emplacement principal**, vérifiez que les détails de l'adresse et du compte sont ceux fournis par votre administrateur.

Pour plus d'informations sur la configuration de l'onglet **Emplacement principal**, reportez-vous à la section [Choix d'une source pour les mises à jour](#) à la page 71.

#### 9.1.3 Sophos Endpoint Security and Control ne peut pas utiliser votre serveur proxy

Si Sophos Endpoint Security and Control se met à jour via Internet, vous devez vous assurer qu'il peut utiliser votre serveur proxy (s'il en existe un).

1. Dans le menu **Configurer**, cliquez sur **Mise à jour**.
2. Sur l'onglet **Emplacement principal**, cliquez sur **Détails du proxy**.
3. Assurez-vous que l'adresse, le numéro du port et les détails du compte du serveur proxy sont corrects.

Pour plus d'informations sur la saisie des détails du proxy, reportez-vous à la section [Mise à jour via un serveur proxy](#) à la page 72.

### 9.1.4 La mise à jour automatique n'est pas correctement planifiée

1. Dans le menu **Configurer**, cliquez sur **Mise à jour**.
2. Cliquez sur l'onglet **Planifier**. (pour plus d'informations sur l'onglet **Planifier**, reportez-vous à la section [Planification des mises à jour](#) à la page 71).
3. Si votre ordinateur est en réseau ou si vous effectuez la mise à jour via une connexion Internet haut débit, sélectionnez **Activer les mises à jour automatiques** et saisissez la fréquence de mise à jour. Si vous effectuez la mise à jour via une connexion par modem, sélectionnez **Vérifier les mises à jour à la connexion**.

### 9.1.5 La source des mises à jour n'est pas gérée

Il se peut que votre entreprise ait déplacé le répertoire (sur le réseau ou sur un serveur web) à partir duquel vous devez procéder à la mise à jour. Ou bien le répertoire n'est peut-être pas géré correctement.

Si vous pensez que c'est le cas, contactez votre administrateur réseau.

## 9.2 Menace non nettoyée

Si Sophos Anti-Virus n'a pas nettoyé de menace de votre ordinateur, c'est peut-être pour l'une des raisons suivantes.

### Le nettoyage automatique est désactivé

Si Sophos Anti-Virus n'a pas tenté de nettoyage, vérifiez que le nettoyage automatique a été activé. Pour activer le nettoyage automatique, reportez-vous à la section [A propos du nettoyage](#) à la page 28 et aux autres rubriques de la section *Nettoyage*. Le nettoyage automatique des adwares et des PUA n'est pas disponible pour le contrôle sur accès.

### Echec du nettoyage

Si Sophos Anti-Virus n'est pas parvenu à nettoyer une menace ("Echec du nettoyage"), c'est peut-être parce qu'il ne peut pas nettoyer ce type de menace ou que vous avez des droits d'accès insuffisants.

### Un contrôle intégral du système est nécessaire

Il se peut que vous deviez exécuter un contrôle intégral de l'ordinateur pour déterminer tous les composants d'une menace à plusieurs composants ou pour détecter une menace dans des fichiers précédemment cachés, avant que Sophos Anti-Virus ne puisse la nettoyer de votre ordinateur.

1. Pour contrôler toutes les unités de disque dur, secteurs de démarrage compris, de l'ordinateur, choisissez la fonction **Effectuer le contrôle de cet ordinateur**. Pour plus d'informations, reportez-vous à la section [Exécution d'un contrôle intégral de l'ordinateur](#) à la page 17.
2. Si la menace n'a pas encore été complètement détectée, c'est peut-être parce que vos droits d'accès sont insuffisants ou que certaines unités ou dossiers de votre ordinateur, contenant les composants de la menace, sont exclus du contrôle. Pour plus d'informations,

reportez-vous à la section [Exclusion de fichiers, de dossiers ou de lecteurs du contrôle sur accès](#) à la page 9. Vérifiez la liste des éléments exclus du contrôle. Si certains éléments figurent dans la liste, supprimez-les de la liste et lancez un nouveau contrôle de l'ordinateur.

### **Le support amovible est protégé en écriture**

Si vous manipulez un support amovible (comme une disquette ou un CD-ROM), assurez-vous qu'il n'est pas protégé en écriture.

### **Le volume NTFS est protégé en écriture**

S'il s'agit de fichiers présents sur un volume NTFS (Windows 2000 ou supérieur), assurez-vous qu'il n'est pas protégé en écriture.

### **Un fragment de virus/spyware a été signalé**

Sophos Anti-Virus ne nettoie pas de fragment de virus/spyware parce qu'il n'a pas trouvé de correspondance exacte du virus/spyware. Reportez-vous à la section [Fragment de virus/spyware signalé](#) à la page 76.

## **9.3 Fragment de virus/spyware signalé**

Si un fragment de virus/spyware est signalé, procédez ainsi :

1. Mettez immédiatement à jour votre protection pour que Sophos Anti-Virus dispose des tout derniers fichiers d'identités virales.
2. Exécutez un contrôle intégral de l'ordinateur

■ [Mise à jour immédiate](#) à la page 71

■ [Exécution d'un contrôle intégral de l'ordinateur](#) à la page 17

Si des fragments de virus/spyware sont toujours signalés, veuillez contacter le support technique de Sophos pour obtenir des conseils.

■ [Support technique](#) à la page 86

Le signalement d'un fragment de virus/spyware indique qu'une partie du fichier correspond à une partie de virus ou à un élément de spyware. Il y a trois causes possibles :

### **Variante d'un virus connu ou d'un élément de spyware**

De nombreux virus ou éléments de spyware nouveaux sont basés sur des existants, afin que les fragments de code typiques d'un virus ou d'un élément de spyware connu apparaisse comme faisant partie d'un nouveau. Si un fragment de virus/spyware est signalé, il est possible que Sophos Anti-Virus ait détecté un nouveau virus ou élément de spyware, qui pourrait devenir actif.

### **Virus corrompu**

De nombreux virus contiennent dans leurs routines de réplication des bogues entraînant une infection incorrecte des fichiers cibles. Une partie inactive du virus (parfois une partie importante) peut apparaître dans le fichier hôte, ceci est détecté par Sophos Anti-Virus. Un virus corrompu ne peut pas se propager.

## Base de données contenant un virus ou un élément de spyware

Lors de l'exécution d'un contrôle intégral, Sophos Anti-Virus peut signaler qu'il y a un fragment de virus/spyware dans un fichier de base de données. Si c'est la cas, ne supprimez pas la base de données. Pour plus de conseils, contactez le support technique de Sophos.

Pour plus d'informations sur comment contacter le support technique, reportez-vous à la section [Support technique](#) à la page 86.

## 9.4 Menace partiellement détectée

Pour contrôler toutes les unités de disque, y compris les secteurs de démarrage, exécutez un contrôle complet de l'ordinateur.

- [Exécution d'un contrôle intégral de l'ordinateur](#) à la page 17

Si la menace n'a pas encore été complètement détectée, c'est peut-être parce que certaines unités ou certains dossiers de votre ordinateur, contenant les composants de la menace, sont exclus du contrôle. Si la liste des exclusions contient certains de ces éléments, supprimez-les, puis effectuez de nouveau un contrôle de votre ordinateur.

- [Exclusion de fichiers, de dossiers ou de lecteurs du contrôle à la demande](#) à la page 15

Si la menace n'a pas été encore complètement détectée, c'est peut-être parce que vous avez des droits d'accès insuffisants.

Il se peut que Sophos Anti-Virus ne parvienne pas à détecter ou à supprimer complètement des menaces avec des composants installés sur des lecteurs réseau.

## 9.5 Disparition d'un adware ou d'une PUA de la quarantaine

Si un élément d'adware ou de PUA détecté par Sophos Anti-Virus a disparu du gestionnaire de quarantaine sans que vous ne preniez de mesures, l'adware ou la PUA peut avoir été autorisé ou nettoyé de la console d'administration ou par un autre utilisateur. Vérifiez la liste des adwares et des PUA autorisés pour voir s'il a été autorisé. Pour savoir comment procéder, reportez-vous à la section [Autorisation d'utilisation d'adwares et de PUA](#) à la page 39.

## 9.6 Ralentissement de l'ordinateur

Si votre ordinateur est très lent, c'est peut-être parce que vous avez une PUA fonctionnant sur votre ordinateur et le surveillant. Si le contrôle sur accès est activé, vous pouvez aussi voir plusieurs alertes de bureau avertissant à propos d'une PUA. Pour résoudre le problème, effectuez les opérations suivantes :

1. Choisissez la fonction **Contrôler cet ordinateur** pour détecter tous les composants de la PUA. Pour plus d'informations, reportez-vous à la section [Exécution d'un contrôle intégral de l'ordinateur](#) à la page 17.

**Remarque :** si, après le contrôle, l'application est partiellement détectée, reportez-vous à l'étape 2 de la section [Menace partiellement détectée](#) à la page 77.

2. Nettoyez l'adware ou la PUA de votre ordinateur. Pour savoir comment procéder, reportez-vous à la section [Traitement des adwares et des PUA en quarantaine](#) à la page 34.

## 9.7 Accès impossible à un disque avec un secteur de démarrage infecté

**Important :** si une console d'administration est utilisée pour administrer Sophos Endpoint Security and Control sur cet ordinateur, il se peut que vous perdiez tous les changements que vous avez effectués.

Par défaut, Sophos Anti-Virus empêche l'accès aux disques amovibles dont les secteurs de démarrage sont infectés.

Pour autoriser l'accès (par exemple, pour copier des fichiers depuis une disquette infectée par un virus de secteur de démarrage) :

1. Dans le menu **Configurer**, pointez votre curseur sur **Antivirus** et cliquez sur **Contrôle sur accès**.
2. Sur l'onglet **Contrôle**, sélectionnez la case à cocher **Permettre l'accès aux lecteurs avec secteurs de démarrage infectés**.

**Important :** dès que vous aurez fini d'accéder à la disquette, dessélectionnez la case à cocher, puis retirez la disquette de l'ordinateur afin qu'elle n'essaie pas de réinfecter l'ordinateur au redémarrage.

## 9.8 Accès impossible à des zones de Sophos Endpoint Security and Control

Si vous ne parvenez pas à utiliser ou à configurer des zones spécifiques de Sophos Endpoint Security and Control, il se peut que ce soit parce que l'accès à ces zones est limité à des membres de groupes d'utilisateurs Sophos particuliers.

Pour plus d'informations sur les groupes d'utilisateurs Sophos, reportez-vous à la section [A propos des groupes Sophos](#) à la page 5.

## 9.9 Guérison des effets secondaires des virus

Après une infection virale, la guérison dépend de la manière dont le virus a infecté l'ordinateur.

### effets secondaires des virus

Certains virus ne laissent aucun effet secondaire tandis que d'autres peuvent en avoir de tellement profonds que, pour guérir, vous allez devoir rétablir le disque dur.

Certains virus apportent peu à peu des changements mineurs aux données. Ce type de corruption peut être difficile à détecter.

### Actions à mener

Il est très important de lire l'analyse de la menace sur le site Web de Sophos et de vérifier soigneusement les documents après désinfection. Reportez-vous à la section [Obtention](#)

[d'informations sur le nettoyage](#) à la page 32 pour savoir comment obtenir plus de détails à propos des effets secondaires des virus sur le site Web de Sophos.

Il est crucial de procéder à des sauvegardes saines. Si vous n'en aviez pas avant l'infection, commencez à les conserver en cas de futures infections.

Parfois, vous pouvez récupérer des données sur les disques endommagés par un virus. Sophos peut fournir des utilitaires pour réparer les dommages occasionnés par certains virus.

Pour plus de conseils, contactez le support technique de Sophos.

Pour plus d'informations sur comment contacter le support technique, reportez-vous à la section [Support technique](#) à la page 86.

## 9.10 Guérison des effets secondaires des adwares et des PUA

La suppression des adwares et des PUA peut avoir certains effets secondaires qui ne peuvent pas être éliminés lors du nettoyage.

### **Le système d'exploitation a été modifié**

Certains éléments d'adware et certains PUA modifient le système d'exploitation Windows, par exemple, changent les paramètres de votre connexion Internet. Sophos Anti-Virus ne peut pas toujours rétablir pour tous les paramètres les valeurs qu'ils avaient avant l'installation de l'adware ou du PUA. Si, par exemple, un élément d'adware ou de PUA a changé la page d'accueil du navigateur, il est impossible pour Sophos Anti-Virus de savoir quel était le paramètre précédent de la page d'accueil.

### **Utilitaires non nettoyés**

Certaines éléments d'adware et certains PUA peuvent installer sur votre ordinateur des utilitaires comme des fichiers .dll ou .ocx. Si un utilitaire est inoffensif (c'est-à-dire s'il ne possède pas les qualités d'un adware ou d'une PUA), par exemple une bibliothèque de langages, et ne fait pas partie intégrante de l'adware ou de la PUA, il se peut que Sophos Anti-Virus ne le détecte pas comme faisant partie de l'adware ou de la PUA. Dans ce cas, le fichier ne sera pas supprimé de votre ordinateur même après le nettoyage sur ce dernier de l'adware ou de la PUA qui l'a installé.

### **L'adware ou la PUA fait partie d'un programme dont vous avez besoin**

Parfois, un élément d'adware ou de PUA fait partie d'un programme que vous avez intentionnellement installé et doit être présent pour le fonctionnement du programme. Si vous supprimez l'adware ou la PUA, le programme peut arrêter de fonctionner sur votre ordinateur.

### **Que faire**

Il est très important que vous lisiez l'analyse de la menace sur le site Web de Sophos. Reportez-vous à la section [Obtention d'informations sur le nettoyage](#) à la page 32 pour savoir comment voir sur le site Web de Sophos les détails sur les effets secondaires d'un adware ou d'un PUA.

Pour pouvoir revenir à l'état précédent de votre système et récupérer ses paramètres, effectuez des sauvegardes régulières de votre système. Effectuez par ailleurs des copies de sauvegarde des fichiers exécutables originaux des programmes que vous voulez utiliser.

Pour plus d'informations ou de conseils pour récupérer des effets secondaires d'un adware et d'une PUA, contactez le support technique Sophos.

Pour plus d'informations sur comment contacter le support technique, reportez-vous à la section [Support technique](#) à la page 86.

## 9.11 Erreur de mot de passe

Si vous essayez de planifier un contrôle personnalisé et si un message d'erreur apparaît concernant le mot de passe, veillez à ce que :

- Le mot de passe saisi est bien celui qui correspond au compte utilisateur
- Le mot de passe n'est pas laissé vierge

Pour s'assurer que le mot de passe est correct, vérifiez les propriétés du compte utilisateur dans **Comptes d'utilisateurs** dans **Panneau de configuration**.

## 9.12 Message d'erreur "Echec du service"

### Symptômes

L'un des messages d'erreur suivants apparaît dans la zone de notification :

- Antivirus et HIPS : échec du service
- Pare-feu : échec du service

### Causes

L'un des services Sophos Endpoint Security and Control de votre ordinateur a échoué et doit être redémarré.

### Résolution du problème

1. A l'aide de Windows, ouvrez les Services.
2. Procédez de l'une des manières suivantes :
  - Si vous voyez le message d'erreur **Anti-virus et HIPS : échec du service**, cliquez avec le bouton droit de la souris sur **Sophos Anti-Virus**, puis cliquez sur **Redémarrer**.
  - Si vous voyez le message d'erreur **Pare-feu : échec du service**, cliquez avec le bouton droit de la souris sur **Sophos Client Firewall**, puis cliquez sur **Redémarrer**.

### Remarques

- Pour ouvrir les Services, cliquez sur **Démarrer**, cliquez sur **Panneau de configuration**, cliquez deux fois sur **Outils d'administration**, puis deux fois sur **Services**.

## 10 Glossaire

<b>Adwares et applications potentiellement indésirables</b>	Un adware affiche de la publicité, comme des messages intempestifs, qui affecte la productivité des utilisateurs et l'efficacité du système. Une application potentiellement indésirable ou PUA (potentially unwanted application) est une application qui n'est pas malveillante en soi mais dont l'utilisation est généralement considérée comme inappropriée pour la majorité des réseaux professionnels.
<b>Analyse comportementale runtime</b>	Analyse dynamique effectuée par la détection des comportements suspects et par celle des dépassements de la mémoire tampon.
<b>Application contrôlée</b>	Application interdite d'exécution sur votre ordinateur par la stratégie de sécurité de votre entreprise.
<b>Application fiable</b>	Application disposant de l'accès complet et inconditionnel à Internet.
<b>Arborescence</b>	Vue qui contrôle quelles données la visionneuse de journaux affiche dans sa vue des données.
<b>Barre de description</b>	Dans le visualiseur de journaux, barre qui apparaît au-dessus de la vue des données et qui contient le nom de l'élément couramment sélectionnée dans l'arborescence.
<b>Bloqué</b>	Applications contrôlées interdites d'exécution par le contrôle sur accès et qui sont nommées "bloquées".
<b>Boîte de dialogue d'apprentissage</b>	Boîte de dialogue demandant à l'utilisateur de choisir d'autoriser ou de bloquer une activité réseau lorsqu'une application inconnue en demande l'accès.
<b>Configuration principale</b>	Configuration du pare-feu utilisée sur le réseau d'entreprise auquel l'utilisateur se connecte pour son activité professionnelle quotidienne.
<b>Configuration secondaire</b>	Configuration du pare-feu utilisée lorsque les utilisateurs ne sont pas connectés au réseau d'entreprise principal mais à un autre réseau tel le réseau sans fil d'un hôtel ou d'un aéroport ou tout autre réseau d'entreprise.
<b>Contrôle des données</b>	Fonction qui réduit la perte accidentelle de données depuis les stations de travail. Elle se déclenche lorsque l'utilisateur d'une station de travail essaie de transférer un fichier qui répond aux critères définis dans la stratégie et dans les règles de contrôle des données. Par exemple, lorsqu'un utilisateur tente de copier une feuille de calcul contenant une liste de données clients dans un dispositif de stockage amovible ou de télécharger en amont un document marqué comme confidentiel dans un compte de

	messagerie web, le contrôle des données va, s'il est configuré pour cela, bloquer le transfert.
<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>Contrôle normal</b>	Contrôle seulement les parties d'un fichier susceptibles d'être infectées par un virus.
<b>Contrôle par clic droit</b>	Contrôle d'un ou de plusieurs fichiers dans Windows Explorer ou sur le Bureau que vous lancez à l'aide d'un menu de raccourcis.
<b>Contrôle planifié</b>	Contrôle de l'ordinateur ou de certaines parties de ce dernier, qui s'exécute à une heure ou à des heures définies.
<b>Contrôle sur accès</b>	Contrôle qui intercepte les fichiers au moment de leur accès (copie, déplacement, enregistrement ou ouverture) et qui autorise l'accès à ces fichiers uniquement s'ils ne représentent pas une menace pour votre ordinateur ou si leur utilisation est autorisée.
<b>Contrôle à la demande</b>	Contrôle que vous lancez. Vous pouvez utiliser un contrôle à la demande afin de contrôler tout ce que vous désirez, que ce soit un seul fichier ou votre ordinateur tout entier.
<b>Contrôle étendu</b>	Contrôle toutes les parties d'un fichier.
<b>Correspondance</b>	Doit être égal au contenu défini dans une Liste de contrôle de contenu.
<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>Détection des dépassements de la mémoire tampon</b>	Détecte les attaques par dépassement de la mémoire tampon.
<b>Erreur de contrôle</b>	Erreur lors du contrôle d'un fichier, par exemple l'accès refusé.
<b>Événement de menace</b>	Détection ou désinfection d'une menace.
<b>Événement de pare-feu</b>	Situation qui a lieu lorsqu'une application inconnue ou le système d'exploitation sur un ordinateur tente de communiquer avec un autre ordinateur par le biais d'une connexion réseau d'une manière qui n'a pas été requise par les applications s'exécutant sur cet ordinateur.
<b>Fichier d'identité virale (IDE)</b>	Fichier qui permet à Sophos Anti-Virus de détecter et de désinfecter un virus, ver, cheval de Troie ou élément de spyware particulier.

<b>Fichier suspect</b>	Un fichier suspect est un fichier qui comporte une combinaison de caractéristiques généralement, mais pas exclusivement, trouvées dans les virus.
<b>Gestionnaire d'autorisation</b>	Module qui vous permet d'autoriser les adwares et PUA, les fichiers suspects et les applications qui révèlent un comportement suspect et un dépassement de la mémoire tampon.
<b>Gestionnaire de quarantaine</b>	Module qui permet de visualiser et de traiter les éléments qui ont été placés en quarantaine.
<b>HIPS (système de prévention des intrusions sur l'hôte)</b>	Terme général désignant une analyse du comportement avant exécution et une analyse du comportement runtime.
<b>ICMP</b>	Abréviation de "Internet Control Message Protocol." Protocole Internet multiréseau qui fournit des corrections d'erreur et toutes autres informations concernant le traitement des paquets d'adresses IP.
<b>Inspection dynamique (stateful)</b>	Technologie de pare-feu qui conserve un tableau des sessions TCP et UDP actives et autorise les chemins étroits par lesquels le trafic peut passer.
<b>Liste de contrôle du contenu (LCC)</b>	Ensemble de conditions qui spécifient le contenu d'un fichier, par exemple, des numéros de carte de crédit ou de débit ou les détails d'un compte bancaire ainsi que d'autres formes d'informations d'identification personnelles. Il existe deux types de Liste de contrôle du contenu : La Liste de contrôle du contenu des SophosLabs et la Liste de contrôle du contenu personnalisée.
<b>Messagerie instantanée</b>	Catégorie d'applications contrôlées comprenant des applications clientes de messagerie instantanée (par exemple, MSN).
<b>Mode de fonctionnement</b>	Paramètre qui détermine si le pare-feu agit sur consultation de l'utilisateur (mode interactif) ou automatiquement (modes non interactif).
<b>Mode interactif</b>	Mode dans lequel le pare-feu affiche une ou plusieurs boîtes de dialogue d'apprentissage lorsqu'il détecte du trafic réseau pour lequel il n'a pas de règle spécifiée.
<b>Mode non interactif</b>	Mode dans lequel le pare-feu bloque ou autorise tout le trafic réseau pour lequel il n'a pas de règle spécifiée.
<b>NetBIOS</b>	Abréviation de "Network Basic Input/Output System", c'est-à-dire système de base d'entrée-sortie de réseau local. Logiciel fournissant une interface entre le système d'exploitation, le bus d'entrée/sortie et le réseau. Presque tous les réseaux locaux de type Windows sont basés sur NetBIOS.

<b>Nettoyage</b>	Le nettoyage élimine les menaces sur votre ordinateur en supprimant un virus d'un fichier ou d'un secteur de démarrage, en déplaçant ou en supprimant un fichier suspect ou en supprimant un élément d'adware ou de PUA. En revanche, il n'annule pas les actions que la menace a déjà exécutées. Il n'est pas disponible pour les menaces détectées par le contrôle des pages web car les menaces ne sont pas téléchargées sur votre ordinateur. C'est la raison pour laquelle aucune mesure n'est nécessaire.
<b>Nettoyage automatique</b>	Nettoyage effectué sans votre intervention ou consentement.
<b>Nettoyage manuel</b>	Nettoyage exécuté grâce à des désinfecteurs ou des utilitaires spéciaux, ou en supprimant des fichiers manuellement.
<b>Paramètres de nettoyage du journal</b>	Paramètres qui contrôlent quand les enregistrements sont supprimés.
<b>Paramètres de processus</b>	Paramètres qui spécifient si l'accès réseau devrait être autorisé à des processus modifiés ou cachés.
<b>Paramètres ICMP</b>	Paramètres spécifiant quels types de communications d'administration réseau sont autorisées.
<b>Processus caché</b>	Application qui 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 : elles lancent une application fiable pour accéder au réseau plutôt que de le faire elles-mêmes.
<b>Protocole réseau</b>	Ensemble de règles et de normes prévues pour permettre aux ordinateurs de se connecter les uns aux autres via un réseau et d'échanger des informations avec le moins d'erreurs possibles.
<b>Périphérique de stockage</b>	Périphériques de stockage amovibles (lecteurs flash USB, lecteurs PC Card et disques durs externes), lecteurs de CD/DVD, lecteurs de disquette et périphériques de stockage amovibles sécurisés (lecteurs flash USB SanDisk Cruzer Enterprise, Kingston Data Traveller, IronKey Enterprise, et IronKey Basic avec chiffrement de matériel).
<b>Rawsocket</b>	Les rawsockets permettent aux processus de contrôler tous les aspects des données qu'ils envoient sur le réseau et peuvent être utilisées à des fins malveillantes.
<b>Rootkit</b>	Cheval de Troie ou technologie utilisée pour dissimuler la présence d'un objet malveillant (processus, fichier, clé de registre ou port réseau) à l'utilisateur de l'ordinateur ou à l'administrateur.
<b>Règle d'application</b>	Règle qui s'applique uniquement aux paquets de données transférées via le réseau vers ou depuis une application donnée.

<b>Règle de contenu</b>	Règle contenant une ou plusieurs Listes de contrôle du contenu et spécifiant l'action prise si l'utilisateur tente de transférer vers la destination spécifiée des données qui correspondent à toutes les Listes de contrôle du contenu dans la règle.
<b>Règle globale à haute priorité</b>	Règle appliquée avant toute autre règle globale ou d'application.
<b>Règle personnalisée</b>	Règle créée par l'utilisateur pour spécifier les circonstances dans lesquelles l'exécution d'une application est autorisée.
<b>Règle système</b>	Règle appliquée à tous les applications et qui autorise ou bloque l'activité réseau d'un système de bas niveau.
<b>Règles globales</b>	Règles appliquées à toutes les connexions réseau et aux applications qui n'ont pas encore de règle. Leur priorité est inférieure à celles définies sur la page Réseau local. Elles sont également une priorité moins élevée que les règles d'applications (sauf mention contraire de l'utilisateur).
<b>Somme de contrôle</b>	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.
<b>Spyware</b>	Programme qui s'installe furtivement, par subterfuge ou par ingénierie sociale sur un ordinateur et qui envoie depuis ce dernier des informations à un tiers sans l'autorisation ou à l'insu de son utilisateur.
<b>Stratégie de pare-feu</b>	Paramètres émis par la console d'administration et que le pare-feu utilise pour surveiller la connexion de l'ordinateur à Internet et à tout autre réseau.
<b>Trafic inconnu</b>	Accès au réseau par une application ou un service pour lequel le pare-feu n'a pas de règle.
<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.
<b>Virus non identifié</b>	Virus pour lequel il n'existe pas d'identité spécifique.
<b>Visualiseur de journaux</b>	Formulaire où l'utilisateur peut voir les informations provenant d'une base de données d'événements, comme des connexions ayant été autorisées ou bloquées, le journal système et toutes les alertes qui ont été signalées.
<b>Voix sur IP</b>	Catégorie d'applications contrôlées incluant des applications clientes de voix sur IP.
<b>Vue des données</b>	Vue qui affiche différentes données en fonction de l'élément sélectionné dans l'arborescence.

## 11 Support technique

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

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

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

## 12 Copyright

Copyright © 2009 Sophos Group. Tous droits réservés. Aucune partie de cette publication ne peut être reproduite, stockée dans un système de recherche documentaire ou transmise, sous quelque forme ou par quelque moyen que ce soit, électronique, mécanique, photocopie, enregistrement ou autre sauf si vous possédez une licence valide, auquel cas vous pouvez reproduire la documentation 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 Plc et de Sophos Group. Sophos Group. Tous les autres noms de produits et d'entreprises cités dans ce document sont des marques ou des marques déposées de leurs propriétaires respectifs.

Les logiciels Sophos mentionnés dans le présent document 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.com](mailto:support@sophos.com) 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>

## Index

### A

- accès aux disques 78
- activation des boîtes de dialogue d'apprentissage des sommes de contrôle 54
- activation du contrôle sur accès 8
- adware 77, 79
  - autorisation 39
  - nettoyage automatique 30
  - recherche de 22
- adwares autorisés, blocage 39
- adwares en quarantaine, traitement 34
- ajouter des utilisateurs aux groupes Sophos 6
- analyse comportementale runtime 12
- analyses des menaces 32
- antivirus
  - configuration de la journalisation des événements 26
  - configuration de la messagerie de bureau 24
  - configuration de la messagerie SNMP 26
  - configuration des alertes par courriel 24
- applications
  - autorisation 49
  - blocage 49
  - utilisation des sommes de contrôle pour authentifier 62
- applications contrôlées
  - autorisation 38
  - recherche de 13
  - traitement de 38
- attribution d'un nouveau nom aux contrôles personnalisés 20
- authentifier les applications, utilisation des sommes de contrôle pour 62
- autorisation
  - adware 39
  - applications 49
  - applications contrôlées 38
  - comportement suspect 37, 39
  - dépassements de la mémoire tampon 37, 39
  - email, courriel 46
  - fichiers suspects 39
  - navigateurs Web 47
  - partage de fichiers et d'imprimantes 48
  - processus cachés 61
  - PUA 39

autorisation (*suite*)

- rawsockets 61
- téléchargements FTP 47
- trafic du réseau local (LAN) 48

### B

- bande passante utilisée pour la mise à jour, limitation 73
- blocage
  - adwares autorisés 39
  - applications 49
  - PUA autorisées 39
- boîtes de dialogue d'apprentissage des sommes de contrôle
  - activation 54
  - Mode interactif 53

### C

- comportement suspect
  - autorisation 37, 39
  - détection 12
- comportements suspects en quarantaine, traitement 37
- configuration 17
  - édition de rapports centralisée 64
  - alerte par courriel pour l'antivirus 24
  - contrôle sur accès 9
  - contrôles personnalisés 19
  - droits utilisateurs pour le Gestionnaire de quarantaine 6
  - journal du contrôle 27
  - journalisation des événements antivirus 26
  - la journalisation 67
  - messagerie de bureau pour l'antivirus 24
  - messagerie SNMP pour l'antivirus 26
- contrôle à la demande
  - exclusion d'éléments de 15
  - spécification des extensions de fichier 14
- contrôle d'éléments uniques 17
- contrôle d'un seul élément 17
- contrôle de tous les fichiers 22
- contrôle des données, désactivation temporaire 43
- contrôle des périphériques 41
  - blocage du pont de réseau 41
  - périphériques contrôlés 41
- contrôle par clic droit 17
- contrôle par clic droit, configuration 17

- contrôle sur accès
  - activation 8
  - configuration 9
  - désactivation 8
  - exclusion d'éléments de 9
  - spécification des extensions de fichier 8
- contrôle sur accès et contrôle à la demande, différences 8
- contrôler dans les fichiers archive 21
- contrôles à la demande, types de 13
- contrôles intégraux de l'ordinateur, exécution 17
- contrôles par clic droit, exécution 17
- contrôles personnalisés
  - attribution d'un nouveau nom 20
  - configuration 19
  - création 18
  - exécution 20
  - planification 19
  - suppression 20
- création de contrôles personnalisés 18

## D

- dépassements de la mémoire tampon
  - autorisation 37, 39
  - détection 12
- désactivation de la recherche des applications contrôlées 13
- désactivation du contrôle 41
- désactivation du contrôle sur accès 8
- désactivation du pare-feu 46
- désinfection 75
- détection des comportements suspects 12
- détection des dépassements de la mémoire tampon 12
- détection partielle 77
- droits d'accès 5, 78
- droits utilisateur 5, 78
- droits utilisateurs pour le Gestionnaire de quarantaine, configuration 6

## E

- édition de rapports centralisée, configuration 64
- effets secondaires 79
- éléments suspects, préautorisation 40
- email, courriel, autorisation 46
- enregistrements du journal
  - filtrage 69
- erreur de mot de passe 80

- exclusion d'éléments du contrôle à la demande 15
- exclusion des éléments du contrôle sur accès 9
- exécution de contrôles intégraux de l'ordinateur 17
- exécution de contrôles par clic droit 17
- exécution de contrôles personnalisés 20
- exportation d'enregistrements depuis le visualiseur de journaux du pare-feu 69, 70
- exportation des fichiers de configuration du pare-feu 54

## F

- fichiers archive, contrôle 21
- fichiers de configuration du pare-feu
  - exportation 54
  - importation 55
- fichiers suspects
  - autorisation 39
  - nettoyage automatique 31
  - recherche de 22
- fichiers suspects en quarantaine, traitement 36
- filtrage des enregistrements du journal 69
- filtrage des messages ICMP 49
- fragment 75
- fragment signalé, résolution des problèmes 76

## G

- gestionnaire de quarantaine 32
- groupes d'utilisateurs 5, 78
- Groupes Sophos 5
  - ajout d'utilisateur à 6
- guérison des effets secondaires 79

## I

- icône de la zone de notification 74
- icônes
  - éléments à contrôler 18
- importation des fichiers de configuration du pare-feu 55
- informations sur la sécurité 32
- informations sur le nettoyage 32
- interruption du contrôle 41
- introduction
  - que faire 45

## J

- journal du contrôle
  - configuration 27
  - visualisation 27
- journal du contrôle personnalisé
  - visualisation 21
- journalisation des mises à jour 73

## L

- la journalisation
  - configuration 67
- limitation de la bande passante utilisée pour la mise à jour 73

## M

- menace partiellement détectée 77
- messages ICMP
  - filtrage 49
  - information sur 50
- mise à jour 71, 73, 74
- mise à jour immédiate 71
- mise à jour via la connexion par modem 71
- mode de fonctionnement, changement en interactif 51
- mode interactif
  - messages d'application 53
  - messages de protocole 52
  - messages de rawsocket 53
  - messages des processus cachés 52
- Mode interactif
  - boîtes de dialogue d'apprentissage des sommes de contrôle 53
- mode interactif, à propos de 51
- mode interactif, activation 51
- mode non interactif, change pour un 51

## N

- navigateurs Web, autorisation 47
- nettoyage 28
  - résolution des problèmes 75
- nettoyage automatique
  - adware 30
  - fichiers suspects 31
  - PUA 30
  - spyware 29

- nettoyage automatique (*suite*)
  - virus 29

## O

- ordinateur lent, résolution des problèmes 77

## P

- Page d'accueil 4
- paramétrage d'une règle 57, 58
- paramétrage des règles globales 56, 58, 60
- paramètres du contrôle par clic droit 28
- paramètres du contrôle personnalisé 28
- paramètres du contrôle sur accès 28
- pare-feu
  - désactivation 46
- partage d'imprimantes, autorisation 48
- partage de fichiers et d'imprimantes, autorisation 48
- partage de fichiers, autorisation 48
- planification d'un contrôle 80
- planification des contrôles personnalisés 19
- planification des mises à jour 71
- préautorisation d'éléments suspects 40
- priorité de règle 55
- processus cachés, autorisation 61
- PUA 77, 79
  - autorisation 39
  - nettoyage automatique 30
  - recherche de 22
- PUA autorisées, blocage 39

## R

- rawsockets, autorisation 61
- recherche d'adwares et de PUA 22
- Recherche des applications contrôlées 13
- Recherche des applications contrôlées, désactivation 13
- recherche des fichiers suspects 22
- recherche des rootkits 23
- rechercher des virus Mac 22
- règle
  - paramétrer 57, 58
- Règle
  - paramétrer 57
- règles globales
  - paramètre 58, 60

Règles globales  
  paramètre 56  
réinitialisation des sommes de contrôle des fichiers  
contrôlés 23  
rootkits, recherche de 23

## S

secteur de démarrage infecté 78  
serveur principal 71  
serveur proxy 72  
serveur secondaire 72  
sommes de contrôle des fichiers contrôlés,  
réinitialisation 23  
sommes de contrôle, utilisation pour authentifier  
les applications 62  
spécification des extensions de fichier pour le  
contrôle sur accès 8  
spyware  
  nettoyage automatique 29  
spywares en quarantaine, traitement 33  
support 86  
support technique 86  
suppression de contrôles personnalisés 20

## T

téléchargements FTP, autorisation 47

tous les fichiers, contrôle 22  
trafic du réseau local (LAN), autorisation 48  
traitement des adwares en quarantaine 34  
traitement des applications contrôlées 38  
Traitement des comportements suspects en  
quarantaine 37  
traitement des fichiers suspects en quarantaine 36  
Traitement des PUA en quarantaine 34  
Traitement des spywares en quarantaine 33  
traitement des virus en quarantaine 33  
types de contrôle à la demande 13

## V

virus  
  guérison des effets secondaires 78  
  nettoyage automatique 29  
virus en quarantaine, traitement 33  
virus Mac, rechercher 22  
visualisation  
  journal du contrôle 27  
  journal du contrôle personnalisé 21  
visualiseur de journaux  
  à propos de 66  
visualiseur de journaux du pare-feu  
  exportation d'enregistrements 69, 70