

SOPHOS

SMALL BUSINESS EDITION

Sophos Control Center Aide

Version du produit : 4.0

Date du document : septembre 2009



Table des matières

| | |
|---|----|
| 1 A propos du Sophos Control Center..... | 3 |
| 2 Présentation du Sophos Control Center..... | 4 |
| 3 Vérification de la protection de mon réseau..... | 8 |
| 4 Protection des nouveaux ordinateurs..... | 10 |
| 5 Mise à jour des ordinateurs..... | 12 |
| 6 Résolution des alertes et des menaces..... | 14 |
| 7 Re-protection des ordinateurs..... | 18 |
| 8 Surveillance des ordinateurs protégés..... | 19 |
| 9 Consultation des événements..... | 23 |
| 10 Configuration d'un contrôle..... | 26 |
| 11 Configuration des mises à jour..... | 35 |
| 12 Configuration du pare-feu..... | 38 |
| 13 Configuration du contrôle des applications..... | 42 |
| 14 Configuration du contrôle des périphériques..... | 45 |
| 15 Gestion des notifications..... | 48 |
| 16 Gestion des rapports..... | 52 |
| 17 Résolution des problèmes..... | 57 |
| 18 Support technique..... | 58 |
| 19 Copyright..... | 59 |

1 A propos du Sophos Control Center

Grâce au Sophos Control Center, vous pouvez :

- Installer les logiciels antivirus et de pare-feu sur votre réseau.
Les licences Sophos Security Suite et Sophos Computer Security incluent le pare-feu au contraire de la licence Sophos Anti-Virus.
- Maintenir à jour automatiquement via Internet les logiciels.
- Configurer de manière centralisée la détection et le nettoyage des virus, vers, chevaux de Troie, spywares et applications potentiellement indésirables tels que les adwares, les composeurs, les outils d'administration à distance et les outils de piratage.
- Contrôler quelles applications peuvent fonctionner sur le réseau.
- Empêcher les utilisateurs d'utiliser des périphériques non autorisés sur les systèmes d'extrémité.
- Configurer de manière centralisée le pare-feu, le contrôle des applications et le contrôle des périphériques pour les ordinateurs de votre réseau.
- Surveiller le réseau et vérifier que les ordinateurs sont protégés et sont conformes à la configuration centrale.
- Constituer un récapitulatif des menaces.
- Générer des rapports sur les tendances des menaces.

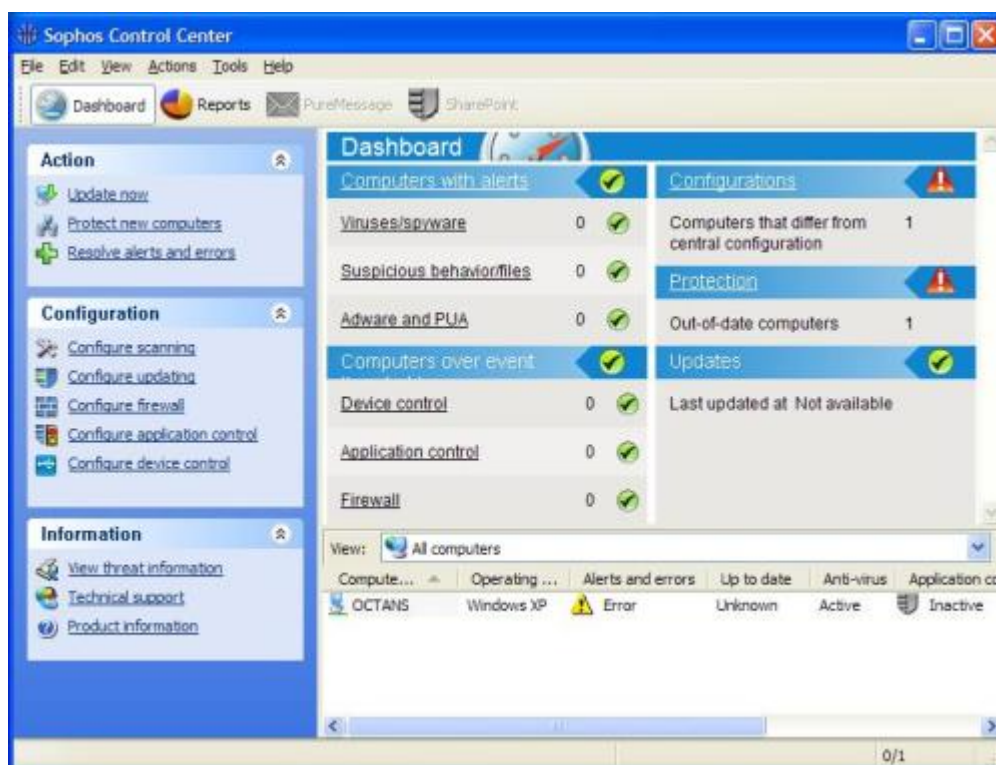
Vous pouvez utiliser Sophos Control Center pour protéger les :

- Ordinateurs Windows 2000 et supérieur
- Windows 98 (SE)
- Ordinateurs Mac OS X

2 Présentation du Sophos Control Center

2.1 A propos de l'interface

Vous pouvez utiliser et configurer les logiciels Sophos Anti-Virus et Sophos Client Firewall via l'interface du Sophos Control Center dont vous pouvez maintenant voir la fenêtre. Les fonctionnalités principales sont décrites ci-dessous :



Menu Actions

Ce menu vous permet de mettre à jour les logiciels antivirus et (si votre licence l'inclut) de pare-feu, de protéger les nouveaux ordinateurs et de résoudre les menaces.

Menu Configuration

Ce menu vous permet de configurer les logiciels antivirus et de pare-feu et de paramétrer des alertes sur les menaces.

Menu Informations

Ce menu vous permet d'accéder aux informations sur les menaces sur le site Web de Sophos, au support technique et aux informations sur les produits.

Barre d'outils

■ Rapports

Cliquez sur ce bouton pour ouvrir la boîte de dialogue **Gestionnaire des rapports**. Pour plus d'instructions sur la manière de générer des rapports, reportez-vous à la section [Génération d'un rapport](#) à la page 52.

■ PureMessage

Si vous êtes un utilisateur PureMessage, vous pouvez, en cliquant sur ce bouton, lancer la console PureMessage. Ce bouton est activé seulement si PureMessage est installé sur le même ordinateur que le Sophos Control Center.

■ SharePoint

Si vous êtes un utilisateur Sophos pour Microsoft SharePoint, vous pouvez, en cliquant sur ce bouton, lancer Sophos pour Microsoft SharePoint. Ce bouton est activé seulement si Sophos pour SharePoint est installé sur le même ordinateur que le Sophos Control Center.

Tableau de bord

Le **tableau de bord** donne un aperçu rapide de l'état de la sécurité du réseau. Pour afficher ou masquer le tableau de bord, cliquez sur le bouton **Tableau de bord** de la barre d'outils. Pour plus d'informations sur le tableau de bord, reportez-vous à la section [Aperçu du tableau de bord](#) à la page 8.

La liste des ordinateurs

Ceci vous permet de voir :

- Si la protection antivirus et de pare-feu est active, inactive ou non installée.
- Si les ordinateurs sont conformes à la configuration définie de manière centralisée via le Sophos Control Center.
- Où les alertes ont lieu.

Pour plus d'explications concernant les icônes affichées dans la liste des ordinateurs, reportez-vous à la section [Que signifient les icônes ?](#) à la page 5.

Pour trier la liste des ordinateurs par colonne, cliquez sur l'en-tête de la colonne par laquelle vous voulez effectuer ce tri.



Pour visualiser les informations relatives à un ordinateur, telles que les versions et l'état des logiciels antivirus et de pare-feu, les alertes à traiter et l'historique de détection des menaces, cliquez deux fois sur cet ordinateur dans la liste pour afficher la fenêtre **Détails de l'ordinateur**. Autrement, sélectionnez l'ordinateur, cliquez dessus avec le bouton droit de la souris et sélectionnez **Voir les détails de l'ordinateur**.

2.2 Que signifient les icônes ?




Dans la liste des ordinateurs, les icônes sont utilisées pour indiquer :

- les alertes
- la protection est désactivée ou non à jour
- l'état de chaque ordinateur, par exemple, si le logiciel est en cours d'installation.






Alertes


| Icône | Description |
|---|--|
|  | L'apparition d'un signal d'avertissement rouge dans la colonne Alertes et erreurs indique qu'un virus, un ver, un cheval de Troie, un spyware ou un comportement suspect a été détecté. |
|  | <p>L'apparition d'un signal d'avertissement jaune dans la colonne Alertes et erreurs indique l'un des problèmes suivants :</p> <ul style="list-style-type: none"> ■ Un fichier suspect a été détecté. ■ Un adware ou toute autre application potentiellement indésirable a été détecté. ■ Une erreur s'est produite. <p>L'apparition d'un signal d'avertissement jaune dans la colonne Configuration centralisée indique que l'ordinateur n'est pas conforme à la configuration centralisée comme les autres ordinateurs de son réseau.</p> |

Protection désactivée ou non à jour



| Icône | Description |
|---|---|
|  | Un bouclier gris et le mot "Inactif" dans la colonne Antivirus de la liste des ordinateurs signifie que le contrôle sur accès est inactif. |
|  | Un pare-feu gris et le mot "Inactif" dans la colonne Pare-feu signifie que le pare-feu est désactivé. |
|  | Une horloge et le mot "Non" dans la colonne A jour signifie que les logiciels ne sont pas à jour. |

Etat de l'ordinateur

| Icône | Description |
|---|---|
|  | Un ordinateur bleu signifie que l'ordinateur est administré par le Sophos Control Center. |
|  | Un ordinateur surmonté d'une flèche jaune signifie que l'installation des logiciels antivirus et de pare-feu est en attente. |
|  | Un ordinateur surmonté d'une flèche verte signifie que l'installation est en cours. |
|  | Un ordinateur surmonté d'un sablier signifie que le composant de mise à jour de Sophos Anti-Virus a été installé et qu'il est désormais en train de télécharger la plus récente version du produit. |
|  | Un ordinateur gris signifie que l'ordinateur n'est pas administré par le Sophos Control Center. |

| Icône | Description |
|---|--|
|  | Un ordinateur près duquel figure une croix rouge signifie que l'ordinateur est déconnecté. |

Etat du Tableau de bord

| Icône | Description |
|---|---|
|  | Une icône verte correspond à l'état "normal". Le nombre d'ordinateurs affectés est en dessous du seuil d'alerte défini. |
|  | Une icône rouge indique que le seuil d'alerte défini a été dépassé pour la catégorie correspondante. |

2.3 Priorité des alertes

S'il y a plusieurs alertes sur un ordinateur, l'icône ayant la priorité la plus élevée s'affiche dans la liste des ordinateurs. Les types d'alertes sont répertoriés ci-dessous par ordre de priorité décroissant.

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

3 Vérification de la protection de mon réseau

3.1 Aperçu du tableau de bord

Vous pouvez utiliser le tableau de bord pour vérifier l'état de la sécurité de votre réseau. Pour afficher ou masquer le tableau de bord, cliquez sur le bouton **Tableau de bord** de la barre d'outils.

| Dashboard | |
|---|---|
| Computers with alerts (0 alerts, green checkmark) | Configurations (1 warning, red exclamation mark) |
| <u>Viruses/spyware</u> 0 (green checkmark) | Computers that differ from central configuration 1 |
| <u>Suspicious behavior/files</u> 0 (green checkmark) | Protection (1 warning, red exclamation mark) |
| <u>Adware and PUA</u> 0 (green checkmark) | Out-of-date computers 1 |
| Computers over event threshold (0 events, green checkmark) | Updates (1 update, green checkmark) |
| <u>Device control</u> 0 (green checkmark) | Last updated at Not available |
| <u>Application control</u> 0 (green checkmark) | |
| <u>Firewall</u> 0 (green checkmark) | |

L'interface du tableau de bord est composé de cinq sections avec des indicateurs d'état de sécurité affichant l'état de chaque section d'après la valeur du seuil :

Ordinateurs avec alertes

Cette section indique le nombre d'ordinateurs administrés avec des alertes concernant :

- Des virus et des spywares connus et inconnus
- Des comportements et des fichiers suspects
- Des adwares et d'autres applications potentiellement indésirables

Pour voir une liste des ordinateurs administrés avec des alertes à traiter, cliquez sur le titre de la section **Ordinateurs avec alertes**.

Ordinateurs au-dessus du seuil

La section affiche le nombre d'événements rencontrés sous le contrôle des périphériques, les applications contrôlées et les applications bloquées par le pare-feu avec des indicateurs d'état affichant l'état de chaque catégorie.

Configurations

Cette section affiche le nombre d'ordinateurs administrés qui n'ont pas la configuration centralisée.

Pour voir une liste des ordinateurs administrés qui diffèrent de la configuration centralisée, cliquez sur le titre de la section **Configurations**.

Protection

Cette section indique le nombre d'ordinateurs administrés et connectés sur lesquels Sophos Anti-Virus n'est pas à jour ou utilise des données de détection inconnues.

Pour voir une liste des ordinateurs administrés connectés et non à jour, cliquez sur le titre de la section **Protection**.

Mises à jour

Cette section indique la date et l'heure de la dernière mise à jour depuis Sophos.

3.2 Configuration du tableau de bord

Le tableau de bord affiche des indicateurs d'état soit d'après le pourcentage d'ordinateurs administrés avec des alertes ou des erreurs à traiter soit d'après le temps écoulé depuis la dernière mise à jour depuis Sophos. Si un niveau est dépassé, l'indicateur d'état du tableau de bord change.

Pour configurer le tableau de bord pour qu'il indique le statut :

1. Dans le menu **Outils**, sélectionnez **Configurer le tableau de bord**.
La boîte de dialogue **Configuration du tableau de bord** apparaît.
2. Changez le cas échéant les valeurs seuil dans les zones de texte des niveaux.
 - a) Sous **Ordinateurs avec des alertes à traiter**, saisissez un pourcentage d'ordinateurs administrés affectés par un problème particulier pour déclencher le changement de l'indicateur respectif.
 - b) Sous **Ordinateurs avec des événements**, saisissez le nombre d'événements après lesquels les alertes doivent être déclenchées.
 - c) Sous **Configuration et protection**, saisissez un pourcentage d'ordinateurs administrés affectés pour déclencher le changement de l'indicateur respectif.
 - d) Sous **Protection la plus récente depuis Sophos**, saisissez le nombre d'heures écoulées après lesquelles la dernière mise à jour réussie de Sophos doit être reçue. Ceci déclenche le changement de l'indicateur "Mises à jour".
 - e) Cliquez sur **OK**.

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

Vous pouvez aussi paramétrer l'envoi d'alertes par courriel aux destinataires de votre choix lorsqu'un seuil d'alerte a été atteint. Pour plus d'informations, reportez-vous à la section [Configuration des alertes par courriel sur l'état du réseau](#) à la page 49.

4 Protection des nouveaux ordinateurs

4.1 Protection des nouveaux ordinateurs

Si de nouveaux ordinateurs sont ajoutés à votre réseau, vous devez les protéger avec les logiciels antivirus et (si votre licence l'inclut) de pare-feu.

Remarque : seuls les ordinateurs Windows 2000 et supérieur sont recherchés en vue d'une installation car l'installation ou la mise à niveau automatique n'est pas possible sur les ordinateurs Windows 98 ou Mac OS X.

Si vous avez des ordinateurs qui exécutent un système d'exploitation différent (comme Windows 98 ou Mac OS X) de ceux que vous avez utilisés auparavant, reportez-vous à la section [Protection des nouveaux systèmes d'exploitation](#) à la page 11.

Pour protéger de nouveaux ordinateurs :

1. Dans le Sophos Control Center, sur le menu **Actions**, cliquez sur **Protéger les nouveaux ordinateurs**.

L'**Assistant Sophos de protection du réseau** démarre.

2. Sur la page **Détails du compte utilisateur Windows**, saisissez les détails du compte d'administrateur pouvant être utilisé pour installer les logiciels sur les ordinateurs de votre réseau.
3. Sur la page **Protection des ordinateurs**, patientez pendant la recherche des ordinateurs.
Dans la colonne **Protéger**, sélectionnez les ordinateurs que vous voulez protéger et cliquez sur **Suivant**.
4. Sur la page **Sélection des fonctions**, sélectionnez les fonctions que vous voulez installer sur les ordinateurs.

- Par défaut, le logiciel antivirus est sélectionné pour une installation sur tous les ordinateurs.

- Si vous voulez installer le pare-feu, sélectionnez la case à cocher **Pare-feu**.

Sophos Client Firewall peut uniquement être installé sur des postes de travail exécutant Windows 2000 ou supérieur, il ne peut pas être installé sur des ordinateurs utilisant des systèmes d'exploitation serveur. Le pare-feu nécessite Sophos Anti-Virus.

Remarque : redémarrez chaque ordinateur si vous choisissez d'installer et d'activer Sophos Client Firewall.

- Si vous voulez supprimer tout logiciel de sécurité tiers, sélectionnez la case à cocher **Suppression du logiciel concurrent**.

5. S'il s'agit d'ordinateurs répertoriés sur la page **Ordinateurs que vous devez protéger manuellement**, cliquez sur **Imprimer** pour imprimer une liste des ordinateurs non protégés.

Autrement, cliquez sur **Enregistrer sous** pour enregistrer une copie de la liste ou notez par écrit ces ordinateurs.

6. Sur la dernière page de l'assistant, cliquez sur **Terminer**.

Dès que vous fermez l'assistant, le Sophos Control Center installe le logiciel automatiquement sur tous les ordinateurs sélectionnés. Ces ordinateurs ainsi que des informations concernant leur état sont répertoriés dans le Sophos Control Center.

7. Allez sur chaque ordinateur de la liste des ordinateurs non protégés et installez les logiciels manuellement.

Pour plus d'informations sur l'installation manuelle des ordinateurs, reportez-vous au guide de démarrage du Sophos Control Center.

4.2 Protection des nouveaux systèmes d'exploitation

Si vous ajoutez un nouveau type d'ordinateur sur votre réseau, par exemple, si vous ajoutez des ordinateurs Windows 98 ou Mac OS X pour la première fois, vous devez activer le Sophos Control Center pour qu'il télécharge le logiciel antivirus correspondant à ce type d'ordinateur.

Sophos Endpoint Security and Control peut uniquement être installé sur des ordinateurs fonctionnant sous Windows 2000 ou supérieur.

Pour protéger de nouveaux systèmes d'exploitation :

1. Dans le volet gauche, sous **Configuration**, cliquez sur **Configurer la mise à jour**.
2. Dans la boîte de dialogue **Configuration de la mise à jour**, sur l'onglet **Logiciels**, sélectionnez le système ou les systèmes d'exploitation que vous voulez protéger.
3. Retournez à la fenêtre principale du Sophos Control Center. Dans le menu **Actions**, cliquez sur **Mettre à jour maintenant**.
4. Allez sur chaque ordinateur du nouveau type et installez les logiciels. Pour plus d'informations sur l'installation manuelle, reportez-vous au *Sophos Control Center Guide de démarrage*.

5 Mise à jour des ordinateurs

5.1 Fonctionnement de la mise à jour

Le Sophos Control Center vérifie les mises à jour depuis Sophos toutes les 60 minutes et, si de nouvelles mises à jour sont disponibles, les télécharge.

Ces logiciels sont alors disponibles sur l'ordinateur sur lequel vous exécutez le Sophos Control Center. Les ordinateurs qui sont administrés par le Sophos Control Center se mettent à jour automatiquement depuis cette copie centralisée (par défaut, ils vérifient les mises à jour toutes les 5 minutes).

L'heure de la dernière mise à jour depuis Sophos apparaît sur le tableau de bord du Sophos Control Center.

5.2 La mise à jour a-t-elle réussi ?

La mise à jour des logiciels de sécurité comporte deux étapes :

1. Le Sophos Control Center télécharge les mises à jour depuis Sophos.
2. Les ordinateurs en réseau se mettent à jour depuis votre serveur.

Si l'une des deux étapes échoue, vous êtes averti ainsi :

■ Le Sophos Control Center ne parvient pas à télécharger les mises à jour

Si le téléchargement échoue, un message apparaît sur le tableau de bord du Sophos Control Center. Vous pouvez choisir de recevoir une alerte en cas d'échec de téléchargement. Pour plus d'informations, reportez-vous à la section [Configuration des alertes par courriel sur l'état du réseau](#) à la page 49.

■ Les ordinateurs ne parviennent pas à se mettre à jour

Dans la liste des ordinateurs, le mot "Non" apparaît dans la colonne **A jour** près de tout ordinateur non à jour. Pour forcer une mise à jour de l'ordinateur, sélectionnez et cliquez avec le bouton droit de la souris sur l'ordinateur que vous voulez mettre à jour. Dans le menu, cliquez sur **Mettre à jour les ordinateurs maintenant**.

5.3 Alertes concernant la dernière mise à jour

Vous pouvez configurer le Sophos Control Center pour qu'il vous alerte en cas de problèmes de téléchargement de mises à jour depuis Sophos.

Pour recevoir des alertes concernant la dernière mise à jour :

1. Dans le menu **Outils**, cliquez sur **Configurer les alertes par courriel**.
2. Dans la boîte de dialogue **Configuration des alertes par courriel**, cliquez sur **Configurer** et saisissez les détails de votre serveur SMTP.
3. Cliquez sur **Ajouter**, saisissez l'adresse électronique et la langue dans laquelle les alertes seront envoyées.

4. Dans la section **Abonnements** sous **Niveau dépassé**, assurez-vous que l'option **Temps écoulé depuis la dernière mise à jour depuis Sophos** est sélectionnée, puis cliquez sur **OK**.

5.4 Mise à jour manuelle du réseau

Vous pouvez choisir de mettre à jour manuellement vos logiciels de sécurité.

Pour mettre à jour manuellement vos logiciels de sécurité :

1. Dans le menu **Actions**, cliquez sur **Mettre à jour maintenant**.
2. Le Sophos Control Center affiche un message vous demandant de confirmer que vous voulez réaliser une mise à jour. Cliquez sur **Oui**.

Le Sophos Control Center contacte Sophos et télécharge la dernière version des logiciels antivirus et (si vous avez sélectionné cette option) de pare-feu. Tous les ordinateurs de votre réseau se mettent alors à jour automatiquement à la vérification suivante des mises à jour sur votre serveur.

5.5 Mise à jour d'un ordinateur individuel

Si un ordinateur individuel apparaît comme non à jour ("Non" apparaît dans la colonne **A jour**), vous pouvez l'inviter à se mettre à jour.

- ❖ Dans la liste des ordinateurs, sélectionnez et cliquez avec le bouton droit de la souris sur celui que vous voulez mettre à jour. Dans le menu, cliquez sur **Mettre à jour les ordinateurs maintenant**.

6 Résolution des alertes et des menaces

6.1 Que se passe-t-il lors de la découverte d'une menace ?

Si une menace a été trouvée sur votre réseau et qu'elle n'a pas été nettoyée automatiquement :

- Le Sophos Control Center vous envoie une alerte, si les alertes de contrôle sont activées. Pour plus d'informations, reportez-vous à la section [Configuration des alertes antivirus et HIPS](#) à la page 48.
- Dans le Sophos Control Center, dans la liste des ordinateurs, une icône d'alerte apparaît près du nom de l'ordinateur infecté. Pour savoir ce qui a provoqué l'alerte, sélectionnez l'ordinateur dans la liste des ordinateurs, cliquez avec le bouton droit de la souris et sélectionnez **Voir les détails de l'ordinateur**. Pour plus d'informations sur les icônes d'alertes, reportez-vous à la section [Que signifient les icônes ?](#) à la page 5
- Le nombre total de virus et de spywares trouvés sur votre réseau apparaît dans le Sophos Control Center, dans le volet **Tableau de bord**.

6.2 Nettoyage de votre ordinateur

Pour traiter les menaces, virus et spywares et les applications potentiellement indésirables (ou PUA) sur vos ordinateurs, procédez ainsi :

1. Dans le menu **Actions**, cliquez sur **Résoudre les alertes et les erreurs**.
Sinon, vous pouvez cliquer sur les liens de type d'alerte sur le Tableau de bord.
La boîte de dialogue **Résolution des alertes et des erreurs** apparaît.
2. Dans l'onglet **Alertes**, dans la liste déroulante **Afficher**, sélectionnez l'une des options.
D'après la sélection, les informations sur chaque ordinateur infecté apparaissent dans les colonnes telles que le nom de l'ordinateur infecté, la date et l'heure de la découverte de la première menace sur l'ordinateur, le type d'alerte, l'état de l'alerte et ainsi de suite.

3. D'après la sélection, la colonne **Etat** affiche l'un des états suivants :

■ **Nettoyable**

Dans ce cas, nettoyez les éléments infectés en utilisant le bouton **Nettoyer** comme cela est décrit plus loin dans cette section.

■ **Non nettoyable**

Pour nettoyer les éléments qui apparaissent comme "non nettoyables" dans le Sophos Control Center, allez sur l'ordinateur infecté et effectuez le nettoyage manuellement. Si la menace n'a pas été supprimée, reportez-vous à la section [Echec du nettoyage](#) à la page 57.

■ **Nettoyage en cours (démarré à <heure>)**

Indique que le processus de nettoyage a démarré.

■ **Délai d'attente dépassé pour le nettoyage (démarré à <heure>)**

Indique que le délai d'attente de l'opération de nettoyage a été dépassé et que la menace n'a pas été nettoyée. Peut être causée lorsque l'ordinateur n'est pas connecté au réseau. Assurez-vous que l'ordinateur est connecté au réseau et réessayez de nettoyer l'ordinateur.

■ **Redémarrage requis**

Indique que l'alerte a été partiellement nettoyée mais qu'un redémarrage est nécessaire pour finir l'opération de nettoyage.

■ **Contrôle intégral requis**

Indique que l'alerte peut être nettoyée mais qu'un contrôle intégral est requis pour finir l'opération de nettoyage.

■ **Echec du nettoyage**

Indique que le nettoyage de l'alerte a échoué. Un nettoyage manuel peut être nécessaire.

■ **Type de menace non nettoyable**

Indique que l'élément ne peut pas être nettoyé car le type d'alerte n'est pas nettoyable.

4. Utilisez les options décrites ci-dessous pour exécuter l'action correspondante :

■ **Tout sélectionner/Tout effacer**

Cliquez sur l'un de ces boutons pour sélectionner ou effacer toutes les entrées. Ceci vous permet d'effectuer la même action sur un groupe d'entrées. Pour sélectionner ou effacer une entrée spécifique, cliquez sur la case à cocher située à gauche de l'entrée en question.

■ **Approuver**

Si vous estimez que l'opération est sûre, cliquez sur cette option pour supprimer les entrées sélectionnées de la liste. Ceci ne supprime pas les éléments du disque.

■ **Nettoyer**

Cliquez sur ce bouton pour nettoyer les ordinateurs sélectionnés des menaces, virus, spywares ou PUA.

Remarque : remplacez ensuite les programmes nettoyés à l'aide des disques originaux ou d'une sauvegarde saine.

Avant de tenter de nettoyer des menaces à plusieurs composants des ordinateurs, Sophos vous conseille d'exécuter un contrôle complet des ordinateurs pour déterminer tous les composants des menaces à plusieurs composants. Pour plus d'informations sur le contrôle des ordinateurs à des heures définies, reportez-vous à la section [Contrôle des ordinateurs à des heures définies](#) à la page 32.

Pour un nettoyage complet de l'ordinateur de certaines menaces dotées de plusieurs composants, il se peut que vous ayez à redémarrer l'ordinateur. Si c'est le cas, un message apparaît sur l'ordinateur affecté, donnant la possibilité de redémarrer l'ordinateur immédiatement ou ultérieurement. Les étapes de nettoyage finales seront exécutées après le redémarrage de l'ordinateur.

Remarque : lors du nettoyage d'une menace sur un ordinateur, l'action est considérée comme un échec si aucune réponse n'est renvoyée par l'ordinateur au bout d'une heure (à partir de l'heure où une instruction pour exécuter l'action a été envoyée depuis le Sophos Control Center vers l'ordinateur).

6.3 Recherche d'informations sur les menaces

Si une menace est signalée, vous pouvez trouver des informations sur ses effets et des conseils sur le nettoyage.

Pour avoir des informations sur les menaces :

1. Dans le Sophos Control Center, dans la liste des ordinateurs, sélectionnez l'ordinateur sur lequel la menace a été trouvée, cliquez avec le bouton droit de la souris et sélectionnez **Voir les détails de l'ordinateur**.
2. Dans la fenêtre **Détails de l'ordinateur**, défilez vers le bas vers **Alertes et erreurs à traiter** et cliquez sur le nom de la menace.

Le Sophos Control Center vous connecte à l'analyse de la menace sur le site Web de Sophos.

Sinon, vous pouvez aussi aller sur le site Web de Sophos et naviguer vers l'analyse de la menace dont vous voulez en savoir plus. Pour ce faire, dans le menu **Aide**, cliquez sur **Voir les informations sur l'élément**.

6.4 Traitement des alertes d'erreur

Des informations sur les erreurs de contrôle et de pare-feu à traiter des 30 derniers jours apparaissent dans l'onglet Erreurs. Vous pouvez voir, en particulier, le nom de l'ordinateur sur lequel l'erreur a été rencontrée, la date et l'heure auxquelles l'erreur s'est produite ainsi que son type, son code et sa description.

Pour traiter les erreurs antivirus et de pare-feu :

1. Dans le menu **Actions**, cliquez sur **Résoudre les alertes et les erreurs**.
2. Dans la boîte de dialogue **Résolution des alertes et des erreurs**, cliquez sur l'onglet **Erreurs**.
3. Utilisez les options décrites ci-dessous pour exécuter l'action correspondante :

- **Tout sélectionner/Tout effacer**

Cliquez sur l'un de ces boutons pour sélectionner ou effacer toutes les entrées. Ceci vous permet d'effectuer la même action sur un groupe d'entrées. Pour sélectionner ou effacer une entrée spécifique, cliquez sur la case à cocher située à gauche de l'entrée en question.

- **Approuver**

Cliquez sur cette option pour marquer les erreurs comme traitées. Les alertes approuvées ne sont plus affichées.

7 Re-protection des ordinateurs

7.1 Re-protection des ordinateurs

Vous pouvez réinstaller les logiciels antivirus et de pare-feu (si votre licence l'inclut) qui étaient à l'origine installés sur tous les ordinateurs de votre réseau.

Pour protéger de nouveau les ordinateurs :

1. Dans la liste des ordinateurs, mettez en surbrillance ceux sur lesquels vous voulez réinstaller les logiciels.
2. Ouvrez le menu **Outils** et sélectionnez **Re-protéger les ordinateurs**.

L'**Assistant de re-protection des ordinateurs** démarre. Celui-ci vous guide tout au long du processus de réinstallation des logiciels.

Pour plus d'informations sur la protection manuelle des ordinateurs, reportez-vous au Guide de démarrage du Sophos Control Center.

8 Surveillance des ordinateurs protégés

8.1 Identification des ordinateurs qui sont conformes à la configuration centralisée

Sophos Control Center vous permet de créer une série de paramètres (par exemple, pour la mise à jour) de manière centralisée et de l'appliquer aux ordinateurs d'extrémité. Cette série de paramètres est appelée configuration centralisée.

Vous pouvez vérifier si tous les ordinateurs sont conformes à la configuration antivirus, de mise à jour, de pare-feu, de contrôle des applications et des périphériques définie de manière centralisée via le Sophos Control Center.

Observez la liste des ordinateurs. Dans la colonne **Configuration centralisée**, le mot "Ok" indique que l'ordinateur est conforme à la configuration centralisée.

- Si un ordinateur n'est pas conforme à la configuration centralisée (par exemple, si la configuration de l'ordinateur a été changée depuis l'ordinateur lui-même et s'il n'est marqué comme configuré localement dans le Sophos Control Center), un signal d'avertissement jaune et le mot "Changé" apparaissent dans la colonne **Configuration centralisée**.
- Si aucun logiciel de sécurité n'est installé sur un ordinateur, la colonne **Configuration centralisée** n'affiche aucun état (elle est vide) pour cet ordinateur. Si les logiciels sont configurés localement, "Configuré localement" apparaît. Si un ordinateur attend la configuration centralisée du Sophos Control Center, vous voyez apparaître "En attente" dans cette colonne.

Pour restaurer la configuration centralisée sur un ordinateur, sélectionnez l'ordinateur, cliquez dessus avec le bouton droit de la souris et sélectionnez **Restaurer la configuration centralisée**.

8.2 Identification des ordinateurs configurés localement

Vous pouvez identifier les ordinateurs sur lesquels les logiciels antivirus et de pare-feu sont configurés localement de deux manières :

- **Afficher seulement les ordinateurs configurés localement**

Vous pouvez afficher seulement les ordinateurs configurés localement.

Dans la liste déroulante **Vue**, sélectionnez **Ordinateurs configurés localement**.

- **Vérifier les ordinateurs individuels**

Pour voir si un ordinateur individuel est configuré localement, cliquez avec le bouton droit de la souris sur le nom de l'ordinateur, si **Utiliser la configuration centralisée** n'est pas sélectionné, l'ordinateur est configuré localement.

8.3 Vérification de la protection des ordinateurs

Dans le Sophos Control Center, une liste des ordinateurs apparaît avec leurs états.

- Dans la colonne **A jour**, le mot "Oui" indique que la protection Sophos est à jour sur cet ordinateur. Une icône en forme d'horloge et le mot "Non" indiquent qu'elle ne l'est pas.

Pour réorganiser les ordinateurs en fonction de leur état de mise à jour, cliquez sur l'en-tête de la colonne **A jour**.

- Dans la colonne **Antivirus**, le mot "Actif" indique que le contrôle sur accès protège l'ordinateur. Un bouclier grisé et le mot "Inactif" indique qu'il ne le protège pas.

Remarque : tant que les ordinateurs de vos utilisateurs sont protégés par le contrôle sur accès, il n'est pas normalement pas nécessaire d'exécuter un contrôle sur accès sur un serveur de fichiers Windows 2000 ou Windows 2003.

Si le logiciel n'est pas installé sur l'ordinateur, vous voyez apparaître "Non installé" dans cette colonne.

- Dans la colonne **Contrôle des applications**, le mot "Actif" apparaît lorsque le contrôle des applications est activé sur l'ordinateur. Un bouclier grisé et le mot "Inactif" indique qu'il ne le protège pas.
- Dans la colonne **Pare-feu**, le mot "Actif" indique que le pare-feu protège l'ordinateur. Une icône de pare-feu grisée et le mot "Inactif" indique qu'il ne le protège pas. Si le logiciel n'est pas installé sur l'ordinateur, la colonne n'affiche aucun état (elle est vide) pour cet ordinateur.

8.4 Recherche des ordinateurs supprimés

Vous pouvez récupérer un ordinateur qui a été supprimé de la liste des ordinateurs dans le Sophos Control Center.

Pour récupérer un ordinateur qui a été supprimé, vous devez rechercher l'ordinateur supprimé comme un nouvel ordinateur. Pour plus d'informations sur la recherche des ordinateurs, reportez-vous à la section [Protection des nouveaux ordinateurs](#) à la page 10.

8.5 Affichage des ordinateurs en fonction de leur états

Vous pouvez afficher la liste des ordinateurs en fonction de leurs états.

Pour visualiser un ordinateur d'après son état :

- ❖ Dans le Sophos Control Center, dans la liste déroulante **Vue**, sélectionnez un état. Le tableau suivant affiche la liste des états :

| Option | Description |
|----------------------|---|
| Tous les ordinateurs | Affiche une liste des ordinateurs actuellement connectés au réseau et administrés par le Sophos Control Center. |

| Option | Description |
|--|---|
| Ordinateurs avec alertes et erreurs | Affiche une liste des ordinateurs qui ont des alertes. Pour savoir ce qui a provoqué l'alerte, sélectionnez l'ordinateur dans la liste des ordinateurs, cliquez avec le bouton droit de la souris et sélectionnez Voir les détails de l'ordinateur . |
| Ordinateurs non administrés | Affiche une liste des ordinateurs qui ne sont pas administrés par le Sophos Control Center. |
| Ordinateurs non à jour administrés | Affiche une liste des ordinateurs qui sont administrés avec des logiciels qui ne sont pas à jour. Pour mettre à jour un ordinateur individuel, cliquez avec le bouton droit sur son entrée dans la liste des ordinateurs et sélectionnez Mettre les ordinateurs à jour maintenant . |
| Ordinateurs administrés | Affiche une liste des ordinateurs actuellement administrés par le Sophos Control Center. |
| Ordinateurs configurés localement | Affiche une liste des ordinateurs qui sont configurés localement. Pour faire en sorte que l'ordinateur utilise de nouveau la configuration centralisée, cliquez avec le bouton droit de la souris sur son nom et sélectionnez Utiliser la configuration centralisée . |
| Ordinateurs connectés | Affiche une liste des ordinateurs qui sont administrés et actuellement disponibles. |
| Ordinateurs non connectés | Affiche une liste des ordinateurs qui sont administrés mais actuellement indisponibles, par exemple, l'ordinateur est hors tension. |

S'il y a plusieurs alertes sur un ordinateur, l'icône de l'alerte ayant la priorité la plus haute apparaît. Pour plus d'informations sur la priorité des icônes, reportez-vous à la section [Priorité des alertes](#) à la page 7.

8.6 Impression du récapitulatif des menaces et de la liste des ordinateurs

Vous pouvez imprimer le récapitulatif des menaces sur vos ordinateurs et la liste des ordinateurs pour une vue sélectionnée.

Pour imprimer le récapitulatif des menaces et la liste des ordinateurs :

1. Dans la fenêtre Sophos Control Center, dans le menu **Fichier**, cliquez sur **Imprimer**.

La boîte de dialogue **Impression** apparaît.

2. Paramétrez les options d'impression et cliquez sur **OK**. Le document résultant inclut les informations suivantes :
 - Nom de l'entreprise
 - Date et heure de l'impression
 - Données affichées dans la liste des ordinateurs pour la vue sélectionnée

9 Consultation des événements

9.1 A propos des événements

Lorsqu'un événement de contrôle d'applications, de pare-feu ou de contrôle des périphériques se produit sur un système d'extrémité, par exemple, une application a été bloquée par le pare-feu, cet événement est envoyé au Sophos Control Center et peut être vue dans l'observateur d'événements correspondant.

A l'aide des observateurs d'événements, vous pouvez vous pencher sur les événements qui ont eu lieu sur le réseau. Vous pouvez aussi générer une liste des événements basés sur un filtre que vous configurez, par exemple, une liste de tous les événements de contrôle des applications ces dernières 24 heures générés par un utilisateur donné.

Le nombre d'ordinateurs avec des événements au-dessus d'un seuil spécifié dans les dernières 24 heures apparaît sur le Tableau de bord. Pour plus d'informations sur la manière de configurer le seuil, reportez-vous à la section [Configuration du tableau de bord](#) à la page 9.

Vous pouvez aussi configurer l'envoi des alertes par courriel aux destinataires de votre choix lorsqu'un événement s'est produit. Pour plus d'informations, reportez-vous à la section [Configuration des alertes antivirus et HIPS](#) à la page 48.

9.2 Consultation des événements du contrôle des applications

Pour consulter les événements du contrôle des applications :

1. Dans le menu **Affichage**, cliquez sur **Événements du contrôle des applications**.
Sinon, cliquez sur le lien **Contrôle des applications** du tableau de bord.
La boîte de dialogue **Contrôle des applications - Observateurs d'événements** apparaît.
2. Dans le champ **Période de recherche**, cliquez sur la flèche du menu déroulant et sélectionnez la période pour laquelle vous souhaitez afficher les événements.
Vous pouvez sélectionner soit une période fixe, par exemple, **Depuis 24 heures** soit **Personnalisée** et spécifiez votre propre période en sélectionnez les dates de début et de fin.
3. Cliquez sur **Rechercher** pour afficher une liste d'événements.

Vous pouvez exporter dans un fichier la liste des événements du contrôle des applications. Pour plus d'informations, reportez-vous à la section [Exportation dans un fichier de la liste des événements](#) à la page 25.

Vous pouvez aussi copier des événements dans le Presse-papiers. Pour plus d'informations, reportez-vous à la section [Copie des événements dans le Presse-papiers](#) à la page 25.

9.3 Consultation des événements du contrôle des périphériques

Pour consulter les événements du contrôle des périphériques :

1. Dans le menu **Affichage**, cliquez sur **Événements du contrôle des périphériques**.
Sinon, cliquez sur le lien **Contrôle des périphériques** du tableau de bord.
La boîte de dialogue **Contrôle des périphériques - Observateur d'événements** apparaît.
2. Dans le champ **Période de recherche**, cliquez sur la flèche du menu déroulant et sélectionnez la période pour laquelle vous souhaitez afficher les événements.
Vous pouvez sélectionner soit une période fixe, par exemple, **Depuis 24 heures** soit **Personnalisée** et spécifiez votre propre période en sélectionnant les dates de début et de fin.
3. Si vous voulez consulter les événements d'un type de périphérique donné, dans le champ **Type de périphérique**, cliquez sur la flèche du menu déroulant et sélectionnez le type de périphérique.
Par défaut, l'observateur d'événements affiche les événements de toutes les types de périphériques.
4. Si vous voulez consulter des événements pour un utilisateur ou un ordinateur donné, saisissez son nom dans le champ prévu.
Si vous laissez les champs vides, les événements de tous les utilisateurs et ordinateurs apparaîtront.
5. Cliquez sur **Rechercher** pour afficher une liste d'événements.

Dans la boîte de dialogue **Contrôle des périphériques - Observateur d'événements**, vous pouvez exempter un périphérique des stratégies de contrôle des périphériques. Pour plus d'informations, reportez-vous à la section [Exemption d'un périphérique](#) à la page 47.

Vous pouvez exporter dans un fichier la liste des événements du contrôle des périphériques. Pour plus d'informations, reportez-vous à la section [Exportation dans un fichier de la liste des événements](#) à la page 25.

Vous pouvez aussi copier des événements dans le Presse-papiers. Pour plus d'informations, reportez-vous à la section [Copie des événements dans le Presse-papiers](#) à la page 25.

9.4 Consultation des événements du pare-feu

Pour consulter les événements du pare-feu :

1. Dans le menu **Affichage**, cliquez sur **Événements du pare-feu**.
Sinon, cliquez sur le lien **Pare-feu** du tableau de bord.
La boîte de dialogue **Pare-feu - Observateur d'événements** apparaît.
2. Dans le champ **Période de recherche**, cliquez sur la flèche du menu déroulant et sélectionnez la période pour laquelle vous souhaitez afficher les événements.
Vous pouvez sélectionner soit une période fixe, par exemple, **Depuis 24 heures** soit **Personnalisée** et spécifiez votre propre période en sélectionnez les dates de début et de fin.
3. Cliquez sur **Rechercher** pour afficher une liste d'événements.

Dans la boîte de dialogue **Pare-feu - Observateur d'événements**, vous pouvez personnaliser une règle de pare-feu comme décrit à la section [Configuration du pare-feu](#) à la page 38.

Vous pouvez exporter dans un fichier la liste des événements du pare-feu. Pour plus d'informations, reportez-vous à la section [Exportation dans un fichier de la liste des événements](#) à la page 25.

Vous pouvez aussi copier des événements dans le Presse-papiers. Pour plus d'informations, reportez-vous à la section [Copie des événements dans le Presse-papiers](#) à la page 25.

9.5 Exportation dans un fichier de la liste des événements

Vous pouvez exporter dans un fichier CSV (valeurs séparées par des virgules) la liste des événements du contrôle des applications, de pare-feu ou du contrôle des périphériques.

1. Dans le menu **Affichage**, cliquez sur l'une des options "événements", en fonction de la liste d'événements que vous voulez exporter.

La boîte de dialogue **Observateur d'événements** apparaît.

2. Si vous voulez afficher certains événements seulement, dans le volet **Critères de recherche**, définissez les filtres de façon appropriée et cliquez sur **Rechercher** pour afficher les événements.

Pour plus d'informations, reportez-vous aux sections [Consultation des événements du contrôle des applications](#) à la page 23, [Consultation des événements du contrôle des périphériques](#) à la page 23 ou [Consultation des événements du pare-feu](#) à la page 24.

3. Cliquez sur **Exporter**.
4. Dans la boîte de dialogue **Enregistrer sous**, saisissez un nom de fichier et naviguez pour sélectionner une destination pour le fichier.

9.6 Copie des événements dans le Presse-papiers

Vous pouvez copier les événements du contrôle des applications, de pare-feu ou du contrôle des périphériques dans le Presse-papiers, puis les coller dans un autre document au format séparé par des tabulations. Vous pouvez copier tous les événements de la liste ou seulement un événement.

1. Dans le menu **Affichage**, cliquez sur l'une des options "événements", en fonction de la liste d'événements que vous voulez exporter.

La boîte de dialogue **Observateur d'événements** apparaît.

2. Si vous voulez afficher certains événements seulement, dans le volet **Critères de recherche**, définissez les filtres de façon appropriée et cliquez sur **Rechercher** pour afficher les événements.

Pour plus d'informations, reportez-vous aux sections [Consultation des événements du contrôle des applications](#) à la page 23, [Consultation des événements du contrôle des périphériques](#) à la page 23 ou [Consultation des événements du pare-feu](#) à la page 24.

3. Dans la boîte de dialogue **Observateur d'événements**, cliquez sur **Copier** pour copier la liste des événements dans le Presse-papiers.

Si vous voulez copier un événement, sélectionnez-le et cliquez sur **Copier**.

10 Configuration d'un contrôle

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

Par défaut, Sophos Anti-Virus détecte les virus, les chevaux de Troie, les spywares et les vers automatiquement dès qu'un utilisateur tente d'accéder à des fichiers les contenant.

Pour contrôler votre ordinateur :

1. Dans le volet gauche, sous **Configuration**, cliquez sur **Configurer le contrôle**.
2. Dans la boîte de dialogue **Configuration du contrôle**, dans le volet **Configurer l'antivirus et HIPS**, assurez-vous que la case à cocher **Activer le contrôle sur accès** est sélectionnée.

10.2 Contrôle à la recherche des applications potentiellement indésirables

Par défaut, Sophos Anti-Virus détecte les virus, les chevaux de Troie, les spywares et les vers. Vous pouvez aussi le configurer pour qu'il détecte les applications potentiellement indésirables (PUA).

Remarque : cette option s'applique uniquement à Sophos Endpoint Security and Control sous Windows 2000 ou supérieur.

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

Pour rechercher les applications potentiellement indésirables :

1. Dans le volet gauche, sous **Configuration**, cliquez sur **Configurer le contrôle**.
2. Dans la boîte de dialogue **Configuration du contrôle**, dans le volet **Contrôle planifié**, cliquez sur **Ajouter** pour créer un nouveau contrôle ou sélectionnez un contrôle dans la liste et cliquez sur **Modifier** pour le modifier.
3. Dans la boîte de dialogue **Paramètres du contrôle planifié**, cliquez sur **Configurer** (en bas de la page).
4. Dans la boîte de dialogue **Paramètres de contrôle et de nettoyage**, cliquez sur l'onglet **Contrôle**. Dans le volet **Autres options de contrôle**, assurez-vous que l'option **Rechercher les adwares et les PUA** est sélectionnée. Cliquez sur **OK**.
5. Pendant le contrôle, Sophos Anti-Virus peut signaler certaines "applications potentiellement indésirables".

Si vous souhaitez que vos ordinateurs exécutent ces applications, vous devez les autoriser. Pour plus d'instructions sur l'autorisation des applications, reportez-vous à la section [Autorisation des applications à l'utilisation](#) à la page 31.

6. Si vous voulez activer la détection sur accès, dans la boîte de dialogue **Configuration du contrôle**, cliquez sur **Contrôle sur accès**.

Dans la boîte de dialogue **Paramètres du contrôle sur accès** qui apparaît, sous **Autres options de contrôle**, sélectionnez **Rechercher les adwares et les PUA**.

Certaines applications "surveillent" les fichiers et tentent d'y accéder régulièrement. Si votre contrôle sur accès est activé, il détecte chaque accès et envoie de nombreuses alertes. Reportez-vous à la section [Alertes régulières concernant les applications potentiellement indésirables](#) à la page 57.

10.3 Paramétrage des options de contrôle sur accès

Pour paramétrer les options de contrôle sur accès :

1. Dans le volet gauche, sous **Configuration**, cliquez sur **Configurer le contrôle**.
2. Dans la boîte de dialogue **Configuration du contrôle**, cliquez sur **Contrôle sur accès**.
3. Dans la boîte de dialogue **Paramètres de contrôle sur accès**, sélectionnez les options de votre choix.

■ Contrôle dans les fichiers archive

Vous pouvez contrôler à l'intérieur des fichiers archive. Par contre, avant d'activer cette option, considérez les faits suivants :

- Le contrôle sur accès vérifie automatiquement les fichiers présents dans une archive lorsque vous accédez à ces fichiers. Le contrôle à l'intérieur des archives est par conséquent facultatif.
- Le contrôle à l'intérieur des archives a des conséquences sur les performances des ordinateurs et n'est pas conseillé pour une utilisation avec le contrôle sur accès.

■ Rechercher les virus Macintosh

Sélectionnez cette option pour contrôler les fichiers Macintosh archivés sur les ordinateurs Windows au cours du contrôle sur accès.

■ Rechercher les adwares et des PUA

Par défaut, Sophos Endpoint Security and Control détecte les virus, les chevaux de Troie et les vers. Vous pouvez aussi le configurer pour qu'il détecte les applications potentiellement indésirables (PUA).

■ Rechercher les fichiers suspects (HIPS).

Sélectionnez cette option pour rechercher les fichiers suspects au cours du contrôle sur accès.

4. Sous **Comportement du contrôle sur accès**, sélectionnez les fichiers à contrôler lorsque l'utilisateur exécute des opérations.
 - **En lecture**, le logiciel Sophos Anti-Virus contrôle automatiquement les fichiers "sur accès". Par défaut, ceci signifie lorsque l'utilisateur ouvre le fichier ("en lecture").
 - **En écriture**, si vous voulez que les fichiers soient vérifiés au moment de leur fermeture.
 - **En renommant**, si vous voulez que les fichiers soient vérifiés au moment où ils sont renommés.

Ces options donnent une protection supérieure contre les virus qui s'écrivent sur le disque dur de l'ordinateur et/ou renomment les fichiers. Par contre, l'accroissement de l'activité peut affecter les performances de l'ordinateur.

5. Sous **Supports amovibles**, sélectionnez **Autoriser l'accès aux lecteurs avec secteurs de démarrage infectés** pour autoriser l'accès. Par exemple, pour copier des fichiers depuis une disquette infectée par un virus de secteur de démarrage.

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

10.4 Modification des types de fichiers contrôlés

Les types de fichiers contrôlés par défaut diffèrent d'un système d'exploitation à l'autre et changent au fur et à mesure de la mise à jour du produit.

■ Sur Mac

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

■ Sur Windows

Par défaut, Sophos Anti-Virus contrôle les types de fichiers qui sont vulnérables aux virus. Vous pouvez contrôler des types de fichiers supplémentaires ou choisir d'exempter du contrôle certains types de fichiers. Pour consulter une liste des types de fichiers, rendez-vous sur un ordinateur possédant le système d'exploitation approprié, ouvrez la fenêtre Sophos Anti-Virus et recherchez la page de configuration "Extensions".

Remarque : sous les ordinateurs Windows 98, les modifications apportées dans les paramètres de contrôle planifié s'appliquent aussi au contrôle sur accès.

Pour modifier les types de fichiers contrôlés :

1. Dans le volet gauche, sous **Configuration**, cliquez sur **Configurer le contrôle**. La boîte de dialogue **Configuration du contrôle** apparaît.
 - Pour configurer le contrôle sur accès, sous **Configurer l'antivirus et HIPS**, cliquez sur **Contrôle sur accès**.
 - Pour configurer les contrôles planifiés, sous **Contrôle planifié**, cliquez sur **Extensions et Exclusions**.
2. Sur l'onglet **Extensions** :
 - Pour contrôler des types de fichiers supplémentaires, cliquez sur **Ajouter** puis saisissez l'extension du fichier, par exemple PDF, dans le champ **Extension**.
 - **Contrôler les fichiers sans extension**. Par défaut, les fichiers sans extension sont contrôlés.
 - Pour exempter certains types de fichiers qui sont d'habitude contrôlés par défaut, cliquez sur **Exclure**. La boîte de dialogue **Exclusion d'extensions** s'ouvre. Saisissez l'extension du fichier.

10.5 Activation du contrôle web

Le contrôle web contrôle les données et les fichiers téléchargés par Internet Explorer. Par défaut, le contrôle web est désactivé.

Pour activer le contrôle web :

1. Dans le volet gauche, sous **Configuration**, cliquez sur **Configurer le contrôle**.
2. Dans la boîte de dialogue **Configurer le contrôle**, près de **Contrôle Web est :**, sélectionnez **Actif**.

Vous pouvez aussi sélectionner **Comme sur accès**, si vous voulez désactiver et activer les contrôles sur accès et web simultanément.

10.6 Exclusion des éléments du contrôle sur accès

Cette section vous indique comment exclure des éléments (par exemple, des lecteurs, des dossiers ou des fichiers) du contrôle sur accès.

Vous pouvez exempter certains types de fichiers du contrôle en ajoutant les extensions de fichiers dans la **Liste des extensions exclues**. Pour plus d'instructions, reportez-vous à la section *Modification des types de fichiers contrôlés* à la page 28.

- Les options "exclusion d'éléments" s'appliquent seulement aux ordinateurs Windows 2000 ou supérieur et Mac OS X.
- Pour exclure les éléments sur les ordinateurs Windows 98, reportez-vous à la section *Exclusion d'éléments du contrôle planifié* à la page 33.

1. Dans le volet gauche, sous **Configuration**, cliquez sur **Configurer le contrôle**.
2. Dans la boîte de dialogue **Configuration du contrôle**, cliquez sur **Contrôle sur accès**.

3. Dans la boîte de dialogue **Paramètres du contrôle sur accès**, cliquez sur l'onglet **Exclusions Windows** ou **Exclusions Mac**.
 - Cliquez sur **Ajouter** pour ajouter des éléments à la liste en saisissant le chemin complet dans la boîte de dialogue **Exclusion d'un élément**.
 - Sélectionnez **Exclure les fichiers distants**, si vous souhaitez empêcher Sophos Anti-Virus de contrôler les fichiers sur les lecteurs réseau.

10.7 Paramétrage du nettoyage automatique

10.7.1 A propos du nettoyage automatique

Vous pouvez faire en sorte que les ordinateurs procèdent à un nettoyage automatique dès la découverte d'un virus. Pour cela, modifiez les paramètres de contrôle comme indiqué.

Remarque : le contrôle sur accès ne peut pas nettoyer les applications potentiellement indésirables, en revanche, comme cela est décrit plus loin dans cette section, vous pouvez activer le nettoyage automatique des applications non autorisées lors d'un contrôle planifié.

10.7.2 Nettoyage automatique des virus

Vous pouvez nettoyer automatiquement les virus lors du contrôle sur accès et planifié.

Pour nettoyer automatiquement les virus :

1. Dans le volet gauche, sous **Configuration**, cliquez sur **Configurer le contrôle**.
2. Pour changer les paramètres du contrôle sur accès, dans la boîte de dialogue **Configuration du contrôle**, cliquez sur le bouton **Contrôle sur accès**. Dans la boîte de dialogue **Paramètres de contrôle sur accès**, cliquez sur l'onglet **Nettoyage**.
3. Pour changer les paramètres d'un contrôle planifié, dans la boîte de dialogue **Configuration du contrôle**, sous **Contrôle planifié**, sélectionnez un contrôle et cliquez sur **Modifier**.

Dans la boîte de dialogue **Paramètres du contrôle planifié**, cliquez sur **Configurer**. Dans la boîte de dialogue **Paramètres de contrôle et de nettoyage**, cliquez sur l'onglet **Nettoyage**.

4. Sélectionnez **Nettoyer automatiquement les éléments contenant un virus/spyware**.
5. Vous pouvez aussi spécifier ce que vous souhaitez faire en cas d'échec du nettoyage. Les options sont :
 - Refuser l'accès uniquement
 - Supprimer
 - Refuser l'accès et déplacer vers l'emplacement par défaut
 - Refuser l'accès et déplacer dans UNC

Remarque : si vous sélectionnez **Déplacer dans** et spécifiez un emplacement. Les ordinateurs Mac OS X continuent de déplacer les éléments infectés dans l'emplacement par défaut.

10.7.3 Nettoyage automatique des applications potentiellement indésirables

Remarque : cette option s'applique uniquement à Sophos Endpoint Security and Control sous Windows 2000 ou supérieur.

Vous pouvez nettoyer les applications potentiellement seulement lors d'un contrôle planifié.

Pour nettoyer automatiquement des applications potentiellement indésirables :

1. Dans le volet gauche, sous **Configuration**, cliquez sur **Configurer le contrôle**.
2. Dans la boîte de dialogue **Configuration du contrôle**, sous **Contrôle planifié**, sélectionnez un contrôle et cliquez sur **Modifier**.
3. Dans la boîte de dialogue **Paramètres du contrôle planifié**, cliquez sur **Configurer**.
4. Dans la boîte de dialogue **Paramètres de contrôle et de nettoyage**, cliquez sur l'onglet **Nettoyage**.
5. Sous **Adware et PUA**, sélectionnez **Nettoyer automatiquement les adwares et les PUA**.

Ceci permettra à Sophos Anti-Virus de supprimer de vos ordinateurs les applications potentiellement indésirables.

6. Vous pouvez également spécifier l'action à effectuer sur les fichiers suspects. Les options sont :

- Refuser l'accès uniquement
- Supprimer
- Refuser l'accès et déplacer vers l'emplacement par défaut
- Refuser l'accès et déplacer dans UNC

Remarque : si vous sélectionnez **Déplacer dans** et que vous définissez un emplacement, les ordinateurs Mac OS X déplaceront quand même les éléments infectés dans l'emplacement par défaut.

10.8 Autorisation des applications à l'utilisation

Si vous avez activé Sophos Anti-Virus pour qu'il détecte les applications potentiellement indésirables, il se peut qu'il empêche l'utilisation d'une application que vous désirez.

Pour autoriser les applications :

1. Dans le volet gauche, sous **Configuration**, cliquez sur **Configurer le contrôle**.
2. Dans la boîte de dialogue **Configuration du contrôle**, cliquez sur **Autorisation**.
3. Dans la boîte de dialogue **Gestionnaire d'autorisations**, dans la liste **Adwares et PUA connus**, sélectionnez l'application que vous voulez autoriser. Cliquez sur **Ajouter** pour l'ajouter à la liste des applications autorisées. Répétez la même opération pour chaque application que vous souhaitez autoriser. Cliquez sur **OK**.
4. Si vous ne voyez pas l'application que vous voulez autoriser, cliquez sur **Nouveau**. Dans la boîte de dialogue **Ajout d'un nouvel adware ou PUA**, saisissez le nom de l'application que vous voulez autoriser et cliquez sur **OK**.

10.9 Contrôle des ordinateurs à des heures définies

Vous pouvez configurer les ordinateurs pour qu'ils effectuent des contrôles à des heures définies.

Pour contrôler les ordinateurs à des heures définies :

1. Dans le volet gauche, sous **Configuration**, cliquez sur **Configurer le contrôle**.
2. Dans la boîte de dialogue **Configurer le contrôle**, dans le volet **Contrôle planifié**, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Paramètres du contrôle planifié**, saisissez un nom de tâche de contrôle.
4. Sélectionnez les éléments à contrôler :
 - Disques durs locaux
 - Lecteurs de disquettes et amovibles
 - Lecteurs de CD

Par défaut, tous les disques durs locaux sont contrôlés.

5. Sélectionnez les jours et heures auxquels vous souhaitez procéder au contrôle.

Si vous voulez changer les options de contrôle ou de nettoyage par défaut du contrôle, cliquez sur **Configurer** au bas de la boîte de dialogue **Paramètres du contrôle planifié**. Pour plus d'informations, reportez-vous aux sections [Paramétrage des options de contrôle planifié](#) à la page 32 ou [Nettoyage automatique des virus](#) à la page 30.

Pour savoir comment changer les types de fichiers contrôlés ou exclure certains éléments du contrôle planifié, reportez-vous aux sections [Modification des types de fichiers contrôlés](#) à la page 28 ou [Exclusion d'éléments du contrôle planifié](#) à la page 33.

10.10 Paramétrage des options de contrôle planifié

Vous pouvez choisir de configurer vos options de contrôle planifié.

Pour configurer les options d'un contrôle planifié :

1. Dans le volet gauche, sous **Configuration**, cliquez sur **Configurer le contrôle**.
2. Dans la boîte de dialogue **Configuration du contrôle**, sélectionnez un contrôle planifié et cliquez sur **Modifier**.
3. Dans la boîte de dialogue **Paramètres du contrôle planifié**, cliquez sur **Configurer**.

4. Dans la boîte de dialogue **Paramètres de contrôle et de nettoyage**, sous l'onglet **Contrôle**, sélectionnez les options de votre choix.

■ **Effectuez un contrôle dans les fichiers archive**

Vous pouvez contrôler à l'intérieur des fichiers archive. Par contre, avant d'activer cette option, considérez les faits suivants :

- Le contrôle sur accès vérifie automatiquement les fichiers présents dans une archive lorsque vous accédez à ces fichiers. Le contrôle à l'intérieur des archives est par conséquent facultatif.
- Le contrôle à l'intérieur des archives a des conséquences sur les performances des ordinateurs et n'est pas conseillé pour une utilisation avec le contrôle sur accès.

■ **Rechercher les virus Macintosh**

Sélectionnez cette option pour contrôler les fichiers Macintosh archivés sur les ordinateurs Windows au cours d'un contrôle planifié.

■ **Rechercher les adwares et des PUA**

Par défaut, Sophos Endpoint Security and Control détecte les virus, les chevaux de Troie et les vers. Vous pouvez aussi le configurer pour qu'il détecte les applications potentiellement indésirables (PUA). Cette option est sélectionnée par défaut pour un contrôle planifié.

■ **Rechercher les fichiers suspects (HIPS).**

Par défaut, la recherche des fichiers suspects est activée au cours d'un contrôle planifié.

■ **Activer la recherche des rootkits**

Le contrôle à la recherche des rootkits s'effectue toujours lorsque vous exécutez un contrôle intégral du système d'un ordinateur. L'option peut aussi être activée pour un contrôle planifié.

Pour plus d'informations sur les options de nettoyage, reportez-vous à la section [A propos du nettoyage automatique](#) à la page 30 et aux autres rubriques de la section Paramétrage du nettoyage automatique.

10.11 Exclusion d'éléments du contrôle planifié

Cette section vous indique comment exclure des éléments (par exemple, des lecteurs, des dossiers ou des fichiers) du contrôle sur planifié.

Vous pouvez aussi exempter certains types de fichiers du contrôle en ajoutant les extensions de fichiers dans la **Liste des extensions exclues**. Pour plus d'instructions, reportez-vous à la section [Modification des types de fichiers contrôlés](#) à la page 28.

Remarque: sous les ordinateurs Windows 98, les modifications apportées dans les paramètres de contrôle planifié s'appliquent aussi au contrôle sur accès.

Pour exclure des éléments du contrôle planifié :


1. Dans le volet gauche, sous **Configuration**, cliquez sur **Configurer le contrôle**. La boîte de dialogue **Configuration du contrôle** apparaît.
2. Dans la zone **Contrôle planifié**, cliquez sur **Extensions et Exclusions**.
3. Dans la boîte de dialogue **Extensions et exclusions du contrôle planifié**, cliquez sur l'onglet **Exclusions Windows** ou sur **Exclusions Mac** selon les fichiers du système d'exploitation qui doivent être exclus du contrôle. Pour ajouter des éléments dans la liste, cliquez sur **Ajouter** et saisissez le chemin complet dans la boîte de dialogue **Exclusion d'un élément**.

10.12 Configuration du contrôle sur des ordinateurs individuels

Vous pouvez configurer certains ordinateurs pour qu'ils utilisent des options différentes de celles définies de manière centralisée dans le Sophos Control Center.

Pour configurer le contrôle sur des ordinateurs individuels :

1. Dans la liste des ordinateurs, mettez en surbrillance l'ordinateur ou les ordinateurs. Cliquez avec le bouton droit de la souris et désélectionnez **Utiliser la configuration centralisée**.
2. Allez maintenant sur le ou les ordinateur(s) individuel(s) et configurez les options antivirus.

Pour configurer le contrôle sur un ordinateur individuel, cliquez avec le bouton droit de la souris sur l'icône de la barre des tâches de Sophos Endpoint Security and Control .

3. Cliquez sur **Ouvrir Sophos Endpoint Security and Control**. Dans la fenêtre de **Sophos Endpoint Security and Control**, cliquez sur **Configurer l'antivirus et HIPS**. Sous **Configurer**, cliquez sur **Contrôle sur accès** et modifiez les paramètres.

Pour plus d'informations sur la configuration du contrôle sur des ordinateurs individuels, reportez-vous à l'Aide de Sophos Endpoint Security and Control.

11 Configuration des mises à jour

11.1 Changement de ce qui est mis à jour

Vous pouvez changer les logiciels qui sont mis à jour. Vous devez exécuter cette opération si :

- Vous ajoutez des ordinateurs dotés d'un système d'exploitation différent, comme Mac OS X, sur votre réseau et si vous avez besoin de Sophos Anti-Virus pour ce système.
- Vous retirez de votre réseau tous les ordinateurs dotés d'un système d'exploitation donné.

Pour changer les logiciels téléchargés :

1. Dans le volet gauche, sous **Configuration**, cliquez sur **Configurer la mise à jour**.
2. Dans la boîte de dialogue **Configuration de la mise à jour**, cliquez sur l'onglet **Logiciels**. Puis sélectionnez le ou les système(s) d'exploitation pour lesquels vous avez besoin de Sophos Anti-Virus et cliquez sur **OK**.

Si vous avez sélectionné des systèmes d'exploitation que vous n'aviez encore jamais protégés (Windows 98 ou Mac OS X), passez aux étapes 3 et 4.

3. Retournez à la fenêtre principale du Sophos Control Center. Dans le menu **Actions**, cliquez sur **Mettre à jour maintenant** pour télécharger les nouveaux logiciels.
4. Allez sur chaque ordinateur du nouveau type et installez Sophos Anti-Virus. Pour plus d'informations sur l'installation manuelle, reportez-vous au Guide de démarrage du Sophos Control Center.

11.2 Mise à jour via un serveur proxy

Si vous utilisez un serveur proxy pour accéder à Internet, vous devez permettre au Sophos Control Center de télécharger des mises à jour via ce proxy.

Pour effectuer la mise à jour via un serveur proxy :

1. Dans le volet gauche, sous **Configuration**, cliquez sur **Configurer la mise à jour**.
2. Dans la boîte de dialogue **Configuration de la mise à jour**, cliquez sur l'onglet **Proxy**. Saisissez l'adresse et le numéro du port du proxy. Saisissez le nom utilisateur et le mot de passe d'un compte qui a un accès au proxy (votre administrateur réseau peut vous fournir ces détails).

11.3 Changement de l'identification de l'utilisateur pour la mise à jour

Vous pouvez changer l'identification de l'utilisateur utilisé pour télécharger les mises à jour.

Pour changer l'identification de l'utilisateur pour la mise à jour :

1. Dans le volet gauche, sous **Configuration**, cliquez sur **Configurer la mise à jour**.

2. Dans la boîte de dialogue **Configuration de la mise à jour**, cliquez sur l'onglet **Identification de l'utilisateur**. Saisissez le nom utilisateur et le mot de passe qui vous ont été fournis par Sophos.

11.4 Désactivation de la mise à jour automatique

Si vous avez besoin de désactiver la mise à jour automatique (par exemple, si vous avez une connexion par modem), procédez ainsi :

Remarque : si vous désactivez la mise à jour automatique, assurez-vous de vérifier régulièrement les mises à jour. Pour plus d'informations sur la vérification manuelle des mises à jour, reportez-vous à la section *Mise à jour manuelle du réseau* à la page 13.

Pour désactiver la mise à jour automatique :

1. Dans le volet gauche, sous **Configuration**, cliquez sur **Configurer la mise à jour**.
2. Dans la boîte de dialogue **Configuration de la mise à jour**, cliquez sur l'onglet **Planification**. Dessélectionnez la case à cocher **Permettre l'utilisation automatique des mises à jour aux ordinateurs**.

11.5 Changement de la fréquence de mise à jour des ordinateurs

Par défaut, les ordinateurs de votre réseau vérifient toutes les 10 minutes si des logiciels de sécurité mis à jour sont disponibles.

Pour changer la fréquence de mise à jour :

1. Dans le volet gauche, sous **Configuration**, cliquez sur **Configurer la mise à jour**.
2. Dans la boîte de dialogue **Configuration de la mise à jour**, cliquez sur l'onglet **Planification**. Assurez-vous que la case à cocher **Permettre l'utilisation automatique des mises à jour aux ordinateurs** est sélectionnée. Dans le champ au-dessous de la case à cocher, saisissez un intervalle de temps en minutes.

11.6 Mise à jour des ordinateurs qui ne sont pas toujours en réseau

Par défaut, les ordinateurs en réseau se mettent à jour depuis un dossier de mises à jour sur l'ordinateur depuis lequel vous exécutez le Sophos Control Center. Si ce dossier devient indisponible pour un ordinateur, par exemple, lorsque ce dernier n'est pas connecté au réseau de l'entreprise mais à Internet, l'ordinateur se met à jour directement depuis Sophos.

Pour mettre à jour les ordinateurs qui ne sont pas toujours en réseau :

1. Dans le volet gauche, sous **Configuration**, cliquez sur **Configurer la mise à jour**.

2. Dans la boîte de dialogue **Configuration de la mise à jour**, cliquez sur l'onglet **Source alternative**, les options suivantes apparaissent :

■ **Depuis Sophos**

Sélectionnez cette option si vous avez des ordinateurs qui ne sont pas toujours connectés au réseau de l'entreprise, par exemple les portables. Les ordinateurs utiliseront les mêmes codes d'accès que votre copie du Sophos Control Center.

■ **Aucune**

Il s'agit de l'option par défaut. Ne spécifie pas de source alternative.

■ **Depuis votre entreprise**

Sélectionnez cette option si vous voulez que vos ordinateurs en réseau se mettent à jour depuis un site Web d'entreprise ou un répertoire, si l'emplacement de mise à jour principal devient indisponible. Saisissez l'adresse d'un dossier réseau (chemin UNC) ou d'un site Web (adresse HTTP).

Si nécessaire, entrez le nom utilisateur et le mot de passe d'un compte que vos ordinateurs peuvent utiliser pour accéder au dossier ou au site Web. Ce compte doit avoir les droits en lecture du répertoire que vous avez saisi dans le champ Adresse ci-dessus. Si le nom utilisateur doit avoir une qualification pour indiquer le domaine, utilisez la forme domaine\nomutilisateur.

Remarque : si vous spécifiez un dossier sur le réseau ou le site Web de votre entreprise, vous devez vous assurer que les copies régulièrement mises à jour des logiciels de sécurité sont disponibles dans ce dossier. Vous pouvez effectuer cette opération en installant le Sophos Control Center. Vous pouvez aussi faire le nécessaire pour publier des copies du dossier des mises à jour.

12 Configuration du pare-feu

12.1 Configuration du pare-feu

Vous pouvez configurer le pare-feu pour bloquer ou autoriser le trafic en fonction de vos besoins. Par défaut, le pare-feu bloque tout le trafic non indispensable.

Pour obtenir une liste complète des paramètres par défaut du pare-feu, consultez l'article suivant : <http://www.sophos.fr/support/knowledgebase/article/16608.html>

Pour configurer le pare-feu :

1. Dans le volet gauche, sous **Configuration**, cliquez sur **Configurer la mise à jour**.
2. Dans l'Assistant de configuration du pare-feu, cliquez sur **Suivant**.
3. Sur la page **Configuration du pare-feu**, choisissez l'une des options suivantes :
 - Sélectionnez **Autoriser tout le trafic** si vous voulez désactiver le pare-feu et autoriser l'intégralité du trafic.
 - Sélectionnez **Emplacement unique** pour les ordinateurs qui sont toujours sur le réseau, par exemple, les stations de travail.
 - Sélectionnez **Emplacement double** si vous voulez que le pare-feu utilise des paramètres différents en fonction de l'emplacement où les ordinateurs sont utilisés, par exemple, au bureau (sur le réseau) et en dehors du bureau. Il peut être intéressant de paramétrer un emplacement double pour les portables.
4. Si vous avez sélectionné **Emplacement double** sur la page précédente, sur la page **Identification réseau**, configurez l'identification DNS ou passerelle (Gateway) de votre réseau.

Remarque : la page **Identification réseau** apparaît seulement si vous sélectionnez **Emplacement double**.

Le Sophos Control Center applique ensuite les différents paramètres du pare-feu sur les ordinateurs en fonction de leur emplacement, c'est-à-dire sur le réseau ou en dehors du réseau.

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

Ceci permet à vos ordinateurs d'accéder à votre réseau et à Internet et de signaler les informations à la console.
 - **Bloquer le trafic entrant et autoriser le trafic sortant**

Ceci permet à vos ordinateurs d'accéder au réseau et à Internet mais de bloquer tout trafic entrant.
 - **Bloquer le trafic entrant et sortant**

Si vous sélectionnez cette option, le pare-feu bloquera tout le trafic sortant, sauf les applications que vous spécifiez en cliquant sur le bouton **Accepter** à droite de cette option. Pour une application "acceptée", toute l'activité du réseau est autorisée.

6. Cliquez sur **Avancés** pour ouvrir une configuration avancée pour le pare-feu.

Remarque : il s'agit d'une option avancée que vous devez utiliser uniquement si vous connaissez les effets des changements que vous apportez.

Pour plus d'informations sur la configuration avancée du pare-feu, reportez-vous à l'Aide de Sophos Endpoint Security and Control.

7. Sur la page **Partage de fichiers et d'imprimantes**, sélectionnez **Autoriser le partage de fichiers et d'imprimantes** si vous souhaitez permettre aux autres ordinateurs de votre réseau local d'accéder aux imprimantes et aux dossiers partagés de votre ordinateur.
8. Si vous avez sélectionné **Emplacement double**, vous serez invité à configurer le trafic entrant et sortant ainsi que le partage de fichiers et d'imprimantes (comme cela est mentionné dans les étapes 5 et 7) pour l'emplacement secondaire (hors réseau).

Après avoir paramétré le pare-feu, vous pouvez consulter les événements de pare-feu (par exemple, les applications bloquées par le pare-feu) dans le **Pare-feu - Observateur d'événements**. Pour plus d'informations, reportez-vous à la section [Consultation des événements du pare-feu](#) à la page 24.

Vous pouvez choisir d'exécuter de nouveau l'assistant, si vous choisissez de modifier ultérieurement l'un des paramètres.

Le nombre d'ordinateurs avec des événements au-dessus d'un seuil spécifié dans les dernières 24 heures apparaît aussi sur le Tableau de bord.

12.2 Désactivation du pare-feu

12.2.1 Désactivation du pare-feu depuis le Sophos Control Center

Vous pouvez choisir de désactiver le pare-feu pour tous les ordinateurs administrés depuis le Sophos Control Center.

Pour une utilisation quotidienne, Sophos vous conseille de conserver le pare-feu activé.

Pour désactiver le pare-feu depuis le Sophos Control Center :

1. Dans le volet gauche, sous **Configuration**, cliquez sur **Configurer la mise à jour**.
L'**Assistant de configuration du pare-feu** démarre.
2. Dans l'**Assistant de configuration du pare-feu**, allez sur la page **Configurer le pare-feu** et sélectionnez **Autoriser tout le trafic**.

12.2.2 Désactivation du pare-feu sur un ordinateur individuel

Vous pouvez choisir de désactiver le pare-feu pour des ordinateurs sélectionnés.

Pour désactiver le pare-feu sur un ordinateur individuel :

1. Dans la liste des ordinateurs, sélectionnez le ou les ordinateur(s). Cliquez avec le bouton droit de la souris et désélectionnez **Utiliser la configuration centralisée**.
Remarque : si vous paramétrez l'ordinateur pour qu'il utilise la configuration centralisée, ainsi que le pare-feu, vous pouvez aussi configurer Sophos Anti-Virus localement.
2. Allez à présent sur le ou les ordinateur(s) individuel(s) et désactivez le pare-feu en repérant l'icône du bouclier de Sophos Endpoint Security and Control.
 - a) Cliquez avec le bouton droit de la souris sur cette icône pour afficher un menu et sélectionnez **Ouvrir Sophos Endpoint Security and Control**.
 - b) Dans la section **Pare-feu**, cliquez sur **Configurer le pare-feu**.
La fenêtre de configuration du pare-feu apparaît.
 - c) Cliquez sur l'onglet **Généralités** et sélectionnez **Autoriser tout le trafic**. Cliquez sur **OK**.

12.3 Autorisation des applications bloquées

Si le pare-feu bloque une application sur vos ordinateurs en réseau, un événement est consigné dans le journal du pare-feu.

Pour obtenir plus de détails sur les applications bloquées, les autoriser ou leur créer de nouvelles règles, procédez comme suit :

1. Dans le menu **Affichage**, pointez votre curseur sur **Événements**, puis cliquez sur **Événements du pare-feu**.
2. Dans la boîte de dialogue **Pare-feu - Observateur d'événements**, sélectionnez l'entrée de l'application pour laquelle vous voulez autoriser ou créer une règle. Cliquez sur **Créer une règle**.
3. Dans la boîte de dialogue qui apparaît, indiquez si vous voulez autoriser l'application ou lui créer une règle à l'aide d'une option prédéfinie existante.
4. A partir de la liste des stratégies de pare-feu, sélectionnez celles auxquelles vous voulez appliquer la règle. Pour appliquer la règle à toutes les stratégies, cliquez sur **Tout sélectionner**, puis cliquez sur **OK**.

12.4 Configuration du pare-feu sur des ordinateurs individuels

Si vous voulez que certains ordinateurs utilisent des options différentes de celles définies centralement sur le Sophos Control Center, procédez ainsi :

1. Dans la liste des ordinateurs, mettez en surbrillance le ou les ordinateur(s). Cliquez avec le bouton droit de la souris et désélectionnez **Utiliser la configuration centralisée**.

2. Allez sur le ou les ordinateur(s) individuel(s) et configurez-y les options de pare-feu comme suit :
 - a) Sur l'ordinateur, repérez l'icône du bouclier de Sophos Endpoint Security and Control.
 - b) Cliquez avec le bouton droit de la souris sur cette icône pour afficher un menu et sélectionnez **Ouvrir Sophos Endpoint Security and Control**.
 - c) Dans la section **Pare-feu**, cliquez sur **Configurer le pare-feu**.

La fenêtre de configuration du pare-feu apparaît.

13 Configuration du contrôle des applications

13.1 A propos du contrôle des applications

Le Sophos Control Center vous permet de détecter et de bloquer les "applications contrôlées", c'est-à-dire des applications légitimes qui ne constituent pas une menace pour la sécurité, mais que vous considérez comme inappropriées dans votre environnement de bureau. Ces applications incluent des clients de messagerie instantanée (IM), des clients de voix sur IP (VoIP), des logiciels d'imagerie numérique, des lecteurs multimédia ou des plug-ins de navigateur.

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

La liste des applications contrôlées est fournie par Sophos et régulièrement mise à jour. Vous ne pouvez pas ajouter de nouvelles applications à la liste, mais vous pouvez soumettre une demande à Sophos pour inclure une nouvelle application légitime sur laquelle vous voulez avoir le contrôle sur votre réseau. Pour plus de détails, consultez l'article 35330 de la base de connaissances du support Sophos (<http://www.sophos.fr/support/knowledgebase/article/35330.html>).

Événements du contrôle des applications

Lorsqu'un événement de contrôle des applications se produit, par exemple, une application contrôlée a été détectée sur le réseau, l'événement est écrit dans le journal de événements du contrôle des applications qui est visible depuis le Sophos Control Center. Pour plus d'informations, reportez-vous à la section *Consultation des événements du contrôle des applications* à la page 23.

Par défaut, le nombre d'ordinateurs avec des événements au-dessus d'un seuil spécifié dans les dernières 24 heures apparaît sur le Tableau de bord.

Vous pouvez aussi configurer l'envoi des alertes par courriel aux destinataires de votre choix lorsqu'un événement de contrôle des applications s'est produit. Pour plus d'informations, reportez-vous à la section *Configuration des alertes de contrôle des applications* à la page 50.

13.2 Configuration du contrôle des applications

Vous pouvez configurer le Sophos Control Center pour qu'il recherche les applications que vous souhaitez contrôler lors de leur accès sur votre réseau.

1. Dans le volet gauche, sous **Configuration**, cliquez sur **Configurer le contrôle des applications**.

La boîte de dialogue **Configuration du contrôle des applications** apparaît.

2. Sur l'onglet **Contrôle**, définissez les options comme suit :

- Pour activer le contrôle sur accès, sélectionnez la case à cocher **Activer le contrôle sur accès**. Si vous voulez détecter des applications sans les bloquer sur accès, sélectionnez la case à cocher **Détecter mais autoriser l'exécution**.
- Pour activer le contrôle à la demande, sélectionnez la case à cocher **Activer le contrôle à la demande et sur planifié**.

Remarque : vos paramètres de stratégie antivirus et HIPS déterminent quels fichiers vont être contrôlés (c'est-à-dire les extensions et les exclusions).

3. Cliquez sur l'onglet **Autorisation** et sélectionnez les applications que vous voulez contrôler.

Pour plus d'informations sur la sélection des applications, reportez-vous à la section [Sélection des applications à contrôler](#) à la page 43.

Si vous voulez supprimer des applications contrôlées trouvées sur vos ordinateurs en réseau, suivez les instructions de la section [Désinstallation des applications contrôlées](#) à la page 44.

Il vous est aussi possible de faire envoyer les alertes à des utilisateurs particuliers lorsqu'une application contrôlée est découverte sur un des ordinateurs du groupe. Pour plus d'informations, reportez-vous à la section [Configuration des alertes de contrôle des applications](#) à la page 50

13.3 Sélection des applications à contrôler

Par défaut, toutes les applications sont autorisées. Vous pouvez sélectionner les applications que vous désirez contrôler de la manière suivante :

1. Dans le volet gauche, sous **Configuration**, cliquez sur **Configurer le contrôle des applications**.
2. Dans la boîte de dialogue **Configuration du contrôle des applications**, cliquez sur l'onglet **Autorisation**.
3. Sélectionnez le **Type d'application**, par exemple **Partage de fichiers**.

Une liste complète des applications incluses dans ce groupe apparaît dans la liste **Autorisées**.

- Pour bloquer une application, sélectionnez-la et déplacez-la dans la liste **Bloquées** en cliquant sur le bouton "Ajouter".



- Pour bloquer toutes les nouvelles applications que Sophos ajoutera à ce type à l'avenir, déplacez **Toutes ajoutées par Sophos à l'avenir** dans la liste **Bloquées**.
- Pour bloquer toutes les applications de ce type, déplacez toutes les applications de la liste **Autorisées** dans la liste **Bloquées** en cliquant sur le bouton "Ajouter tout".



13.4 Désinstallation des applications contrôlées

Avant de désinstaller les applications contrôlées, assurez-vous que le contrôle sur accès des applications contrôlées est désactivé. Ce type de contrôle bloque les programmes utilisés pour installer et désinstaller les applications, aussi il se peut qu'il perturbe la désinstallation.

Vous pouvez supprimer une application de deux manières :

- Rendez-vous sur chaque ordinateur et exécutez le programme de désinstallation correspondant au produit. Vous effectuez généralement cette opération en ouvrant le Panneau de configuration Windows et en utilisant Ajout/Suppression de programmes.
- Sur le serveur, utilisez votre script ou votre outil d'administration habituel pour lancer le programme de désinstallation correspondant au produit sur vos ordinateurs en réseau.

Vous pouvez à présent activer le contrôle sur accès des applications contrôlées.

14 Configuration du contrôle des périphériques

14.1 A propos du contrôle des périphériques

Important : le contrôle des périphériques Sophos ne doit pas être déployé en parallèle à des logiciels de contrôle des périphériques d'autres éditeurs.

Le contrôle des périphériques vous permet d'empêcher les utilisateurs d'utiliser sur leurs ordinateurs des périphériques de stockage externes, des supports de stockage amovibles et des technologies de connexion sans fil non autorisés. Ceci peut aider à réduire considérablement votre exposition aux pertes accidentelles de données et limiter les possibilités pour les utilisateurs d'introduire des logiciels de l'extérieur de votre environnement réseau.

Les périphériques de stockage amovibles, les unités de disque optiques et les lecteurs de disquettes peuvent aussi être paramétrés pour fournir un accès en lecture seule.

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

Si vous voulez activer le contrôle des périphériques pour la première fois, Sophos vous conseille de :

- Sélectionner des types de périphériques à contrôler.
- Détecter des périphériques sans les bloquer.
- Configurer les des alertes de contrôle des périphériques.
- Détecter et bloquer ou autoriser l'accès en lecture seule aux périphériques de stockage.

Événements de contrôle des périphériques

Lorsqu'un événement de contrôle des périphériques se produit, par exemple, un périphérique de stockage amovible a été bloqué, l'événement est consigné dans le journal des événements du contrôle des périphériques qui peut être consulté depuis le Sophos Control Center. Pour plus d'informations, reportez-vous à la section [Consultation des événements du contrôle des périphériques](#) à la page 23.

Par défaut, le nombre d'ordinateurs avec des événements au-dessus d'un seuil spécifié dans les dernières 24 heures apparaît sur le Tableau de bord.

Vous pouvez aussi configurer l'envoi des alertes par courriel aux destinataires de votre choix lorsqu'un événement de contrôle des périphériques s'est produit. Pour plus d'informations, reportez-vous à la section [Configuration des alertes de contrôle des périphériques](#) à la page 51.

14.2 Quels types de périphériques peuvent être contrôlés ?

Le contrôle des périphériques vous permet de bloquer trois types de périphériques : *stockage, réseau et courte portée*.

Stockage

- Périphériques de stockage amovibles (par exemple, les clés USB à mémoire flash, les lecteurs de cartes PC et les lecteurs de disques durs externes)

- Lecteurs de disques optiques (lecteurs de CD-ROM/DVD/Blu-ray)
- Lecteurs de disquettes
- Périphériques de stockage amovibles sécurisés (par exemple, lecteurs flash SanDisk Cruzer Enterprise, SanDisk Cruzer Enterprise FIPS Edition, Kingston Data Traveler Vault - Privacy Edition, Kingston Data Traveler BlackBox et IronKey Enterprise Basic Edition avec chiffrement matériel)

A l'aide de la catégorie de stockage amovible sécurisée, vous pouvez facilement autoriser l'utilisation de périphériques de stockage amovibles sécurisés pris en charge tout en bloquant d'autres. Pour obtenir une liste à jour des périphériques de stockage amovibles sécurisés pris en charge, visitez le site Web de Sophos (www.sophos.fr).

Réseau

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

Pour les interfaces réseau, vous pouvez définir un niveau d'accès supplémentaire du mode Bloquer le pont. Cela permet l'activation (c'est-à-dire les adaptateurs Wi-Fi) du périphérique réseau lorsque l'ordinateur est physiquement déconnecté du réseau. Sélectionnez l'option Bloquer le pont lors du choix des niveaux d'accès pour les périphériques réseau.

Remarque : le mode Bloquer le pont empêche tout pont de réseau, par exemple, entre un réseau professionnel et un réseau non professionnel. Ce mode est disponible pour les types de périphériques sans fil et modem. Ce mode fonctionne en désactivant les adaptateurs réseau sans fil ou modem lorsqu'un système d'extrémité est connecté à un réseau physique (généralement, via une connexion Ethernet). Une fois le poste déconnecté du réseau physique, les adaptateurs réseau sans fil ou modem sont réactivés de manière transparente.

Courte portée

- Interfaces Bluetooth
- Infrarouge (interfaces infrarouge IrDA)

Le contrôle des périphériques bloque à la fois les périphériques et les interfaces internes et externes. Par exemple, le blocage des interfaces Bluetooth va bloquer :

- L'interface Bluetooth incorporée dans un ordinateur
- Tous les adaptateurs Bluetooth de type USB connectés à l'ordinateur.

14.3 Configuration du contrôle des périphériques

Vous pouvez configurer le Sophos Control Center pour qu'il recherche les périphériques que vous souhaitez contrôler lors de leur accès sur votre réseau.

1. Dans le volet gauche, sous **Configuration**, cliquez sur **Configurer le contrôle des périphériques**.

La boîte de dialogue **Stratégie de contrôle des périphériques** apparaît.

2. Sur l'onglet **Configuration**, définissez les options comme suit :
 - Pour activer le contrôle des périphériques, sélectionnez la case à cocher **Activer le contrôle des périphériques**. Si vous voulez détecter des périphériques mais ne voulez pas les bloquer, sélectionnez la case à cocher **Détecter mais ne pas bloquer les périphériques**.
 - Pour définir le niveau d'accès de chaque type de périphérique, cliquez dans la colonne **Etat** située près du type de périphérique, puis cliquez sur la flèche de menu déroulant qui apparaît. Sélectionnez le type d'accès que vous voulez autoriser.

Par défaut, les périphériques ont un accès complet. Pour les périphériques de stockage amovibles, les unités de disque optiques et les lecteurs de disquettes, vous pouvez changer l'état de "Bloqué" ou en "Lecture seule". Pour les périphériques de stockage amovibles, vous pouvez changer cela en "Bloqué."

14.4 Exemption d'un périphérique

Vous pouvez exempter un périphérique des stratégies de contrôle des périphériques.

Vous pouvez exempter une instance ("ce périphérique uniquement") ou un modèle ("tous les périphériques de ce modèle") de périphérique. Ne paramétrez pas d'exemptions à la fois au niveau du modèle et de l'instance du périphérique. Si les deux sont définis, le niveau de l'instance du périphérique aura priorité.

Pour exempter un périphérique :

1. Dans le menu **Affichage**, cliquez sur **Événements du contrôle des périphériques**.

La boîte de dialogue **Contrôle des périphériques - Observateur d'événements** apparaît.
2. Si vous voulez afficher certains événements seulement, dans le volet **Critères de recherche**, définissez les filtres de façon appropriée et cliquez sur **Rechercher** pour afficher les événements.

Pour plus d'informations, reportez-vous à la section [Consultation des événements du contrôle des périphériques](#) à la page 23.
3. Sélectionnez l'entrée du périphérique que vous voulez exempter, puis cliquez sur **Exempter un périphérique**.

La boîte de dialogue **Exemption d'un périphérique** apparaît. Sous **Détails du périphérique**, le type, le modèle et l'identification du périphérique apparaissent.

15 Gestion des notifications

15.1 Configuration des notifications

Vous pouvez configurer Sophos Control Center pour qu'il envoie des alertes lorsque des menaces sont détectées sur votre réseau et/ou en cas de modification de l'état de votre réseau. Sophos Control Center vous permet également de choisir la façon dont vous souhaitez gérer les anciennes alertes.

Les alertes par courriel dans Sophos Control Center se divisent en deux catégories :

- Une alerte est envoyée aux destinataires de votre choix en cas de détection d'un virus, d'un comportement suspect, d'une application indésirable ou d'une erreur sur l'un des ordinateurs du réseau. Ces alertes sont configurées via les options **Configuration du contrôle > Messagerie**. Pour plus d'informations, reportez-vous à la section [Configuration des alertes antivirus et HIPS](#) à la page 48.
- Une alerte est envoyée aux destinataires de votre choix lors du dépassement d'un niveau défini sur le Tableau de bord. Il est configuré de deux façons :
 - **Outils > Configurer les alertes par courriel**
 - **Outils > Configurer le tableau de bord > Alertes par courriel**

Pour plus d'informations, reportez-vous à la section [Configuration des alertes par courriel sur l'état du réseau](#) à la page 49.

15.2 Configuration des alertes antivirus et HIPS

Sophos Control Center peut afficher une alerte sur le bureau ou envoyer une alerte par courriel si un virus ou une application potentiellement indésirable est détectée sur l'un des ordinateurs du réseau.

Pour configurer les alertes de contrôle :

1. Dans le volet gauche, sous **Configuration**, cliquez sur **Configurer le contrôle**.
2. Dans la boîte de dialogue **Configuration du contrôle**, cliquez sur **Messagerie**.
3. Dans le volet **Messagerie**, l'option **Activer la messagerie de bureau** est activée par défaut et toutes les options du volet **Messages à envoyer** sont sélectionnées. Vous pouvez modifier ces paramètres si nécessaire.

Dans la zone de texte Message défini par l'utilisateur, vous pouvez saisir un message qui sera ajouté à la fin du message de bureau standard.

4. Sur l'onglet **Alertes par courriel**, sélectionnez **Activer les alertes par courriel** pour recevoir les alertes par courriel.

Remarque : aucune alerte par courriel n'est envoyée au sujet d'éléments bloqués par le pare-feu.

5. Dans le volet **Messages à envoyer**, sélectionnez les événements pour lesquels vous voulez envoyer des alertes par courriel.

Remarque : les paramètres Détection des comportements suspects, Détection des fichiers suspects et Détection et nettoyage des adwares et des PUA s'appliquent seulement à Windows 2000 et supérieur. Le paramètre Autres erreurs s'applique uniquement à Windows.

6. Dans le volet **Destinataires**, cliquez sur **Ajouter** ou sur **Supprimer** pour respectivement ajouter ou supprimer des adresses électroniques auxquelles les alertes par courriel doivent être envoyées. Cliquez sur **Renommer** pour changer une adresse électronique que vous avez ajoutée.

Remarque : les ordinateurs Mac OS X envoient uniquement des messages au premier destinataire de la liste.

7. Cliquez sur **Configurer SMTP** pour changer les paramètres du serveur SMTP et la langue des alertes par courriel
8. Dans la boîte de dialogue **Configuration des paramètres SMTP**, saisissez les détails comme décrit ci-dessous.

- Dans la zone de texte **Serveur SMTP**, saisissez le nom d'hôte ou l'adresse IP du serveur SMTP. Cliquez sur Tester pour envoyer une alerte par courriel de test.
- Dans la zone de texte **Adresse expéditeur SMTP**, saisissez une adresse électronique à laquelle les messages renvoyés et les rapports de non-distribution peuvent être envoyés.
- Dans la zone de texte **Adresse réponse SMTP**, vous pouvez saisir une adresse électronique à laquelle les réponses aux alertes par courriel peuvent être envoyées. Les alertes par courriel sont envoyées depuis une boîte aux lettres sans surveillance.

Remarque : les ordinateurs Linux et UNIX ignorent les adresses expéditeur et réponse SMTP et utilisent l'adresse root@<nomhôte>.

- Dans le volet **Langue**, cliquez sur la flèche du menu déroulant et sélectionnez la langue dans laquelle les alertes par courriel doivent être envoyées.

15.3 Configuration des alertes par courriel sur l'état du réseau

Vous pouvez paramétrer l'envoi d'alertes par courriel aux destinataires de votre choix lorsqu'un seuil d'alerte a été atteint sur le Tableau de bord.

Pour configurer les alertes par courriel :

1. Dans le menu **Outils**, sélectionnez **Configurer les alertes par courriel**.

La boîte de dialogue **Configuration des alertes par courriel** apparaît.

2. Si les paramètres SMTP n'ont pas été configurés ou si vous voulez visualiser ou changer les paramètres, cliquez sur **Configurer**. Dans la boîte de dialogue **Configuration des paramètres SMTP**, saisissez les détails comme décrit ci-dessous :
 - a) Dans la zone de texte **Adresse du serveur**, saisissez le nom d'hôte ou l'adresse IP du serveur SMTP.
 - b) Dans la zone de texte **Expéditeur**, saisissez une adresse électronique à laquelle les messages renvoyés et les rapports de non-distribution peuvent être envoyés.
 - c) Cliquez sur **Tester** pour tester la connexion.
3. Dans le volet **Destinataires**, cliquez sur **Ajouter**.

La boîte de dialogue **Ajout d'un nouveau destinataire d'alerte par courriel** apparaît.
4. Dans le champ **Adresse électronique**, saisissez l'adresse de votre destinataire.
5. Dans le champ **Langue**, sélectionnez la langue dans laquelle vous souhaitez que soient envoyées les alertes par courriel.
6. Dans le volet **Abonnements**, sélectionnez les options qui doivent être envoyées au destinataire sous la forme d'une alerte par courriel lorsqu'un niveau seuil est dépassé.

Pour plus d'informations sur la manière de modifier les valeurs seuil, reportez-vous à la section [Configuration du tableau de bord](#) à la page 9.

15.4 Configuration des alertes de contrôle des applications

Vous pouvez envoyer des alertes à des utilisateurs particuliers lors de la découverte d'une application contrôlée.

1. Dans le volet gauche, sous **Configuration**, cliquez sur **Configurer le contrôle des applications**.

La boîte de dialogue **Configuration du contrôle des applications** apparaît.
2. Sur l'onglet **Messagerie**, définissez les options comme cela est décrit ci-dessous :
 - a) Dans le volet **Messagerie**, la case à cocher **Activer la messagerie de bureau** est activée par défaut.

Lorsqu'une application contrôlée non autorisée est détectée par le contrôle sur accès et bloquée, un message apparaît sur le bureau informant l'utilisateur que l'application a été bloquée.
 - b) Dans la zone **Texte du message**, saisissez un message que vous voulez voir ajouté à la fin du message standard du bureau.
 - c) Sélectionnez la case **Activer les alertes par courriel** pour que Sophos Anti-Virus puisse envoyer des alertes par courriel. Pour plus d'informations sur la configuration des alertes par courriel, reportez-vous à la section [Configuration des alertes antivirus et HIPS](#) à la page 48.

15.5 Configuration des alertes de contrôle des périphériques

Vous pouvez envoyer des alertes à des utilisateurs particuliers lorsqu'un événement de contrôle des périphériques est rencontré.

1. Dans le volet gauche, sous **Configuration**, cliquez sur **Configurer le contrôle des périphériques**.

La boîte de dialogue **Configuration du contrôle des périphériques** apparaît.

2. Sur l'onglet **Messagerie**, définissez les options comme cela est décrit ci-dessous :

- a) Dans le volet **Messagerie**, la case à cocher **Activer la messagerie de bureau** est activée par défaut.

Lorsqu'un périphérique non autorisé est détecté par le contrôle sur accès et bloqué, un message apparaît sur le bureau informant l'utilisateur que le périphérique a été bloqué.

- b) Dans la zone **Texte du message**, saisissez un message que vous voulez voir ajouté à la fin du message standard du bureau.

- c) Sélectionnez la case **Activer les alertes par courriel** pour que le Sophos Control Center puisse envoyer des alertes par courriel.

Dans le champ **Destinataires de la messagerie**, saisissez les adresses électroniques auxquelles vous voulez envoyer les alertes.

15.6 Suppression d'anciennes alertes

Vous pouvez configurer le Sophos Control Center pour qu'il supprime automatiquement d'anciennes alertes. Par défaut, les alertes sont stockées dans la base de données pendant 12 mois, puis sont supprimées.

Remarque : les alertes à traiter ne sont jamais supprimées.

Pour supprimer d'anciennes alertes :

1. Dans le menu **Outils**, sélectionnez **Configurer les rapports**.

La boîte de dialogue **Configuration des rapports** apparaît.

2. Cliquez sur l'onglet **Purge**.

Dans le volet **Purge**, en fonction de vos besoins en matière de rapports, choisissez la manière dont vous voulez gérer les anciennes alertes.

- **Ne pas purger les anciennes alertes.**
- **Purger les alertes antérieures à n mois** (où n est un nombre que vous spécifiez).

16 Gestion des rapports

16.1 Génération d'un rapport

Vous pouvez générer un rapport existant à l'aide du gestionnaire des rapports.

Pour générer un rapport :

1. Dans la fenêtre Sophos Control Center, dans la barre d'outils, cliquez sur **Rapports**.
La boîte de dialogue **Gestionnaire des rapports** apparaît.
2. Sélectionnez le type de rapport que vous voulez générer.
Pour plus d'informations sur la création d'un nouveau rapport, reportez-vous à la section [Création d'un nouveau rapport](#) à la page 52.
3. Cliquez sur **Exécuter**.

Un rapport apparaît récapitulant les critères utilisés pour créer le rapport.

4. Choisissez l'un des onglets suivants pour visualiser le rapport au format désiré :

Remarque : selon les critères du rapport, il se peut que certains de ces rapports n'aient qu'un seul format d'affichage des données.

- **Diagramme**
- **Tableau**

16.2 Création d'un nouveau rapport

Vous pouvez créer un nouveau rapport à l'aide du gestionnaire des rapports.

Pour créer un nouveau rapport :

1. Dans la fenêtre Sophos Control Center, dans la barre d'outils, cliquez sur **Rapports**.
La boîte de dialogue **Gestionnaire des rapports** apparaît.
2. Cliquez sur **Créer**.
La fenêtre **Création d'un nouveau rapport** apparaît.
 - A l'aide de l'assistant : Dans le menu déroulant, sélectionnez le modèle de rapport que vous voulez utiliser et cliquez sur **OK**.
L'assistant vous guide tout au long du processus de création d'un rapport d'après le modèle sélectionné.
 - A l'aide de la fenêtre Propriétés : Deselectionnez la case à cocher **Utiliser l'assistant pour créer le rapport** et cliquez sur **OK**.
Une fenêtre **Propriétés** apparaît avec des options pour créer un rapport.

16.3 Configuration des rapports planifiés

Le Sophos Control Center peut envoyer des rapports avec le nombre et les détails des menaces trouvées lors de la période spécifiée.

Les destinataires recevront un rapport par courriel avec les informations suivantes :

- Date du rapport
- Nom de l'entreprise (Cliquez sur **Outils** > **Configurer les rapports** pour choisir le nom de votre entreprise)
- Nombre de fichiers/comportements suspects
- Nombre d'adwares/applications potentiellement indésirables détectés
- Nombre de virus/spywares détectés.
- Liste de menaces détectées dans l'ordre chronologique, avec le nom de la menace et le nombre d'infections
- Liste des applications bloquées dans l'ordre chronologique, avec le nom de l'application et le nombre d'ordinateurs affectés Vous pouvez inclure les alertes Bloqué par le pare-feu, Applications contrôlées et Contrôle des périphériques.

Pour configurer les rapports planifiés :

1. Dans la fenêtre Sophos Control Center, dans la barre d'outils, cliquez sur **Rapports**.
La boîte de dialogue **Gestionnaire des rapports** apparaît.
2. Sélectionnez un rapport existant et cliquez sur **Planifier**.
La boîte de dialogue des *propriétés* de **Nom du rapport** apparaît (où *Nom du rapport* correspond au nom de votre rapport).
3. Sur l'onglet **Planification**, paramétrez les options comme requis :
 - a) Sélectionnez **Planifier ce rapport**.
 - b) Sous la section Planification, choisissez l'heure et la date voulues de génération du rapport dans les champs **Démarrer à** et **Le**.
Dans le menu déroulant **Répéter**, définissez la fréquence à laquelle vous souhaitez que le rapport soit généré.
 - c) Dans la section **Sortie**, sélectionnez un **Format** sous lequel vous souhaitez envoyer la pièce jointe de courriel.
 - d) Choisissez la **Langue** dans laquelle vous voulez recevoir le rapport.
 - e) Sélectionnez l'adresse électronique à laquelle vous voulez envoyer le courriel et ajoutez-la aux destinataires.
Vous devez configurer les paramètres du serveur SMTP pour envoyer des messages. Pour plus d'informations sur la manière de configurer ces paramètres, reportez-vous à la section [Configuration des alertes par courriel sur l'état du réseau](#) à la page 49.

16.4 Modification d'un rapport

Vous pouvez modifier un rapport existant et générer des données.

Pour modifier un rapport existant :

1. Dans la fenêtre Sophos Control Center, dans la barre d'outils, cliquez sur **Rapports**.
2. Dans la boîte de dialogue **Gestionnaire des rapports**, sélectionnez le rapport que vous voulez modifier et cliquez sur **Propriétés**.

Remarque : en fonction des critères sélectionnés, seuls certains des champs apparaissent dans les onglets.

3. Dans l'onglet **Configuration**, sélectionnez l'une des options suivantes pour modifier :

- **Détails du rapport**

Saisissez le **Nom** sous lequel enregistré le rapport. Par défaut, la boîte **Description** du rapport contient une description d'après les sélections qui ont été faites.

- **Période du rapport**

Dans la liste déroulante **Période**, sélectionnez une période de temps définie. Sélectionnez **Personnalisé** pour spécifier une période à l'aides des zones **De** et **A**.

- **Emplacement du rapport**

Sélectionnez la liste déroulante **Tous les ordinateurs** ou **Ordinateur individuel** pour spécifier le nom d'un ordinateur.

- **Types d'alertes à inclure**

Sélectionnez les types d'alertes que vous voulez inclure.

Vous pouvez configurer le rapport pour qu'il affiche uniquement les ordinateurs ayant signalé une menace particulière. Pour spécifier une seule menace, cliquez sur **Avancés**.

Dans la fenêtre **Configuration avancée**, sélectionnez le alertes à inclure dans le rapport. Vous pouvez saisir un nom de menace dans la zone de texte **Expression** ou pour spécifier plus d'une menace, saisissez un nom dans cette zone de texte en utilisant des caractères jokers. Utilisez ? pour remplacer un seul caractère du nom et * pour remplacer une chaîne de caractères quelconque. Par exemple, W32/* correspond à tous les virus dont le nom commence par W32/.

4. Dans l'onglet **Options d'affichage**, sélectionnez l'une des options suivantes pour modifier :
 - Par défaut, les **Options d'affichage** affichent tous les éléments sélectionnés. Par contre, vous pouvez configurer le rapport qu'il indique :
 - Seulement les n premières alertes (où n est un nombre que vous définissez).
 - Seules les alertes avec n occurrences ou plus.
 - **Afficher les résultats par**
Par défaut, les résultats sont affichés par **Jour**. Vous pouvez aussi choisir de les afficher par **Heure**, **Semaine** ou **Mois**.
 - **Afficher les résultats en**
Par défaut, les résultats sont affichés en **Pourcentages**. Vous pouvez aussi choisir de les afficher en **Chiffres**.
 - **Tri par**
Par défaut, le rapport répertorie les menaces dans l'ordre décroissant du nombre d'alertes par menace. Vous pouvez aussi choisir de les trier par **Nom d'alerte**, **Nom d'ordinateur** ou **Date et heure**.
5. Dans l'onglet Planification, sélectionnez les options pour modifier la planification :
 - a) Sélectionnez **Planifier ce rapport**.
 - b) Sous la section Planification, choisissez l'heure et la date voulues de génération du rapport dans les champs **Démarrer à** et **Le**.

La liste déroulante **Répéter** vous permet de choisir la fréquence à laquelle vous voulez répéter la tâche.
 - c) Dans la section **Sortie**, sélectionnez un **Format du fichier** sous lequel vous souhaitez envoyer la pièce jointe de courriel.
 - d) Choisissez la **Langue** dans laquelle vous voulez recevoir le rapport.
 - e) Sélectionnez l'adresse électronique à laquelle vous voulez envoyer le courriel et ajoutez-la aux destinataires.

Pour plus d'informations sur la configuration ou l'ajout d'adresses électroniques, reportez-vous à la section [Configuration des alertes par courriel sur l'état du réseau](#) à la page 49.

16.5 Exporter un rapport dans un fichier

Une fois que le rapport a été généré, vous pouvez choisir de l'exporter dans plusieurs formats. Pour exporter un rapport dans un fichier :

1. Dans la fenêtre Sophos Control Center, dans la barre d'outils, cliquez sur **Rapports**.
La boîte de dialogue **Gestionnaire des rapports** apparaît.

2. Sélectionnez un rapport que vous souhaitez exporter et cliquez sur **Exécuter**.
3. Dans la fenêtre **Edition de rapports**, sur la barre d'outils, cliquez sur l'icône **Exporter**.



4. Dans la boîte de dialogue **Exportation du rapport**, sélectionnez le type de document ou de feuille de calcul dans lequel vous souhaitez exporter le rapport.
5. Cliquez sur le bouton de navigation **Nom du fichier** pour sélectionner un emplacement.
6. Dans la boîte de dialogue **Enregistrer sous**, naviguez vers un emplacement sous lequel vous voulez enregistrer le rapport, saisissez un nom de rapport, puis cliquez sur **Enregistrer**.
7. Dans la boîte de dialogue **Exportation du rapport**, cliquez sur **OK**.

16.6 Modifier la mise en page du rapport

Vous pouvez modifier la mise en page utilisée pour les rapports. Par exemple, vous pouvez afficher un rapport au format paysage (largeur de page).

Pour modifier la mise en page du rapport :

1. Dans la fenêtre Sophos Control Center, dans la barre d'outils, cliquez sur **Rapports**.
La boîte de dialogue **Gestionnaire des rapports** apparaît.
2. Sélectionnez un rapport et cliquez sur **Exécuter**.
3. Dans la fenêtre **Edition de rapports**, sur la barre d'outils, cliquez sur l'icône de mise en page.



4. Dans la boîte de dialogue **Mise en page**, définissez la taille, l'orientation et les marges de la page. Cliquez sur **OK**. Le rapport s'affichera ensuite avec ces paramètres de mise en page.
5. Ces paramètres de mise en page seront aussi utilisés lorsque vous imprimerez ou exporterez le rapport.

17 Résolution des problèmes

17.1 Echec du nettoyage

S'il n'est pas possible de supprimer une menace de manière centralisée, allez sur l'ordinateur infecté et exécutez le nettoyage manuellement.

Si la menace n'a pas été supprimée et si vous avez besoin d'assistance pour vous en occuper :

1. Notez le nom de la menace.
2. Dans le volet gauche, sous **Informations**, cliquez sur **Informations sur la menace** pour vous connecter à la page des analyses des menaces sur le site Web de Sophos.
3. Sur la page des analyses des menaces, recherchez la menace. Suivez les liens pour obtenir des conseils sur le nettoyage.

Si vous n'arrivez pas à éliminer la menace vous-même, sous **Informations**, cliquez sur **Support technique**.

Saisissez le nom de la menace et les détails du ou des ordinateur(s) affecté(s) et envoyez-nous un courriel.

17.2 Alertes régulières concernant les applications potentiellement indésirables

Il est possible que vous receviez un très grand nombre d'alertes à propos d'applications potentiellement indésirables, y compris de nombreux rapports concernant la même application.

Ceci peut se produire si certains types d'applications potentiellement indésirables "surveillent" les fichiers et essayent d'y accéder régulièrement. Si le contrôle sur accès est activé, Sophos Anti-Virus détecte chaque accès à un fichier et envoie une alerte.

Procédez de la manière suivante :

- Désactivez le contrôle sur accès à la recherche des applications potentiellement indésirables. Vous pouvez utiliser un contrôle planifié à la place.
- Autorisez l'application si vous désirez qu'elle soit exécutée sur vos ordinateurs. Pour plus d'informations, reportez-vous à la section [Autorisation des applications à l'utilisation](#) à la page 31.
- Nettoyez les applications que vous n'avez pas autorisées. Pour plus d'informations, reportez-vous à la section [Nettoyage de votre ordinateur](#) à la page 14.

18 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

19 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 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>

ACE™, TAO™, CIAO™, and CoSMIC™

ACE¹, TAO², CIAO³, and CoSMIC⁴ (henceforth referred to as “DOC software”) are copyrighted by Douglas C. Schmidt⁵ and his research group⁶ at Washington University⁷, University of California⁸, Irvine, and Vanderbilt University⁹, Copyright © 1993–2005, all rights reserved.

Since DOC software is open-source¹⁰, free software, you are free to use, modify, copy, and distribute—perpetually and irrevocably—the DOC software source code and object code produced from the source, as well as copy and distribute modified versions of this software. You must, however, include this copyright statement along with code built using DOC software.

You can use DOC software in commercial and/or binary software releases and are under no obligation to redistribute any of your source code that is built using DOC software. Note, however, that you may not do anything to the DOC software code, such as copyrighting it yourself or claiming authorship of the DOC software code, that will prevent DOC software from being distributed freely using an open-source development model. You needn't inform anyone that you're using DOC software in your software, though we encourage you to let us¹¹ know so we can promote your project in the DOC software success stories¹².

DOC software is provided as is with no warranties of any kind, including the warranties of design, merchantability, and fitness for a particular purpose, noninfringement, or arising from a course of dealing, usage or trade practice. Moreover, DOC software is provided with no support and without any obligation on the part of Washington University, UC Irvine, Vanderbilt University, their employees, or students to assist in its use, correction, modification, or enhancement. A number of companies¹³ around the world provide commercial support for DOC software, however. DOC software is Y2K-compliant, as long as the underlying OS platform is Y2K-compliant.

Washington University, UC Irvine, Vanderbilt University, their employees, and students shall have no liability with respect to the infringement of copyrights, trade secrets or any patents by DOC software or any part thereof. Moreover, in no event will Washington University, UC Irvine, or Vanderbilt University, their employees, or students be liable for any lost revenue or profits or other special, indirect and consequential damages.

The ACE¹⁴, TAO¹⁵, CIAO¹⁶, and CoSMIC¹⁷ web sites are maintained by the DOC Group¹⁸ at the Institute for Software Integrated Systems (ISIS)¹⁹ and the Center for Distributed Object Computing of Washington University, St. Louis²⁰ for the development of open-source software as part of the open-source software community²¹. By submitting comments, suggestions, code, code snippets, techniques (including that of usage), and algorithms, submitters acknowledge that they have the right to do so, that any such submissions are given freely and unreservedly, and that they waive any claims to copyright or ownership. In addition, submitters acknowledge that any such submission might become part of the copyright maintained on the overall body of code, which comprises the DOC software. By making a submission, submitter agree to these terms. Furthermore, submitters acknowledge that the incorporation or modification of such submissions is entirely at the discretion of the moderators of the open-source DOC software projects or their designees.

The names ACE, TAO, CIAO, CoSMIC, Washington University, UC Irvine, and Vanderbilt University, may not be used to endorse or promote products or services derived from this source without express written permission from Washington University, UC Irvine, or Vanderbilt University. Further, products or services derived from this source may not be called ACE, TAO, CIAO, or CoSMIC nor may the name Washington University, UC Irvine, or Vanderbilt University appear in their names, without express written permission from Washington University, UC Irvine, and Vanderbilt University.

If you have any suggestions, additions, comments, or questions, please let me²² know.

Douglas C. Schmidt²³

The ACE home page is <http://www.cs.wustl.edu/ACE.html>

References

1. <http://www.cs.wustl.edu/~schmidt/ACE.html>
2. <http://www.cs.wustl.edu/~schmidt/TAO.html>
3. <http://www.dre.vanderbilt.edu/CIAO/>
4. <http://www.dre.vanderbilt.edu/cosmic/>
5. <http://www.dre.vanderbilt.edu/~schmidt/>
6. <http://www.cs.wustl.edu/~schmidt/ACE-members.html>
7. <http://www.wustl.edu/>
8. <http://www.uci.edu/>
9. <http://www.vanderbilt.edu/>
10. [://www.the-it-resource.com/Open-Source/Licenses.html](http://www.the-it-resource.com/Open-Source/Licenses.html)
11. mailto:doc_group@cs.wustl.edu
12. <http://www.cs.wustl.edu/~schmidt/ACE-users.html>
13. <http://www.cs.wustl.edu/~schmidt/commercial-support.html>
14. <http://www.cs.wustl.edu/~schmidt/ACE.html>
15. <http://www.cs.wustl.edu/~schmidt/TAO.html>
16. <http://www.dre.vanderbilt.edu/CIAO/>

17. <http://www.dre.vanderbilt.edu/cosmic/>
18. <http://www.dre.vanderbilt.edu/>
19. <http://www.isis.vanderbilt.edu/>
20. <http://www.cs.wustl.edu/~schmidt/doc-center.html>
21. <http://www.opensource.org/>
22. <mailto:d.schmidt@vanderbilt.edu>
23. <http://www.dre.vanderbilt.edu/~schmidt/>

Index

A

- activer un contrôle sur accès 26
- afficher les ordinateurs 20
- alertes
 - antivirus 48
 - configurer 48
 - contrôle des applications 50
 - contrôle des périphériques 51
 - état du réseau 49
 - HIPS 48
 - supprimer 51
 - tableau de bord 49
- applications contrôlées
 - bloquer 42
 - sélectionner les applications 43
- approuver
 - alertes 17
 - erreurs 17
- assistant de protection automatique 10
- autoriser les applications 31

B

- bloquer
 - applications contrôlées 42

C

- changer
 - identification de l'utilisateur 35
 - proxy 35
- configuration centrale 19
- configuration du Tableau de bord 9
- configurer le contrôle 34
- configurer les fichiers
 - Mac 28
 - Windows 28
- configurer un contrôle sur accès 26
- configurés localement 19
- conformité à la configuration 19
- contrôle
 - PUA 26
 - sur accès 26, 27
- contrôle des applications 42
 - alertes 50

- contrôle des applications (*suite*)
 - événements 23
- contrôle des périphériques
 - activer le contrôle des périphériques 46
 - alertes 51
 - événements 23
- Contrôle des périphériques
 - aperçu 45
 - blocage du pont 45
 - exemption d'un périphérique 47
 - réseau
 - courte portée 45
 - stockage 45
 - types de périphériques 45
- contrôle planifié 26, 32
- contrôle web 29
- contrôler les ordinateurs individuels 34
- créer
 - rapports 52

D

- dernière mise à jour 12
- désactiver
 - mises à jour automatique 36
 - pare-feu
 - ordinateur individuel 39
 - Sophos Control Center 39
- désinfection 14
- désinstallation
 - applications contrôlées 44
- désinstallation des applications contrôlées 44

E

- échec du nettoyage 57
- état de l'ordinateur 20
- événements 23
 - contrôle des applications 23
 - contrôle des périphériques 23
 - copie dans le Presse-papiers 25
 - exportation dans un fichier 25
 - pare-feu 24
- exclure du contrôle 29
- exclure du contrôle planifié 33
- exporter
 - rapports 55

F

fichiers suspects 31

G

générer
rapports 52

I

icônes 5
imprimer le récapitulatif 21
informations sur les menaces 16
interface
vue Gestionnaires de mise à jour 4
vue Systèmes d'extrémité 4
interface de Sophos Control Center 4

M

messagerie de bureau 48
mise à jour
automatique 36
hors réseau 36
identification de l'utilisateur 35
intervalle 36
proxy 35
sélectionner les applications 35
mise à jour d'un ordinateur individuel 13
mise à jour du réseau 13
mise à jour immédiate 13
mise à jour manuelle 13
mise en page
rapports 56
modifier
rapports 54

N

nettoyage 14
échec 57
nettoyage automatique 30
PUA 31
virus 30

O

options de contrôle
exclure un fichier 28

options de contrôle (*suite*)
inclure une extension 28
options de contrôle planifié 32
options de contrôle sur accès 27
ordinateurs administrés 5
ordinateurs non à jour
mise à jour 13
ordinateurs non connectés 5
ordinateurs protégés 20

P

pare-feu
autorisation des applications 40
configuration 38
configurer le pare-feu sur des ordinateurs
individuels 40
désactiver depuis Sophos Control Center 39
désactiver sur un ordinateur individuel 39
événements 24
planification
rapports 53
priorité des alertes 7
processus de mise à jour 12
protection des ordinateurs
assistant de protection automatique 10
protection des systèmes d'exploitation 11
PUA
alertes régulières 57

R

rapports
créer 52
exporter 55
générer 52
mise en page 56
modifier 54
planification 53
re-protection des ordinateurs 18
recherche des ordinateurs supprimés 20
réseau protégé 20
résolution des problèmes
alertes régulières 57
nettoyage 57
PUA 57
résoudre
alertes 17
erreurs 17
menaces 14

restaurer la configuration centralisée 19

S

signaux d'avertissement 5
Sophos Control Center 3, 4

T

Tableau de bord
aperçu 8

Tableau de bord (*suite*)
configuration 9

V

vérification de la mise à jour 12
vérification du réseau 20
vue Systèmes d'extrémité 4