SOPHOS

Cybersecurity made simple.

Sophos Enterprise Console

Aide

Version du produit : 5.5

Table des matières

1 À propos de Sophos Enterprise Console

Sophos Enterprise Console est une console automatisée qui administre et met à jour les logiciels de sécurité Sophos sur les ordinateurs utilisant des systèmes d'exploitation Windows, Mac OS X, Linux et UNIX et sur les environnements virtuels VMware vShield.

Enterprise Console vous permet d'exécuter les opérations suivantes :

- Protéger votre réseau contre les programmes malveillants, les types de fichiers et les sites Web dangereux, le trafic réseau malveillant et contre les adwares et autres applications potentiellement indésirables.
- Contrôler les sites Web sur lesquels les utilisateurs peuvent se rendre, protégeant ainsi davantage le réseau contre les malwares et empêchant tout utilisateur de se rendre sur des sites Web inappropriés.
- Contrôler quelles applications peuvent fonctionner sur le réseau.
- Administrer la protection du pare-feu client sur les terminaux.
- Évaluer les ordinateurs à la recherche de tout correctif manquant.
- Réduire la perte accidentelle de données, comme le transfert involontaire de données sensibles depuis des terminaux.
- Empêcher l'utilisation de périphériques de stockage externes non autorisés et de technologies de connexion sans fil sur des terminaux.
- Empêcher l'utilisateur de reconfigurer, désactiver ou désinstaller les logiciels de sécurité Sophos.

Remarque
Certaines des fonctionnalités ci-dessus ne sont pas incluses dans toutes les licences. Si vous voulez les utiliser, il se peut que vous deviez changer votre contrat de licence. Retrouvez plus de renseignements sur les licences disponibles sur www.sophos.com/fr-fr/products/enduser-protection-suites/how-to-buy et sur www.sophos.com/fr-fr/products/server-security/how-to-buy.

2 Guide de l’interface de l’Enterprise Console

2.1 Agencement de l’interface d’utilisation

L’interface d’utilisation de Enterprise Console est composée des sections suivantes :

Barre d’outils

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

Retrouvez plus de renseignements à la section Boutons de la barre d’outils (page 2).

Tableau de bord

Le **Tableau de bord** donne un aperçu rapide de l’état de la sécurité de votre réseau.

Retrouvez plus de renseignements à la section Volets du tableau de bord (page 4).

Liste des ordinateurs

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

- La vue **Terminaux** affiche les ordinateurs du groupe sélectionné dans le volet **Groupes** en bas à gauche. Retrouvez plus de renseignements à la section Navigation dans la vue Terminaux (page 6).
- La vue **Gestionnaires de mise à jour** affiche les ordinateurs sur lesquels Sophos Update Manager est installé. Retrouvez plus de renseignements à la section Navigation dans la vue Gestionnaires de mise à jour (page 10).

2.2 Boutons de la barre d’outils

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

Bouton de la barre d'outils	Description	Remarques
	**Détecter des ordinateurs**	Recherche des ordinateurs sur le réseau et les ajoute à la console. Retrouvez plus de renseignements à la section Détection des ordinateurs sur le réseau (page 34).
	**Créer un groupe**	Crée un nouveau groupe pour les ordinateurs. Retrouvez plus de renseignements à la section Création d'un groupe (page 25).
	**Voir/modifier une stratégie**	Ouvre la stratégie sélectionnée dans le volet **Stratégies** en vue d'une modification. Retrouvez plus de renseignements à la section Modification d'une stratégie (page 32).
	**Protéger**	Installe les logiciels antivirus et de pare-feu sur les ordinateurs sélectionnés dans la liste des ordinateurs. Retrouvez plus de renseignements à la section Protection automatique des ordinateurs (page 46).
	**Terminaux**	Passe à la vue **Terminaux** dans la liste des ordinateurs. La vue **Terminaux** affiche les ordinateurs du groupe qui est sélectionné dans le volet **Groupes**. Retrouvez plus de renseignements à la section Navigation dans la vue Terminaux (page 6).
	**Gestionnaires de mise à jour**	Passe à la vue **Gestionnaires de mise à jour** dans la liste des ordinateurs. La vue **Gestionnaires de mise à jour** affiche les ordinateurs sur lesquels Sophos Update Manager est installé. Retrouvez plus de renseignements à la section Navigation dans la vue Gestionnaires de mise à jour (page 10).
	**Tableau de bord**	Affiche ou masque le **Tableau de bord**. Le **Tableau de bord** donne un aperçu rapide de l'état de la sécurité de votre réseau. Retrouvez plus de renseignements à la section Volets du tableau de bord (page 4).
	**Rapports**	Démarre le **Gestionnaire des rapports** de manière à ce que vous puissiez générer des rapports sur les alertes et sur les événements sur votre réseau. Retrouvez plus de renseignements à la section Création de rapports (page 212).

Bouton de la barre d'outils	Description	Remarques
	**Sophos Central**	Ouvre Sophos Central. Retrouvez plus de renseignements sur Sophos Central dans l'article 119598 de la base de connaissances. Retrouvez plus de renseignements sur la migration vers Sophos Central dans l'article 122264 de la base de connaissances.
	**Sophos Mobile**	Lorsque l'URL de Sophos Mobile est configurée, la console Web Sophos Mobile s'ouvre. Il s'agit d'une solution de gestion des appareils mobiles (smartphones et tablettes) qui va vous aider à gérer les apps et les paramètres de sécurité. Retrouvez plus de renseignements à la section Configuration de l'URL de Sophos Mobile (page 44).

2.3 Volets du tableau de bord

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

Volet du Tableau de bord	Description
Ordinateurs	Indique le nombre total d'ordinateurs sur le réseau ainsi que le nombre d'ordinateurs connectés, administrés et non administrés. Pour voir une liste des ordinateurs administrés, non administrés, connectés ou de tous les ordinateurs, cliquez sur l'un des liens de la section **Ordinateurs**.
Mises à jour	Indique l'état des gestionnaires de mise à jour.
Ordinateurs avec alertes	Indique le nombre et le pourcentage d'ordinateurs administrés avec des alertes concernant : • Des virus et des spywares connus et inconnus • Des comportements et fichiers suspects • Des adwares et autres applications potentiellement indésirables Pour voir une liste des ordinateurs administrés avec des alertes à traiter, cliquez sur le titre du volet **Ordinateurs avec alertes**.

Volet du Tableau de bord	Description
Ordinateurs au-dessus du seuil	Indique le nombre d'ordinateurs avec des événements au-dessus du seuil au cours des sept derniers jours. Pour consulter une liste des ordinateurs avec le contrôle des périphériques, le contrôle des données, le contrôle des applications ou des événements de pare-feu, cliquez sur le lien respectif dans le volet **Ordinateurs dépassant le seuil d'un événement**. **Remarque** Selon votre licence, il se peut que certains types d'événements ne s'affichent pas.
Stratégies	Indique le nombre et le pourcentage d'ordinateurs administrés avec violations de leur stratégie de groupe ou erreurs de comparaison de stratégie. Il inclut aussi les ordinateurs qui n'ont pas encore répondu à la stratégie modifiée que leur a transmis la console. Pour voir une liste des ordinateurs administrés qui diffèrent de la stratégie, cliquez sur le titre du volet **Stratégies**.
Protection	Indique le nombre et le pourcentage d'ordinateurs administrés et connectés sur lesquels Sophos Endpoint Security and Control ou Sophos Anti-Virus est obsolète ou utilise des données de détection inconnues. Pour voir une liste des ordinateurs administrés connectés et non à jour, cliquez sur le titre du volet **Protection**.
Erreurs	Indique le nombre et le pourcentage d'ordinateurs administrés ayant des erreurs de contrôle, de mise à jour ou de pare-feu à traiter. Pour voir une liste des ordinateurs administrés avec des erreurs de produits Sophos à traiter, cliquez sur le titre du volet **Erreurs**.

2.4 Icônes d'état de la sécurité

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

Icône d'état de la sécurité	Description
	**Normal** Le nombre d'ordinateurs affectés est en dessous du niveau d'alerte.
	**Alerte** Le niveau d'alerte a été dépassé.
	**Critique** Le niveau critique a été dépassé.

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

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

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

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

L'icône d'état de fonctionnement du réseau

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

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

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

À la première installation ou mise à niveau de l'Enterprise Console, le **Tableau de bord** utilise les niveaux d'alerte et critique par défaut. Retrouvez plus de renseignements sur la configuration de vos propres niveaux d'alerte ou critique à la section Volets du tableau de bord (page 4).

Vous pouvez aussi configurer l'envoi des alertes par courriel aux destinataires de votre choix lorsqu'un niveau d'alerte ou critique a été dépassé pour un volet du **Tableau de bord**. Retrouvez plus d'instructions à la section Configuration des alertes par email sur l'état du réseau (page 197).

2.5 Navigation dans la vue Terminaux

Liste des ordinateurs

Dans la vue **Terminaux**, la liste des ordinateurs affiche les terminaux du groupe sélectionné dans le volet **Groupes**.

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

Vous pouvez filtrer la liste des ordinateurs à l'aide du filtre **Vue**. Dans la liste déroulante **Vue**, sélectionnez les ordinateurs que vous voulez voir. Par exemple, sélectionnez **Ordinateurs avec problèmes éventuels** pour afficher les ordinateurs ayant des problèmes.

Vous pouvez également filtrer la liste des ordinateurs en fonction du nom d'un élément détecté tel qu'un programme malveillant, une application potentiellement indésirable ou un fichier suspect.

Retrouvez plus de renseignements à la section Filtrage des ordinateurs en fonction du nom d'un élément détecté (page 9).

Vous pouvez rechercher les ordinateurs par leurs noms, leurs descriptions ou leurs adresses IP. Retrouvez plus de renseignements à la section Recherche d'un ordinateur dans l'Enterprise Console (page 9).

Retrouvez plus d'explications concernant les icônes affichées dans la liste des ordinateurs à la section Icônes de la liste des ordinateurs (page 7).

Vous pouvez copier ou imprimer les données affichées dans la liste des ordinateurs. Retrouvez plus de renseignements aux sections Copie de données depuis la liste des ordinateurs (page 224) et Impression de données depuis la liste des ordinateurs (page 224).

Volet Groupes

Dans le volet **Groupes**, créez des groupes

et placez-y les ordinateurs en réseau. Vous pouvez créer des groupes vous-même ou importer des conteneurs Active Directory, avec ou sans ordinateurs, et les utiliser comme groupes d'ordinateurs de l'Enterprise Console.

Retrouvez plus de renseignements à la section Création et utilisation de groupes (page 24).

Le groupe **Non affectés**

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

Volet Stratégies

Dans le volet **Stratégies**, vous créez et configurez les stratégies appliquées aux groupes d'ordinateurs. Retrouvez plus de renseignements à la section Création et utilisation de stratégies (page 27).

2.6 Icônes de la liste des ordinateurs

Alertes

Icône	Explication
	L'apparition d'un signal d'avertissement rouge dans la colonne **Alertes et erreurs** de l'onglet **État** signifie qu'un virus, un ver, un cheval de Troie, un spyware ou un comportement suspect a été détecté.

Icône	Explication
	L'apparition d'un signal d'avertissement jaune dans la colonne **Alertes et erreurs** de l'onglet **État** indique l'un des problèmes suivants : • Un fichier suspect a été détecté. • Un adware ou toute autre application potentiellement indésirable a été détecté. • Une erreur s'est produite. L'apparition d'un signal d'avertissement jaune dans la colonne **Conforme à la stratégie** indique que l'ordinateur n'utilise pas la même stratégie ou les mêmes stratégies que les autres ordinateurs de son groupe.

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

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

Si plusieurs alertes ayant la même priorité sont signalées sur le même ordinateur, l'alerte la plus récente est affichée dans la liste des ordinateurs.

Protection désactivée ou non à jour

Une icône de fonction grisée dans la colonne d'état de la fonction dans l'onglet **État** signifie que la fonction est désactivée. Par exemple, un bouclier gris

dans la colonne **Sur accès** signifie que le contrôle sur accès est inactif.

L'icône d'une horloge

dans la colonne **À jour** signifie que le logiciel de sécurité n'est plus à jour.

État de l'ordinateur

Icône	Explication
	Un ordinateur surmonté d'un connecteur vert signifie que l'ordinateur est administré par Enterprise Console.
	Un ordinateur surmonté d'un sablier jaune signifie que l'installation des logiciels de sécurité est en attente.
	Un ordinateur surmonté d'une flèche jaune vers le bas signifie que l'installation des logiciels de sécurité est en cours.

Icône	Explication
	Un symbole avec un ordinateur gris signifie que l'ordinateur n'est pas administré par Enterprise Console.
	Un ordinateur surmonté d'une croix rouge signifie que cet ordinateur qui est généralement administré par Enterprise Console est déconnecté du réseau (les ordinateurs non connectés et non administrés ne sont pas affichés).

2.7 Filtrage des ordinateurs en fonction du nom d'un élément détecté

Vous pouvez filtrer la liste des ordinateurs en fonction du nom d'un élément détecté tel qu'un programme malveillant, une application potentiellement indésirable ou un fichier suspect. Pour cela, vous devez configurer le filtre « Ordinateurs administrés affectés par... ». Le filtre s'affiche dans la liste déroulante **Vue** avec les autres filtres de la liste des ordinateurs.

Pour configurer le filtre :

1. Dans le menu **Outils**, cliquez sur **Configurer les filtres**.
2. Dans la boîte de dialogue **Configuration du filtre de la liste des ordinateurs**, saisissez le nom de l'élément détecté que vous souhaitez filtrer. Vous pouvez retrouver les noms des éléments détectés sur votre réseau dans :
   - La vue de la liste des ordinateurs, l'onglet **Détails des alertes et des erreurs** et dans la colonne **Élément détecté**.

     Veuillez noter que si plusieurs éléments sont détectés sur un ordinateur, la colonne **Élément détecté** affiche uniquement l'élément ayant la priorité la plus élevée qui ne correspondra peut être pas à celui que vous recherchez à l'aide du filtre.
   - La boîte de dialogue **Résolution des alertes et des erreurs**. Pour ouvrir la boîte de dialogue, sélectionnez un ou plusieurs ordinateurs dans la liste des ordinateurs ou un groupe d'ordinateurs dans le volet **Groupes**, cliquez avec le bouton droit de la souris et cliquez sur **Résoudre les alertes et les erreurs**.
   - La boîte de dialogue **Détails de l'ordinateur**. Pour ouvrir la boîte de dialogue, cliquez deux fois sur l'ordinateur affecté. Puis, défilez jusqu'à la section **Alertes et erreurs à traiter**.
   - Les **Rapports** (par exemple, **Récapitulatif des alertes** ou **Alertes et événements par nom d'élément**). Pour ouvrir le **Gestionnaire des rapports**, dans le menu **Outils**, cliquez sur **Gérer les rapports**.

   Vous pouvez utilisez les caractères de remplacement. Utilisez ? pour remplacer un seul caractère du nom et * pour remplacer une chaîne de caractères quelconque. Par exemple, si vous saisissez « Mal*l » et appliquez le filtre, la vue de la liste des ordinateurs affiche les ordinateurs infectés par le programme malveillant dont le nom commence par « Mal » comme « Mal/Conficker-Al » et « Mal/Packerl ».

2.8 Recherche d'un ordinateur dans l'Enterprise Console

Vous pouvez rechercher un ou plusieurs ordinateurs dans Enterprise Console par :

- Nom
- Description
- Adresse IP

1. Pour rechercher un ordinateur, procédez de l'une des manières suivantes :
   - Appuyez sur CTRL+F.
   - Dans le menu **Édition**, cliquez sur **Rechercher un ordinateur**.
   - Cliquez n'importe où dans la liste des ordinateurs, puis cliquez sur **Rechercher un ordinateur**.
2. Dans la boîte de dialogue **Rechercher**, saisissez vos critères de recherche.

   Le champ **Rechercher** n'est pas sensible aux majuscules. Les caractères joker de fin sont implicites.

   Vous pouvez utiliser les caractères de remplacement * et ?

   Par exemple :

Critères de recherche	Résultats de la recherche
UKlapt	Recherche toute chaîne de caractères commençant par « uklapt », par exemple, UKlaptop-011, UKlaptop-155, uklaptop132.
Ukla*	Recherche toute chaîne de caractères commençant par « ukla ». Le caractère joker n'est pas nécessaire car il y est de manière implicite ; la recherche renvoie les mêmes résultats que dans l'exemple précédent, UKlaptop-011, UKlaptop-155, uklaptop132.
***ukla**	Recherche toute chaîne de caractères contenant « ukla », par exemple, UKlaptop-011, 055uklax, 056-Dukla-sales.
Ukl*t	Recherche toute chaîne de caractères commençant par « ukl », contenant un « t » et se terminant par n'importe quel caractère, par exemple UKlaptop-011, ukLite55.
?klap	Recherche toute chaîne de caractères commençant par n'importe quel caractère unique suivi de « klap » et se terminant par n'importe quel caractère, par exemple, UKlaptop-011, uklapland33.
UKl??t	Recherche toute chaîne de caractères commençant par « ukl », suivie de deux caractères, suivi d'un « t » et se terminant par n'importe quel caractère, par exemple, UKlaptop-011, uklist101.

2.9 Navigation dans la vue Gestionnaires de mise à jour

Liste des ordinateurs

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

La liste des ordinateurs affiche les ordinateurs sur lesquels Sophos Update Manager est installé.

Abonnements logiciels

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

3 Démarrage avec Sophos Enterprise Console

Retrouvez ici un aperçu des tâches à effectuer pour protéger votre réseau suite à l'installation de Enterprise Console et après avoir effectué toutes les étapes de l'**Assistant de téléchargement des logiciels de sécurité**. Retrouvez plus de renseignements sur l'utilisation de Enterprise Console dans les documents et sections mentionnés.

Nous vous conseillons de consulter le *Guide de configuration des stratégies de Sophos Enterprise Console* pour obtenir des conseils pratiques en matière d'utilisation et d'administration des logiciels de sécurité Sophos. La documentation Sophos est disponible sur http://www.sophos.com/fr-fr/support/documentation.

Si vous n'avez pas effectué toutes les étapes de l'**Assistant de téléchargement des logiciels de sécurité**, veuillez consulter la section Exécution de l'Assistant de téléchargement des logiciels de sécurité (page 69).

Pour protéger votre réseau, suivez les étapes suivantes :

1. **Création de groupes.**

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

   Retrouvez plus de renseignements sur l'importation de conteneurs Active Directory à la section Importation de conteneurs et d'ordinateurs depuis Active Directory (page 34). Nous vous conseillons de commencer par importer des conteneurs à partir d'Active Directory sans ordinateurs, puis d'assigner des stratégies de groupe aux groupes, et enfin d'ajouter des ordinateurs aux groupes, par exemple, en synchronisant les groupes avec Active Directory.

   Retrouvez plus de renseignements sur la création manuelle de groupes à la section Création et utilisation de groupes (page 24).
2. **Configuration des stratégies.**

   Enterprise Console dispose d'une série de stratégies par défaut essentielles au maintien de la protection du réseau. Les stratégies de **Mise à jour** et les stratégies **Antivirus et HIPS** sont prêtes à l'emploi. Pour configurer la stratégie de pare-feu, lancez l'assistant de **Stratégie de pare-feu**. Retrouvez plus de renseignements à la section Configuration d'une stratégie de pare-feu (page 115).
3. **Détection des ordinateurs sur le réseau et ajout à la console.**

   Si vous avez importé des conteneurs et des ordinateurs depuis Active Directory à l'étape 1, aucune autre opération n'est nécessaire. Autrement, veuillez consulter la section Détection des ordinateurs sur le réseau (page 34).
4. **Protection des ordinateurs.**

   Vous pouvez choisir entre deux approches pour protéger vos ordinateurs en réseau, en fonction de ce qui vous convient le mieux.

   - **Utilisation de l'Assistant de protection des ordinateurs**

     Lorsque vous faites glisser un ordinateur depuis le groupe **Non assigné** et le déposez dans un autre groupe, un assistant se lance pour vous aider à protéger les ordinateurs. Retrouvez plus de renseignements à la section Protection automatique des ordinateurs (page 46).
   - **Protection automatique des ordinateurs lors de la synchronisation avec Active Directory**

Si vous avez choisi de synchroniser avec Active Directory, vous pouvez aussi choisir de protéger automatiquement vos ordinateurs Windows. Vous pouvez exécuter cette opération dans l'**Assistant de synchronisation avec Active Directory** ou dans la boîte de dialogue **Propriétés de synchronisation**. Retrouvez plus d'instructions à la section Utilisation de la synchronisation pour protéger les ordinateurs automatiquement (page 42).

5. **Vérification de la protection des ordinateurs.**

   Une fois l'installation terminée, consultez de nouveau la liste des ordinateurs dans le nouveau groupe. Dans la colonne **Sur accès**, vous devriez voir apparaître le mot *Actif* qui indique que l'ordinateur est protégé par le contrôle sur accès et qu'il est désormais administré par Enterprise Console. Retrouvez plus de renseignements à la section Vérification de la protection de votre réseau (page 48).

6. **Nettoyage des ordinateurs.**

   En cas de détection d'un virus, d'une application indésirable ou de tout autre problème sur votre réseau, procédez au nettoyage des ordinateurs affectés comme le décrit la section Nettoyage immédiat des ordinateurs (page 55).

Options de protection supplémentaires

Par défaut Sophos Endpoint Security and Control détecte les programmes malveillants (virus, chevaux de Troie, vers et spywares), les adwares et autres applications potentiellement indésirables, les comportements suspects et le trafic réseau malveillant. Il bloque également l'accès aux sites Web connus pour héberger des programmes malveillants et contrôle le contenu téléchargé à partir d'Internet. Vous pouvez activer d'autres fonctions de sécurité et de productivité comme indiqué à la section Création et utilisation de groupes (page 24).

Options administratives

Vous pouvez paramétrer différents *rôles* dans Enterprise Console, ajouter des droits aux rôles, puis assigner des utilisateurs Windows et des groupes aux rôles. Le rôle de l'administrateur système qui inclut le groupe Windows « Sophos Full Administrators » dispose des droits complets et ne nécessite aucun paramétrage. Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Vous pouvez diviser votre parc informatique en *sous-parcs* et assigner des groupes d'ordinateurs Enterprise Console à ces sous-parcs. Vous pouvez ensuite contrôler l'accès aux sous-parcs en leur assignant des utilisateurs et des groupes Windows. Le sous-parc **par défaut** contient tous les groupes Enterprise Console et le dossier **Non assigné**. Retrouvez plus de renseignements sur les sous-parcs à la section Gestion des rôles et des sous-parcs (page 14).

Conseil
Consultez les vidéos vous indiquant comment configurer et utiliser Enterprise Console sur la chaîne YouTube SophosGlobalSupport à la section Sophos Enduser Protection.

4 Paramétrage de l’Enterprise Console

4.1 Gestion des rôles et des sous-parcs

Important
Si vous avez déjà utilisé l’administration déléguée, vous devez disposer du droit **Administration déléguée** pour configurer les rôles et les sous-parcs. Le rôle de l’administrateur système qui inclut le groupe Windows « Sophos Full Administrators » dispose des droits complets et ne nécessite aucun paramétrage. Retrouvez plus de renseignements aux sections Que sont les rôles préconfigurés ? (page 15) et Quelles tâches les droits autorisent-ils ? (page 18).

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

Pour ouvrir l’Enterprise Console, un utilisateur doit être membre du groupe Sophos Console Administrators et être assigné au moins à un rôle Enterprise Console et à un sous-parc. Les membres du groupe Sophos Full Administrators ont un accès complet à l’Enterprise Console.

Remarque
Retrouvez plus de renseignements sur l’autorisation d’un utilisateur à se servir d’une Enterprise Console à distance ou supplémentaire à la section Comment un autre utilisateur peut-il utiliser l’Enterprise Console ? (page 23)

Vous pouvez créer vos propres rôles ou utiliser des rôles préconfigurés.

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

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

Vous pouvez aussi restreindre les ordinateurs et les groupes sur lesquels les utilisateurs peuvent effectuer des opérations. Vous pouvez diviser votre parc informatique en sous-parcs et assigner des groupes d’ordinateurs Enterprise Console à ces sous-parcs. Vous pouvez ensuite contrôler l’accès aux sous-parcs en leur assignant des utilisateurs et des groupes Windows. Le sous-parc **par défaut** contient tous les groupes Enterprise Console et le dossier **Non assignés**.

Un utilisateur peut seulement voir le sous-parc auquel il est assigné. Si un utilisateur a été assigné à plus d’un sous-parc, il peut choisir quel sous-parc visualiser, un à la fois. Le sous-parc ouvert dans l’Enterprise Console est le *sous-parc actif*. Un utilisateur ne peut pas modifier une stratégie appliquée hors de son sous-parc actif.

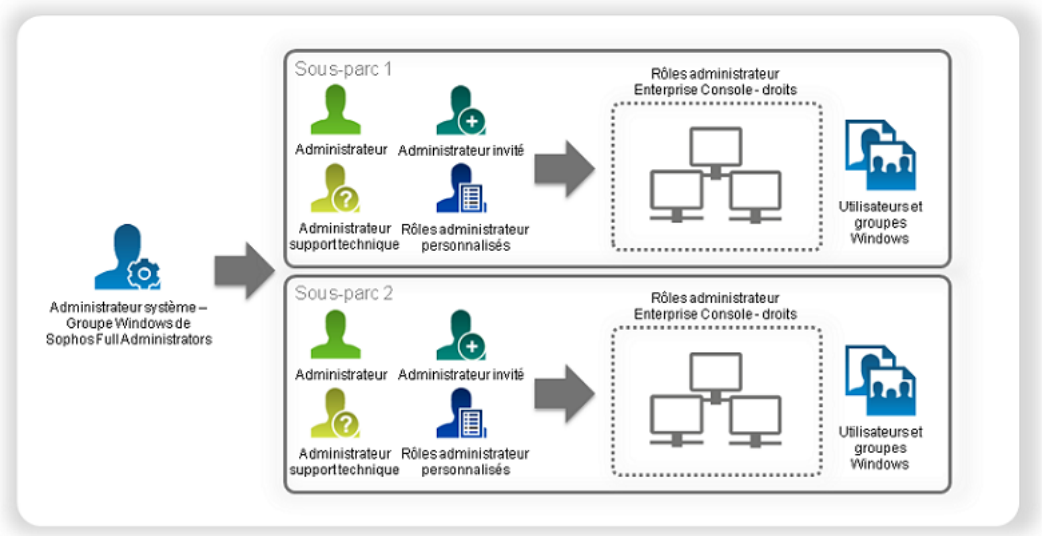


Illustration 1 : Rôles et sous-parcs

4.1.1 Que sont les rôles préconfigurés ?

Il existe quatre rôles préconfigurés dans l'Enterprise Console :

Rôle	Description
Administrateur système	Rôle préconfiguré disposant des droits complets d'administration des logiciels de sécurité Sophos sur le réseau et des rôles dans l'Enterprise Console. Le rôle Administrateur système ne peut pas être modifié ou supprimé.
Administrateur	Rôle préconfiguré disposant des droits d'administration des logiciels de sécurité Sophos sur le réseau mais ne pouvant pas administrer les rôles dans l'Enterprise Console. Le rôle Administrateur peut être renommé, modifié ou supprimé.
Service d'assistance	Rôle préconfiguré disposant uniquement des droits d'actualisation, par exemple, pour nettoyer ou mettre à jour les ordinateurs. Le rôle Service d'assistance peut être renommé, modifié ou supprimé.
Invité	Rôle préconfiguré avec un accès en lecture seule à l'Enterprise Console. Le rôle Invité peut être renommé, modifié ou supprimé.

Vous pouvez modifier les rôles Administrateur, Service d'assistance et Invité, ou créer vos propres rôles comme indiqué à la section Création d'un rôle (page 15).

4.1.2 Création d'un rôle

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Administration déléguée** pour réaliser cette tâche. Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

1. Dans le menu **Outils**, cliquez sur **Gérer les rôles et les sous-parcs**.

2. Dans la boîte de dialogue **Gestion des rôles et des sous-parcs**, dans l'onglet **Gestion des rôles**, cliquez sur **Créer**.
   La boîte de dialogue **Création de rôle** apparaît.
3. Dans le champ **Nom du rôle**, saisissez un nom de rôle.
4. Dans le volet **Droits**, sélectionnez le ou les droits que vous voulez attribuer au rôle et cliquez sur **Ajouter**.
5. Dans le volet **Utilisateurs et groupes**, cliquez sur **Ajouter**.
6. Dans la boîte de dialogue **Sélection d'un utilisateur ou d'un groupe**, saisissez le nom d'un utilisateur ou d'un groupe Windows que vous voulez attribuer au rôle. Cliquez sur **OK**.

   Si nécessaire, attribuez plus d'utilisateurs ou de groupes au rôle, comme le décrivent les étapes 5 et 6.

4.1.3 Suppression d'un rôle

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Administration déléguée** pour réaliser cette tâche. Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

1. Dans le menu **Outils**, cliquez sur **Gérer les rôles et les sous-parcs**.
2. Dans la boîte de dialogue **Gestion des rôles et des sous-parcs**, sur l'onglet **Gestion des rôles**, sélectionnez le rôle que vous voulez supprimer et cliquez sur **Supprimer**.

Remarque
Le rôle Administrateur système préconfiguré ne peut pas être supprimé.

4.1.4 Modification d'un rôle

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Administration déléguée** pour réaliser cette tâche. Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

1. Dans le menu **Outils**, cliquez sur **Gérer les rôles et les sous-parcs**.
2. Dans la boîte de dialogue **Gestion des rôles et des sous-parcs**, dans l'onglet **Gestion des rôles**, sélectionnez le rôle que vous voulez modifier et cliquez sur **Modifier**.
   La boîte de dialogue **Modification du rôle** apparaît.
3. Dans le volet **Droits**, attribuez les droits au rôle ou supprimez les droits existants selon le cas.
4. Dans le volet **Utilisateurs et groupes**, ajoutez les utilisateurs ou les groupes Windows au rôle ou supprimez les utilisateurs ou les groupes existants selon le cas.

4.1.5 Attribution de droits à un rôle

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Administration déléguée** pour réaliser cette tâche. Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

1. Dans le menu **Outils**, cliquez sur **Gérer les rôles et les sous-parcs**.
2. Dans la boîte de dialogue **Gestion des rôles et des sous-parcs**, sur l'onglet **Gestion des rôles**, sélectionnez le rôle auquel vous voulez ajouter un droit et cliquez sur **Modifier**.
   La boîte de dialogue **Modification du rôle** apparaît.

3. Dans le volet **Droits**, dans la liste **Droits disponibles**, sélectionnez un droit et cliquez sur **Ajouter**.

4.1.6 Création d'un sous-parc

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Administration déléguée** pour réaliser cette tâche. Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

1. Dans le menu **Outils**, cliquez sur **Gérer les rôles et les sous-parcs**.
2. Dans la boîte de dialogue **Gestion des rôles et des sous-parcs**, sur l'onglet **Gestion des sous-parcs**, cliquez sur **Créer**.
   La boîte de dialogue **Création d'un sous-parc** apparaît.
3. Dans le champ **Nom du sous-parc**, saisissez un nom de sous-parc.
4. Dans le groupe **Groupes Enterprise Console**, sélectionnez les groupes que vous voulez ajouter au sous-parc.
5. Dans le volet **Utilisateurs et groupes**, cliquez sur **Ajouter** pour ajouter des utilisateurs et des groupes Windows au sous-parc.

4.1.7 Changement du sous-parc actif

Si vous avez été assigné à plus d'un sous-parc, vous pouvez choisir celui que vous voulez consulter lors de l'ouverture de l'Enterprise Console. Vous pouvez aussi basculer entre les sous-parcs dans l'Enterprise Console.

Vous pouvez seulement voir un sous-parc à la fois. Lorsque vous changez votre sous-parc actif, l'Enterprise Console est actualisée avec un nouveau sous-parc.

Pour changer de sous-parc actif :

1. Dans le menu **Outils**, sélectionnez **Sélectionner un sous-parc actif**.
2. Dans la boîte de dialogue **Sélection du sous-parc actif**, sélectionnez le sous-parc que vous voulez ouvrir et cliquez sur **OK**.

4.1.8 Modification d'un sous-parc

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Administration déléguée** pour réaliser cette tâche. Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

1. Dans le menu **Outils**, cliquez sur **Gérer les rôles et les sous-parcs**.
2. Dans la boîte de dialogue **Gestion des rôles et des sous-parcs**, dans l'onglet **Gestion des sous-parcs**, sélectionnez le sous-parc que vous voulez modifier et cliquez sur **Modifier**.
3. Dans la boîte de dialogue **Modification d'un sous-parc**, changez le nom du sous-parc, changez les groupes Enterprise Console inclus dans le sous-parc ou changez les utilisateurs et groupes qui ont accès au sous-parc, selon le cas. Cliquez sur **OK**.

4.1.9 Copie d'un sous-parc

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Administration déléguée** pour réaliser cette tâche. Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

1. Dans le menu **Outils**, cliquez sur **Gérer les rôles et les sous-parcs**.
2. Dans la boîte de dialogue **Gestion des rôles et des sous-parcs**, dans l'onglet **Gestion des sous-parcs**, sélectionnez le sous-parc que vous voulez copier et cliquez sur **Copier**.
   Une copie du sous-parc apparaît dans la liste des sous-parcs.
3. Sélectionnez le sous-parc nouvellement créé et cliquez sur **Modifier**. Renommez le sous-parc. Changez les groupes qui sont inclus dans le sous-parc et/ou les utilisateurs et les groupes Windows qui y ont accès, si vous le souhaitez.

4.1.10 Suppression d'un sous-parc

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Administration déléguée** pour réaliser cette tâche. Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

1. Dans le menu **Outils**, cliquez sur **Gérer les rôles et les sous-parcs**.
2. Dans la boîte de dialogue **Gestion des rôles et des sous-parcs**, sur l'onglet **Gestion des sous-parcs**, sélectionnez le sous-parc que vous voulez supprimer et cliquez sur **Modifier**.

   Vous ne pouvez pas supprimer le sous-parc **par défaut**.

4.1.11 Affichage des rôles d'utilisateur ou de groupe et des sous-parcs

Pour voir les rôles et les sous-parcs auxquels un utilisateur ou un groupe Windows a été attribué :

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

4.1.12 Quelles tâches les droits autorisent-ils ?

Remarque
Selon votre licence, il se peut que certains droits ne s'appliquent pas.

Droit	Tâches
Audit	Activer l'audit, désactiver l'audit

Droit	Tâches
Recherche d’ordinateurs, protection et groupes	Démarrer la recherche, arrêter la recherche et découvrir des domaines pour la recherche sur réseau, rechercher par plage d’adresses IP et rechercher avec Active Directory Importer des ordinateurs et des groupes à partir d’Active Directory ; importer des groupes à partir d’Active Directory Importer des ordinateurs depuis un fichier Supprimer un ordinateur Protéger un ordinateur Synchroniser un groupe avec Active Directory Changer les propriétés de synchronisation des groupes Supprimer la synchronisation des groupes Déplacer un ordinateur Créer un groupe Renommer un groupe Déplacer un groupe Supprimer un groupe Assigner une stratégie à un groupe
Personnaliser le contrôle des données	Créer une règle de contrôle des données Modifier une règle de contrôle des données Copier une règle de contrôle des données Supprimer une règle de contrôle des données Exclure des fichiers du contrôle des données Créer une liste de contrôle du contenu Modifier une liste de contrôle du contenu Copier une liste de contrôle du contenu Supprimer une liste de contrôle du contenu
Événements de contrôle des données	Afficher l’observateur d’événements du contrôle des données Afficher les événements du contrôle des données dans les détails de l’ordinateur

Droit	Tâches
Paramétrage de la stratégie - antivirus et HIPS	Créer une stratégie antivirus et HIPS Dupliquer une stratégie antivirus et HIPS Renommer une stratégie antivirus et HIPS Modifier une stratégie antivirus et HIPS Rétablir les paramètres antivirus et HIPS par défaut Supprimer une stratégie antivirus et HIPS Ajouter ou supprimer une entrée de la liste principale des menaces
Paramétrage de la stratégie - contrôle des applications	Créer une stratégie de contrôle des applications Dupliquer une stratégie de contrôle des applications Renommer une stratégie de contrôle des applications Modifier une stratégie de contrôle des applications Rétablir les paramètres de contrôle des applications par défaut Supprimer une stratégie de contrôle des applications
Paramétrage de la stratégie - contrôle des données	Créer une stratégie de contrôle des données Dupliquer une stratégie de contrôle des données Renommer une stratégie de contrôle des données Modifier une stratégie de contrôle des données Rétablir les paramètres de contrôle des données par défaut Supprimer une stratégie de contrôle des données
Paramétrage de la stratégie - contrôle des périphériques	Créer une stratégie de contrôle des périphériques Dupliquer une stratégie de contrôle des périphériques Renommer une stratégie de contrôle des périphériques Modifier une stratégie de contrôle des périphériques Rétablir les paramètres de contrôle des périphériques par défaut Supprimer une stratégie de contrôle des périphériques
Paramétrage de la stratégie - pare-feu	Créer une stratégie de pare-feu Dupliquer une stratégie de pare-feu Renommer une stratégie de pare-feu Modifier une stratégie de pare-feu Rétablir les paramètres de pare-feu par défaut Supprimer une stratégie de pare-feu

Droit	Tâches
Paramétrage de la stratégie - correctif	Créer une stratégie de correctif Dupliquer une stratégie de correctif Renommer une stratégie de correctif Modifier une stratégie de correctif Rétablir les paramètres de correctif par défaut Supprimer une stratégie de correctif
Paramétrage de la stratégie - protection antialtération	Créer une stratégie de protection antialtération Dupliquer une stratégie de protection antialtération Renommer une stratégie de protection antialtération Modifier une stratégie de protection antialtération Rétablir les paramètres de protection antialtération par défaut Supprimer une stratégie de protection antialtération
Paramétrage de la stratégie - mise à jour	Créer une stratégie de mise à jour Dupliquer une stratégie de mise à jour Renommer une stratégie de mise à jour Modifier une stratégie de mise à jour Rétablir les paramètres de mise à jour par défaut Supprimer une stratégie de mise à jour Créer un abonnement Modifier un abonnement Renommer un abonnement Dupliquer un abonnement Supprimer un abonnement Configurer les gestionnaires de mise à jour
Paramétrage de la stratégie - contrôle du Web	Créer une stratégie de contrôle du Web Dupliquer une stratégie de contrôle du Web Renommer une stratégie de contrôle du Web Modifier une stratégie de contrôle du Web Réinitialiser une stratégie de contrôle du Web Supprimer une stratégie de contrôle du Web

Droit	Tâches
Paramétrage de la stratégie - Prévention des Exploits	Créer une stratégie de prévention des Exploits Dupliquer une stratégie de prévention des Exploits Renommer une stratégie de prévention des Exploits Modifier une stratégie de prévention des Exploits Ajouter une exclusion de limitation des Exploits Supprimer une exclusion de limitation des Exploits Réinitialiser une stratégie de prévention des Exploits Supprimer une stratégie de prévention des Exploits
Actualisation - nettoyage	Nettoyer les éléments détectés Approuver les alertes Approuver les erreurs
Actualisation - mise à jour et contrôle	Mettre les ordinateurs à jour maintenant Exécuter un contrôle intégral du système d'un ordinateur Mettre les ordinateurs en conformité avec la stratégie de groupe Mettre le gestionnaire de mise à jour en conformité avec la configuration Demander au gestionnaire de mise à jour de se mettre à jour maintenant
Configuration du rapport	Créer, modifier ou supprimer un rapport
Administration déléguée	Créer un rôle Renommer un rôle Supprimer un rôle Modifier les droits d'un rôle Ajouter un utilisateur ou un groupe à un rôle Supprimer un utilisateur ou un groupe depuis un rôle Gestion des sous-parcs : créer un sous-parc ; renommer un sous-parc ; supprimer un sous-parc ; ajouter un groupe racine de sous-parc ; supprimer un groupe racine de sous-parc ; ajouter un utilisateur ou un groupe à un sous-parc ; supprimer un utilisateur ou un groupe d'un sous-parc

Droit	Tâches
Configuration du système	Modifier les paramètres du serveur SMTP ; tester les paramètres du serveur SMTP ; modifier les destinataires des alertes par email Configurer les niveaux d'alerte et critique du tableau de bord Configurer les rapports : configurer la purge des alertes de la base de données ; définir le nom de l'entreprise affiché dans les rapports Configurer les rapports envoyés à Sophos : activer ou désactiver l'envoi de rapports à Sophos ; modifier le nom d'utilisateur ; modifier l'adresse électronique du contact Configurer l'utilisation de packages du logiciel de la version fixe
Événements Web	Afficher l'observateur d'événements Web Afficher les événements Web dans la boîte de dialogue des détails de l'ordinateur

4.1.13 Comment un autre utilisateur peut-il utiliser l'Enterprise Console ?

Les membres du groupe Sophos Full Administrators ont un accès complet à l'Enterprise Console.

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

- Membre du groupe Sophos Console Administrators.
- Assigné à au moins un rôle Enterprise Console.
- Assigné à au moins un sous-parc Enterprise Console.

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

Pour assigner un utilisateur à un rôle ou à un sous-parc Enterprise Console, dans le menu **Outils**, cliquez sur **Gérer les rôles et les sous-parcs**. Retrouvez plus de renseignements sur les rôles et les sous-parcs à la section Gestion des rôles et des sous-parcs (page 14).

Pour utiliser une Enterprise Console distante ou supplémentaire, un utilisateur doit être :

- Membre du groupe Sophos Console Administrators sur le serveur sur lequel le serveur d'administration de l'Enterprise Console est installé.
- Membre du groupe Distributed COM Users sur le serveur sur lequel le serveur d'administration de l'Enterprise Console est installé. (le groupe Distributed COM Users est placé dans le conteneur Builtin de l'outil Utilisateurs et ordinateurs Active Directory).
- Assigné à au moins un rôle Enterprise Console.
- Assigné à au moins un sous-parc Enterprise Console.

4.2 Création et utilisation de groupes

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

4.2.1 À quoi servent les groupes ?

Grâce aux groupes, vous pouvez :

- Mettre à jour les ordinateurs présents dans différents groupes depuis des sources différentes ou selon des planifications différentes.
- Utiliser différentes stratégies antivirus et HIPS, de contrôle des applications, de pare-feu et d'autres stratégies pour différents groupes.
- Administrer les ordinateurs plus facilement.

Conseil
Vous pouvez créer des groupes à l'intérieur de groupes et appliquer un ensemble de règles spécifiques à chaque groupe et sous-groupe.

4.2.2 Qu'est-ce qu'un groupe ?

Un groupe

est un dossier contenant un certain nombre d'ordinateurs.

Vous pouvez créer des groupes vous-même ou importer des conteneurs Active Directory, avec ou sans ordinateurs, et les utiliser comme groupes d'ordinateurs dans l'Enterprise Console. Vous pouvez aussi paramétrer la synchronisation avec Active Directory afin que les nouveaux ordinateurs et conteneurs ainsi que d'autres changements dans Active Directory soient copiés automatiquement dans l'Enterprise Console.

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

Un groupe peut contenir des sous-groupes.

4.2.3 Qu'est-ce que le groupe Non assigné ?

Le groupe **Non assigné** est un groupe dans lequel l'Enterprise Console conserve les ordinateurs avant de les placer dans des groupes.

Vous ne pouvez pas :

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

4.2.4 Création d’un groupe

Si vous utilisez l’administration déléguée, vous devez disposer du droit **Recherche d’ordinateurs, protection et groupes** pour réaliser cette tâche. Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Pour créer un groupe pour les ordinateurs :

1. Dans la vue **Terminaux**, dans le volet **Groupes** (sur le côté gauche de la console), sélectionnez l’endroit où vous souhaitez créer le groupe.

   Cliquez sur le nom de l’ordinateur en haut de la liste si vous souhaitez créer un nouveau groupe principal. Cliquez sur un groupe déjà existant si vous souhaitez créer un sous-groupe.
2. Dans la barre d’outils, cliquez sur l’icône **Créer un groupe**.
   Un « Nouveau groupe » est ajouté à la liste et son nom est mis en surbrillance.
3. Saisissez un nouveau nom pour le groupe.

Les stratégies de mise à jour, antivirus et HIPS, de contrôle des applications, de pare-feu, de correctif, de contrôle des données, de contrôle des périphériques, de protection antialtération et de contrôle du Web sont automatiquement appliquées au nouveau groupe. Vous pouvez modifier ces stratégies ou en appliquer des différentes. Retrouvez plus de renseignements à la section Modification d’une stratégie (page 32) ou Assignation d’une stratégie à un groupe (page 32).

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

4.2.5 Ajout d’ordinateurs dans un groupe

Si vous utilisez l’administration déléguée, vous devez disposer du droit **Recherche d’ordinateurs, protection et groupes** pour réaliser cette tâche. Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

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

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

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

4.2.6 Suppression d’ordinateurs d’un groupe

Si vous utilisez l’administration déléguée, vous devez disposer du droit **Recherche d’ordinateurs, protection et groupes** pour réaliser cette tâche. Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

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

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

Si vous avez procédé à la mise à niveau à partir d'une version antérieure de Enterprise Console et avez des ordinateurs chiffrés avec l'ancienne fonction de chiffrement intégral du disque administrée dans Enterprise Console, ne supprimez pas ces ordinateurs de la console. La récupération du chiffrement ne pourra pas être effectuée en cas de suppression.

Pour supprimer des ordinateurs :

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

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

4.2.7 Opération de couper-coller d'un groupe

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Recherche d'ordinateurs, protection et groupes** pour réaliser cette tâche. Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

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

4.2.8 Suppression d'un groupe

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Recherche d'ordinateurs, protection et groupes** pour réaliser cette tâche. Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

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

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

4.2.9 Changement de nom d'un groupe

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Recherche d'ordinateurs, protection et groupes** pour réaliser cette tâche. Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

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

4.2.10 Vérification des stratégies utilisées par un groupe

Pour voir quelles stratégies ont été assignées à un groupe :

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

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

4.3 Création et utilisation de stratégies

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

Lorsque vous installez l'Enterprise Console, des stratégies par défaut offrant un niveau de sécurité basique sont créées pour vous. Ces stratégies s'appliquent à tous les groupes que vous créez. Vous pouvez modifier les stratégies par défaut ou créer de nouvelles stratégies.

Remarque
Certaines fonctions seront indisponibles si elles ne font pas partie de votre contrat de licence.

Vous pouvez créer plusieurs stratégies pour chaque type.

Vous pouvez appliquer la même stratégie à plusieurs groupes.

4.3.1 Quelles stratégies sont disponibles ?

Remarque
Certaines fonctions seront indisponibles si elles ne font pas partie de votre contrat de licence.

- La stratégie de **Mise à jour** définit la manière dont les ordinateurs sont mis à jour avec le nouveau logiciel de sécurité.
- La stratégie **Antivirus et HIPS** définit la manière dont le logiciel de sécurité effectue le contrôle des ordinateurs à la recherche de virus, chevaux de Troie, vers, spywares, adwares, applications potentiellement indésirables, comportements et fichiers suspects et la manière dont il les nettoie.
- La stratégie de **Contrôle des applications** définit quelles applications sont bloquées et autorisées sur vos ordinateurs.
- La stratégie de **Pare-feu** définit la manière dont le pare-feu assure la protection des ordinateurs.
- La stratégie de **Contrôle des données** spécifie les règles pour la surveillance ou la restriction du transfert des fichiers, d'après le contenu du fichier, le nom de fichier ou le type de fichier.
- La stratégie de **Contrôle des périphériques** spécifie les périphériques de stockage et de réseau qui ne sont pas autorisés d'utilisation sur les stations de travail.
- La stratégie de **Correctif** spécifie si l'évaluation des correctifs est activée et la fréquence d'évaluation des correctifs manquants sur les ordinateurs.
- La stratégie de **Protection antialtération** définit le mot de passe permettant aux utilisateurs autorisés de reconfigurer, désactiver ou désinstaller les logiciels de sécurité Sophos.

- La stratégie de **Contrôle du Web** spécifie quels sites Web peuvent être visités par les utilisateurs. Une notification apparaît à l'utilisateur pour les sites qui sont configurés comme « bloquer » ou « avertir ».
- La stratégie de **Prévention des Exploits** spécifie les applications, fonctions et processus protégés contre les attaques d'exploitation. Il peut, par exemple, s'agir de la protection de fichiers document contre les ransomwares (CryptoGuard) ou de la protection de fonctions critiques des navigateurs Web (Safe Browsing).

4.3.2 Quelles sont les stratégies par défaut ?

Lorsque vous installez l'Enterprise Console, des stratégies par défaut sont créées.

Remarque
Certaines fonctions seront indisponibles si elles ne font pas partie de votre contrat de licence.

Stratégie de mise à jour

La stratégie de mise à jour par défaut disponible suite à une nouvelle installation de l'Enterprise Console offre :

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

Stratégie antivirus et HIPS

La stratégie antivirus et HIPS par défaut disponible suite à une nouvelle installation de l'Enterprise Console offre :

- Le contrôle sur accès des virus, chevaux de Troie, vers, spywares, adwares et autres applications potentiellement indésirables (mais pas des comportements suspects).
- La détection des dépassements de la mémoire tampon, du comportement malveillant et suspect des programmes exécutés sur le système et du trafic réseau malveillant.
- Le blocage de l'accès aux sites Web connus pour héberger des programmes malveillants.
- Le contrôle du contenu téléchargé à partir d'Internet.
- L'affichage d'alertes de sécurité sur le bureau de l'ordinateur affecté et leur ajout au journal des événements.

Retrouvez une liste complète des paramètres par défaut de la stratégie antivirus et HIPS suite à une nouvelle installation de l'Enterprise Console dans l'article 27267 de la base de connaissances.

Stratégie de contrôle des applications

Par défaut, toutes les applications et tous les types d'applications sont autorisés. Le contrôle sur accès des applications que vous pourriez souhaiter contrôler sur votre réseau est désactivé.

Stratégie de pare-feu

Par défaut, Sophos Client Firewall est activé et bloque tout le trafic non indispensable. Avant de l'utiliser sur votre réseau, configurez-le pour autoriser les applications que vous désirez utiliser. Retrouvez plus de renseignements à la section Configuration d'une stratégie de pare-feu (page 115).

Retrouvez une liste complète des paramètres du pare-feu par défaut dans l'article 57757 de la base de connaissances.

Stratégie de contrôle des données

Par défaut, le contrôle des données est désactivé et aucune règle n'est spécifiée pour surveiller ou restreindre le transfert des fichiers sur Internet ou sur les périphériques de stockage.

Stratégie de contrôle des périphériques

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

Stratégie de correctif

Par défaut, l'évaluation des correctifs est désactivée. Pour les nouvelles stratégies de correctif, l'évaluation est activée. Dès que l'évaluation des correctifs est activée, les ordinateurs sont évalués tous les jours afin de détecter tout correctif manquant (sauf si vous avez changé l'intervalle d'évaluation des correctifs).

Stratégie de protection antialtération

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

Stratégie de contrôle du Web

Par défaut, le contrôle du Web est désactivé et les utilisateurs peuvent naviguer sur tous les sites non restreints dans le cadre de la protection Web de l'Enterprise Console. Retrouvez plus de renseignements à la section Protection Web (page 104).

Stratégie de prévention des Exploits

Par défaut, la prévention des Exploits est activée. Retrouvez plus de renseignements à la section Stratégie de prévention des Exploits (page 186).

4.3.3 Dois-je créer mes propres stratégies ?

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

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

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

Remarque
Si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de la stratégie** pour créer ou modifier une stratégie. Par exemple, le droit **Paramétrage de la stratégie - antivirus et HIPS** vous permet de créer ou de modifier une stratégie antivirus et HIPS. Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Stratégie de mise à jour

La stratégie de mise à jour par défaut est paramétrée pour que les terminaux vérifient la présence de mises à jour pour l'abonnement recommandé toutes les 10 minutes depuis le partage UNC de distribution du logiciel par défaut. Pour changer les abonnements, mettre à jour les emplacements et voir d'autres paramètres, configurez les stratégies de mise à jour comme indiqué à la section Configuration de la stratégie de mise à jour (page 70).

Antivirus et HIPS

La stratégie antivirus et HIPS par défaut protège les ordinateurs contre les virus et autres programmes malveillants. Toutefois, pour activer la détection d'autres applications ou comportements indésirables ou suspects, vous pouvez créer de nouvelles stratégies ou changer la stratégie par défaut. Retrouvez plus de renseignements à la section Stratégie antivirus et HIPS (page 81).

Contrôle des applications

Pour définir et bloquer des applications non autorisées, configurez les stratégies de contrôle des applications comme indiqué à la section Stratégie de contrôle des applications (page 147).

Stratégie de pare-feu

Pour autoriser l'accès au réseau aux applications fiables, configurez les stratégies de pare-feu comme indiqué à la section Stratégie de pare-feu (page 115).

Contrôle des données

Par défaut, le contrôle des données est désactivé. Pour limiter les fuites de données, configurez les stratégies de contrôle des données comme indiqué à la section Stratégie de contrôle des données (page 150).

Contrôle des périphériques

Par défaut, le contrôle des périphériques est désactivé. Pour limiter l'utilisation de périphériques autorisés, configurez les stratégies de contrôle des périphériques comme indiqué à la section Stratégie de contrôle des périphériques (page 165).

Correctif

Par défaut, l'évaluation des correctifs est désactivée. Pour les nouvelles stratégies de correctif, l'évaluation est activée. Dès que l'évaluation des correctifs est activée, les ordinateurs sont évalués tous les jours afin de détecter tout correctif manquant (sauf si vous avez changé l'intervalle d'évaluation des correctifs). Pour activer ou désactiver l'évaluation des correctifs ou pour modifier l'intervalle d'évaluation, configurez les stratégies de correctif comme indiqué à la section Stratégie de correctif (page 176).

Protection antialtération

Par défaut, la protection antialtération est désactivée. Pour activer la protection antialtération, configurez les stratégies antialtération comme indiqué à la section Stratégie de protection antialtération (page 173).

Contrôle du Web

Par défaut, le contrôle du Web est désactivé. Retrouvez plus de renseignements sur le contrôle du Web et la configuration des stratégies de contrôle du Web à la section Stratégie de contrôle du Web (page 178).

Prévention des Exploits

Par défaut, la prévention des Exploits est activée. Retrouvez plus de renseignements sur la configuration des stratégies de prévention des Exploits à la section Stratégie de prévention des Exploits (page 186).

4.3.4 Création d'une stratégie

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de la stratégie** pour réaliser cette tâche. Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Pour créer une stratégie :

1. Dans la vue **Terminaux**, dans le volet **Stratégies**, cliquez avec le bouton droit de la souris sur le type de stratégie que vous désirez créer, par exemple “Mise à jour” et sélectionnez **Créer une stratégie**.
   Une « Nouvelle stratégie » est ajoutée à la liste et son nom est mis en surbrillance.
2. Saisissez un nouveau nom pour cette stratégie.
3. Cliquez deux fois sur la nouvelle stratégie. Saisissez les paramètres de votre choix.

   Retrouvez plus d’instructions sur la manière de choisir les paramètres à la section sur la configuration de la stratégie appropriée.

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

4.3.5 Assignation d’une stratégie à un groupe

Si vous utilisez l’administration déléguée, vous devez disposer du droit **Recherche d’ordinateurs, protection et groupes** pour réaliser cette tâche. Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

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

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

4.3.6 Modification d’une stratégie

Si vous utilisez l’administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie** approprié pour réaliser cette tâche.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

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

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

Retrouvez plus de renseignements sur la manière de configurer différentes stratégies aux sections respectives.

4.3.7 Attribution d’un nouveau nom à une stratégie

Si vous utilisez l’administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie** approprié pour réaliser cette tâche.
- Vous ne pouvez pas renommer une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Remarque
il est impossible de renommer une stratégie “Par défaut”.

Pour renommer une stratégie :

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

4.3.8 Suppression d’une stratégie

Si vous utilisez l’administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie** approprié pour réaliser cette tâche.
- Vous ne pouvez pas supprimer une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Remarque
il est impossible de supprimer une stratégie “Par défaut”.

Pour supprimer une stratégie :

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

4.3.9 Affichage des groupes utilisant une stratégie

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

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

  Une liste des groupes qui utilisent la stratégie apparaît.

4.3.10 Vérification de l’utilisation de la stratégie de groupe par les ordinateurs

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

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

Retrouvez plus de renseignements sur l'état des fonctions de sécurité sur l'ordinateur et des stratégies appliquées à l'ordinateur sur l'onglet respectif dans la vue **Terminaux**, par exemple, l'onglet **Détails de l'antivirus**.

Retrouvez plus de renseignements sur la mise en conformité de vos ordinateurs à leurs stratégies de groupe à la section Application de la stratégie de groupe par les ordinateurs (page 34).

4.3.11 Application de la stratégie de groupe par les ordinateurs

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Actualisation - mise à jour et contrôle** pour effectuer cette tâche. Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

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

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

4.4 Détection des ordinateurs sur le réseau

Pour administrer les ordinateurs dans l'Enterprise Console, veuillez d'abord les ajouter dans l'Enterprise Console. Vous pouvez utiliser la fonction de détection des ordinateurs et choisir parmi les différentes options qui vous permettent de retrouver les ordinateurs en réseau et de les ajouter dans l'Enterprise Console. Retrouvez les différentes options ci-dessous :

- Importation de conteneurs et d'ordinateurs depuis Active Directory (page 34)
- Détection des ordinateurs avec Active Directory (page 35)
- Détection des ordinateurs sur le réseau (page 36)
- Détection des ordinateurs par plage IP (page 36)
- Importation d'ordinateurs depuis un fichier (page 37)

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Recherche d'ordinateurs, protection et groupes** pour ajouter des ordinateurs dans la console. Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

4.4.1 Importation de conteneurs et d'ordinateurs depuis Active Directory

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Recherche d'ordinateurs, protection et groupes** pour réaliser cette tâche. Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

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

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

Pour importer des groupes depuis Active Directory :

1. Dans la barre d’outils, cliquez sur l’icône **Détecter des ordinateurs**.
2. Dans la boîte de dialogue **Détection des ordinateurs**, dans le volet **Importation depuis Active Directory**, sélectionnez **Importer** et cliquez sur **OK**.

   Sinon, sélectionnez un groupe dans lequel vous voulez importer votre ou vos conteneurs Active Directory, cliquez avec le bouton droit de la souris et sélectionnez **Importer depuis Active Directory**.

   L’**Assistant d’importation depuis Active Directory** démarre.
3. Suivez les instructions de l’assistant. Lorsqu’on vous demande de choisir ce que vous voulez importer, sélectionnez **Ordinateurs et conteneurs** ou **Conteneurs uniquement**, en fonction de ce que vous voulez importer.

Dès que vous avez importé les conteneurs depuis Active Directory, appliquez les stratégies aux groupes. Retrouvez plus de renseignements à la section Quelles stratégies sont disponibles ? (page 27).

Dès que vous avez appliqué les stratégies de groupe aux groupes, vous avez la possibilité de synchroniser les groupes avec Active Directory. Retrouvez plus d’instructions à la section Synchronisation avec Active Directory (page 37).

4.4.2 Détection des ordinateurs avec Active Directory

Si vous utilisez l’administration déléguée, vous devez disposer du droit **Recherche d’ordinateurs, protection et groupes** pour réaliser cette tâche. Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

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

1. Dans la barre d’outils, cliquez sur l’icône **Détecter des ordinateurs**.
2. Dans la boîte de dialogue **Détection des ordinateurs**, sélectionnez **Détecter avec Active Directory** et cliquez sur **OK**.
3. Vous êtes invité à saisir un nom utilisateur et un mot de passe. Ceci est indispensable si vous avez des ordinateurs (par exemple, Windows XP Service Pack 2) dont l’accès est impossible sans les détails d’un compte.

   Le compte doit être un compte d’administrateur de domaine ou disposer des pleins droits administratifs sur les ordinateurs XP cibles.

   Si vous utilisez un compte de domaine, vous *devez* saisir le nom d’utilisateur au format domaine \utilisateur.
4. Dans la boîte de dialogue **Détection des ordinateurs**, sélectionnez les domaines dans lesquels vous souhaitez effectuer la recherche. Cliquez sur **OK**.
5. Cliquez sur le groupe **Non affectés** pour visualiser les ordinateurs qui ont été trouvés.

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

4.4.3 Détection des ordinateurs sur le réseau

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Recherche d'ordinateurs, protection et groupes** pour réaliser cette tâche. Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

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

1. Dans la barre d'outils, cliquez sur l'icône **Détecter des ordinateurs**.
2. Dans la boîte de dialogue **Détection des ordinateurs**, sélectionnez **Détecter sur le réseau** et cliquez sur **OK**.
3. Dans la boîte de dialogue **Codes d'accès**, saisissez le nom utilisateur et le mot de passe d'un compte qui dispose des droits suffisants pour récupérer les informations relatives à l'ordinateur.

   Le compte doit être un compte d'administrateur de domaine ou disposer des pleins droits administratifs sur les ordinateurs cibles. Si vous utilisez un compte de domaine, vous *devez* saisir le nom d'utilisateur au format domaine\utilisateur.

   Vous pouvez ignorer cette étape si vos ordinateurs cibles sont accessibles sans les détails d'un compte.
4. Dans la boîte de dialogue **Détection des ordinateurs**, sélectionnez les domaines ou groupes de travail dans lesquels vous souhaitez rechercher. Cliquez sur **OK**.
5. Cliquez sur le groupe **Non affectés** pour visualiser les ordinateurs qui ont été trouvés.

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

4.4.4 Détection des ordinateurs par plage IP

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Recherche d'ordinateurs, protection et groupes** pour réaliser cette tâche. Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

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

Remarque
vous ne pouvez pas utiliser les adresses IPV6.

1. Dans la barre d'outils, cliquez sur l'icône **Détecter des ordinateurs**.
2. Dans la boîte de dialogue **Détection des ordinateurs**, sélectionnez **Détecter par plage IP** et cliquez sur **OK**.
3. Dans la boîte de dialogue **Codes d'accès**, vous êtes invité à saisir un nom utilisateur et un mot de passe. Ceci est indispensable si vous avez des ordinateurs (par exemple, Windows XP Service Pack 2) dont l'accès est impossible sans les détails d'un compte.

   Le compte doit être un compte d'administrateur de domaine ou disposer des pleins droits administratifs sur les machines XP cibles.

   Si vous utilisez un compte de domaine, vous *devez* saisir le nom d'utilisateur au format domaine \utilisateur.

   Dans le volet **SNMP**, saisissez le nom de la communauté SNMP.
4. Dans la boîte de dialogue **Détection des ordinateurs**, saisissez le **Début de plage IP** et la **Fin de plage IP**. Cliquez sur **OK**.

5. Cliquez sur le groupe **Non affectés** pour visualiser les ordinateurs qui ont été trouvés.

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

4.4.5 Importation d'ordinateurs depuis un fichier

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Recherche d'ordinateurs, protection et groupes** pour réaliser cette tâche. Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Pour que l'Enterprise Console puisse répertorier vos ordinateurs, vous pouvez importer les noms des ordinateurs depuis un fichier. Vous pouvez créer le fichier en utilisant des entrées semblables à celles-ci :

```
[NomGroupe1]
 Domaine1|Windows7|NomOrdinateur1
 Domaine1|Windows2008ServerR2|NomOrdinateur2
```

Remarque
Il n'est pas nécessaire d'indiquer dans quel groupe seront placés les ordinateurs. Si vous saisissez `[]` (sans espace entre les crochets) pour le nom du groupe, les ordinateurs seront placés dans le groupe **Non assignés**.

les noms des systèmes d'exploitation valides sont : WindowsXP, Windows2003, WindowsVista, Windows7, WindowsServer2008, Windows2008ServerR2, Windows8, WindowsServer2012, Windows81, WindowsServer2012R2, Windows10, WindowsServer2016, MACOSX, Linux et Unix.

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

```
[NomGroupe1]
 NomOrdinateur1
```

Importez les noms des ordinateurs comme suit :

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

4.5 Synchronisation avec Active Directory

Cette section donne un aperçu de la synchronisation avec Active Directory.

Que m'apporte la synchronisation avec Active Directory ?

Grâce à la synchronisation avec Active Directory, vous pouvez synchroniser les groupes Enterprise Console avec les conteneurs Active Directory. Les nouveaux ordinateurs et conteneurs trouvés dans Active Directory sont copiés automatiquement dans l'Enterprise Console. Vous pouvez aussi choisir de protéger automatiquement les postes de travail Windows trouvés. De cette manière, vous

réduisez au minimum le temps au cours duquel vos ordinateurs pourraient être infectés ainsi que le temps de travail que vous consacrez à l'organisation et à la protection des ordinateurs.

Remarque
Les ordinateurs exécutant des systèmes d'exploitation serveur Windows, Mac OS, Linux ou UNIX ne sont pas protégés automatiquement. Protégez ces ordinateurs manuellement.

Suite à la configuration de la synchronisation, vous pouvez configurer l'envoi des alertes par email aux destinataires de votre choix pour les informer de la découverte de nouveaux ordinateurs et conteneurs au cours des prochaines synchronisations. Si vous optez pour une protection automatique des ordinateurs dans les groupes synchronisés de l'Enterprise Console, vous pouvez aussi définir l'envoi d'alertes informant des échecs de la protection automatique.

Comment fonctionne la synchronisation avec Active Directory ?

Dans l'Enterprise Console, vous pouvez avoir des groupes « normaux » et non synchronisés que vous administrez vous-même ainsi que des groupes synchronisés avec Active Directory.

Lors de la configuration de la synchronisation, vous sélectionnez ou créez un point de synchronisation, un groupe Enterprise Console à synchroniser avec un conteneur Active Directory. Tous les ordinateurs et sous-groupes contenus dans Active Directory sont copiés dans l'Enterprise Console et maintenus synchronisés avec Active Directory.

Remarque
Retrouvez plus de renseignements sur les points de synchronisation à la section Qu'est-ce qu'un point de synchronisation ? (page 39) et sur les groupes synchronisés à la section Qu'est-ce qu'un groupe synchronisé ? (page 39)

Suite à la configuration de la synchronisation avec Active Directory, la partie synchronisée de la structure du groupe Enterprise Console correspond exactement au conteneur Active Directory avec lequel elle est synchronisée. C'est-à-dire :

- Si un nouvel ordinateur est ajouté au conteneur Active Directory, il apparaît également dans l'Enterprise Console.
- Si un ordinateur est supprimé d'Active Directory ou déplacé dans un conteneur non synchronisé, alors cet ordinateur est aussi déplacé dans le groupe **Non assignés** dans l'Enterprise Console.

  Remarque
  Lorsqu'un ordinateur est déplacé dans le groupe **Non affectés**, il ne reçoit plus les nouvelles stratégies.

- Si un ordinateur est déplacé d'un conteneur synchronisé vers un autre, alors cet ordinateur est aussi déplacé d'un groupe Enterprise Console vers un autre.
- Si un ordinateur existe déjà dans un groupe Enterprise Console lorsqu'il est synchronisé pour la première fois, alors il est aussi déplacé de ce groupe vers le groupe synchronisé qui correspond à son emplacement dans Active Directory.
- Lorsqu'un ordinateur est déplacé dans un nouveau groupe avec des stratégies différentes, alors les nouvelles stratégies sont envoyées à cet ordinateur.

Par défaut, la synchronisation a lieu toutes les 60 minutes. Vous pouvez modifier l'intervalle de synchronisation si cela est nécessaire.

Comment planifier la synchronisation ?

Vous décidez des groupes à synchroniser avec Active Directory et du nombre de points de synchronisation à configurer. Considérez si la taille des groupes qui vont être créés est gérable. Vous devez être en mesure de pouvoir facilement déployer les logiciels et de contrôler et nettoyer les ordinateurs. Ceci est tout particulièrement important lors du déploiement initial.

Remarque
Si vous avez une structure Active Directory complexe et souhaitez synchroniser des groupes locaux de domaine ou des groupes Active Directory imbriqués, veuillez activer cette fonctionnalité conformément aux instructions de l'article 122529 de la base de connaissances.

La manœuvre recommandée est la suivante :

1. Importez la structure du groupe (sans les ordinateurs) en utilisant la fonction **Importation depuis Active Directory**. Retrouvez plus d'instructions à la section Importation de conteneurs et d'ordinateurs depuis Active Directory (page 34).
2. Vérifiez la structure du groupe importé et choisissez vos points de synchronisation.
3. Configurez les stratégies de groupe et appliquez-les aux groupes et aux sous-groupes. Retrouvez plus d'instructions aux sections Création d'une stratégie (page 31) et Assignation d'une stratégie à un groupe (page 32).
4. Synchronisez les points de synchronisation de votre choix, (l'un après l'autre) avec Active Directory. Retrouvez plus d'instructions à la section Synchronisation avec Active Directory (page 40).

4.5.1 Qu'est-ce qu'un point de synchronisation ?

Un *point de synchronisation* est un groupe Enterprise Console qui dirige vers un conteneur (ou une sous-arborescence) dans Active Directory. Un point de synchronisation peut contenir des groupes synchronisés importés depuis Active Directory.

Dans le volet **Groupes**, un point de synchronisation apparaît comme suit :

Vous *pouvez* déplacer, renommer ou supprimer un point de synchronisation. Vous pouvez aussi modifier les paramètres des stratégies et de la synchronisation, y compris les paramètres de la protection automatique, pour un point de synchronisation.

Vous ne *pouvez pas* créer ou supprimer de sous-groupes dans un point de synchronisation ou y déplacer d'autres groupes. Vous ne pouvez pas déplacer des ordinateurs dans ou depuis le point de synchronisation.

4.5.2 Qu'est-ce qu'un groupe synchronisé ?

Un *groupe synchronisé* est un sous-groupe d'un point de synchronisation importé depuis Active Directory.

Dans le volet **Groupes**, un groupe synchronisé apparaît comme suit :

Vous *pouvez* modifier les stratégies affectées à un groupe synchronisé.

Vous ne *pouvez pas* modifier d'autres paramètres d'un groupe synchronisé que ceux qui concernent les stratégies de groupe. Vous ne pouvez pas, renommer, déplacer ou supprimer un groupe synchronisé. Vous ne pouvez pas déplacer des ordinateurs ou des groupes dans ou depuis le groupe. Vous ne pouvez pas créer ou supprimer de sous-groupes dans le groupe. Vous ne pouvez pas modifier les paramètres de synchronisation du groupe.

4.5.3 Synchronisation avec Active Directory

Avant d'exécuter cette tâche :

- Si vous utilisez l'administration déléguée, vous devez disposer du droit **Recherche d'ordinateurs, protection et groupes**. Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).
- Si vous voulez protéger automatiquement les ordinateurs dans les groupes synchronisés, assurez-vous d'avoir préparé les ordinateurs comme indiqué à la section Préparation de l'installation du logiciel de sécurité (page 45).
- Si vous avez une structure Active Directory complexe et souhaitez synchroniser des groupes locaux de domaine ou des groupes Active Directory imbriqués, veuillez activer cette fonctionnalité conformément aux instructions de l'article 122529 de la base de connaissances.

Pour synchroniser avec Active Directory :

1. Sélectionnez un groupe qui va devenir votre point de synchronisation, cliquez avec le bouton droit de la souris et sélectionnez **Synchroniser avec Active Directory**.
   L'assistant de **Synchronisation avec Active Directory** se lance.
2. Sur la page **Aperçu** de l'assistant, cliquez sur **Suivant**.
3. Sur la page **Sélection du groupe Enterprise Console**, sélectionnez ou créez un groupe Enterprise Console dont vous souhaitez qu'il reste synchronisé avec Active Directory (point de synchronisation). Cliquez sur **Suivant**.
4. Sur la page **Sélection d'un conteneur Active Directory**, sélectionnez un conteneur Active Directory que vous souhaitez synchroniser avec le groupe. Saisissez le nom du conteneur, par exemple, LDAP://CN=Ordinateurs,DC=nom_domaine,DC=local ou cliquez sur **Parcourir** pour naviguer jusqu'au conteneur dans Active Directory. Cliquez sur **Suivant**.

   Important
   Si le même ordinateur est présent dans plusieurs conteneurs Active Directory synchronisés, ceci entraîne un problème d'échange continuel de messages entre cet ordinateur et Enterprise Console. Chaque ordinateur doit uniquement être répertorié une fois dans Enterprise Console.

5. Si vous désirez assurer la protection automatique des postes de travail Windows, sur la page **Protection automatique des ordinateurs**, sélectionnez la case **Installer automatiquement les logiciels de sécurité Sophos** puis sélectionnez le logiciel que vous souhaitez installer.

   Remarque
   Retrouvez une liste des configurations requises pour les logiciels sur la page des différentes configurations requises du site Web de Sophos (http://www.sophos.com/fr-fr/products/all-system-requirements.aspx).

- Avant d'installer le **Pare-feu** sur les ordinateurs, assurez-vous que vous avez configuré le pare-feu pour autoriser le trafic, les applications et les processus que vous voulez utiliser. Par défaut, le pare-feu est activé et bloque tout le trafic non indispensable. Retrouvez plus de renseignements à la section Stratégie de pare-feu (page 115).
- Laissez la case **Détection des logiciels de sécurité tiers** sélectionnée si vous voulez que le logiciel d'un autre éditeur soit supprimé automatiquement. Retrouvez plus de renseignements sur la suppression de l'outil de mise à jour d'un autre éditeur à la section Suppression du logiciel de sécurité tiers (page 45).

Tous les postes de travail Windows découverts lors de cette synchronisation et de celles à venir seront protégés automatiquement, conformément à leurs stratégies de groupe respectives.

Important
Les ordinateurs exécutant des systèmes d'exploitation serveur Windows, Mac OS, Linux ou UNIX ne seront pas protégés automatiquement. Protégez-les manuellement comme le décrit le *Guide de démarrage avancé de Sophos Enterprise Console*.

Remarque
Vous avez la possibilité d'activer ou de désactiver la protection automatique ultérieurement, dans la boîte de dialogue **Propriétés de synchronisation**. Retrouvez plus d'instructions à la section Affichage et modification des propriétés de synchronisation (page 42).

Cliquez sur **Suivant**.

6. Si vous avez choisi d'assurer la protection automatique de vos ordinateurs, sur la page **Saisie des codes d'accès Active Directory**, saisissez les détails d'un compte administrateur qui sera utilisé pour installer les logiciels sur les ordinateurs. Cliquez sur **Suivant**.
7. Sur la page **Sélection de l'intervalle de synchronisation**, choisissez la fréquence à laquelle vous souhaitez synchroniser le groupe Enterprise Console avec le conteneur Active Directory. La valeur par défaut est 60 minutes.

   Remarque
   Vous avez la possibilité de modifier l'intervalle de synchronisation ultérieurement, dans la boîte de dialogue **Propriétés de synchronisation**. Retrouvez plus d'instructions à la section Affichage et modification des propriétés de synchronisation (page 42).

8. Sur la page **Confirmation de vos choix**, vérifiez les détails saisis et cliquez sur **Suivant** pour continuer.
9. Sur la dernière page de l'assistant apparaissent les détails des groupes et ordinateurs qui ont été synchronisés.

   Vous pouvez aussi définir l'envoi des alertes par email aux destinataires de votre choix pour les informer des nouveaux ordinateurs et groupes découverts au cours des prochaines synchronisations. Si vous avez opté pour une protection automatique des ordinateurs dans les groupes synchronisés, vous pouvez aussi définir l'envoi d'alertes informant des échecs de la protection automatique. Pour ouvrir la boîte de dialogue **Configuration des alertes par email** après avoir cliqué sur **Terminer**, cochez la case se trouvant sur la dernière page de l'assistant. Retrouvez plus d'instructions à la section Configuration des alertes par email pour la synchronisation avec Active Directory (page 198).

   Pour fermer l'assistant, cliquez sur **Terminer**.

4.5.4 Utilisation de la synchronisation pour protéger les ordinateurs automatiquement

Avant d'exécuter cette tâche :

- Si vous utilisez l'administration déléguée, vous devez disposer du droit **Recherche d'ordinateurs, protection et groupes**. Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).
- Assurez-vous d'avoir préparé les ordinateurs pour l'installation automatique du logiciel de sécurité comme indiqué à la section Préparation de l'installation du logiciel de sécurité (page 45).

Les postes de travail Windows peuvent être protégés automatiquement lorsqu'ils sont découverts lors de la synchronisation avec Active Directory.

Important
Les ordinateurs exécutant des systèmes d'exploitation serveur Windows, Mac OS, Linux ou UNIX ne seront pas protégés automatiquement. Protégez-les manuellement comme le décrit le *Guide de démarrage avancé de Sophos Enterprise Console*.

Vous pouvez protéger des ordinateurs dans des groupes synchronisés automatiquement soit lors de la configuration de la synchronisation (section Synchronisation avec Active Directory (page 40)), soit en modifiant ultérieurement les propriétés de synchronisation.

Les instructions ci-dessous vous indiquent comment protéger les ordinateurs en modifiant les propriétés de synchronisation.

1. Dans le volet **Groupes**, sélectionnez le groupe (point de synchronisation) sur lequel vous souhaitez activer la protection automatique. Cliquez avec le bouton droit de la souris sur le groupe et sélectionnez **Propriétés de la synchronisation**.
2. Dans la boîte de dialogue **Propriétés de la synchronisation**, sélectionnez la case **Installer automatiquement les logiciels de sécurité Sophos** puis sélectionnez le logiciel que vous souhaitez installer.
    - Avant d'installer le **Pare-feu** sur les ordinateurs, assurez-vous que vous avez configuré le pare-feu pour autoriser le trafic, les applications et les processus que vous voulez utiliser. Par défaut, le pare-feu est activé et bloque tout le trafic non indispensable. Retrouvez plus de renseignements à la section Stratégie de pare-feu (page 115).
    - Laissez la case **Détection des logiciels de sécurité tiers** sélectionnée si vous voulez que le logiciel d'un autre éditeur soit supprimé automatiquement. Retrouvez plus de renseignements sur la suppression de l'outil de mise à jour d'un autre éditeur à la section Suppression du logiciel de sécurité tiers (page 45).
3. Saisissez le nom utilisateur et le mot de passe d'un compte administrateur qui sera utilisé pour installer les logiciels sur les ordinateurs. Cliquez sur **OK**.

Si vous désirez désactiver la protection automatique ultérieurement, dans la boîte de dialogue **Propriétés de la synchronisation**, dessélectionnez la case **Installer automatiquement les logiciels de sécurité Sophos**.

4.5.5 Affichage et modification des propriétés de synchronisation

Avant d'exécuter cette tâche :

- Si vous utilisez l'administration déléguée, vous devez disposer du droit **Recherche d'ordinateurs, protection et groupes**. Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).
- Si vous voulez protéger automatiquement les ordinateurs dans les groupes synchronisés, assurez-vous d'avoir préparé les ordinateurs comme indiqué à la section Préparation de l'installation du logiciel de sécurité (page 45).
- Si vous avez une structure Active Directory complexe et souhaitez synchroniser des groupes locaux de domaine ou des groupes Active Directory imbriqués, veuillez activer cette fonctionnalité conformément aux instructions de l'article 122529 de la base de connaissances.

Pour consulter et modifier les propriétés de synchronisation :

1. Dans le volet **Groupes**, sélectionnez le groupe (point de synchronisation) sur lequel vous souhaitez modifier les propriétés de synchronisation. Cliquez avec le bouton droit de la souris sur le groupe et sélectionnez **Propriétés de la synchronisation**.
   La boîte de dialogue **Propriétés de la synchronisation** apparaît.
2. Dans le champ **Conteneur Active Directory**, vous pouvez consulter le conteneur avec lequel le groupe est synchronisé. Si vous désirez synchroniser le groupe avec un conteneur différent, supprimez la synchronisation et exécutez de nouveau l'**Assistant de synchronisation avec Active Directory**. Retrouvez plus de renseignements aux sections Activation ou désactivation de la synchronisation (page 44) et Synchronisation avec Active Directory (page 40).
3. Dans le champ **Intervalle de synchronisation**, définissez la fréquence de synchronisation. La valeur par défaut est 60 minutes. La valeur minimum est 5 minutes.
4. Sélectionnez la case **Installer automatiquement les logiciels de sécurité Sophos** si vous souhaitez protéger automatiquement tous les nouveaux postes de travail Windows trouvés, conformément à leurs stratégies de groupe respectives. Sous **Fonctions**, la protection antivirus est sélectionnée par défaut. Si vous souhaitez avoir d'autres logiciels de sécurité installés, sélectionnez les cases à cocher correspondantes. Saisissez le nom utilisateur et le mot de passe d'un compte administrateur qui sera utilisé pour installer les logiciels sur les ordinateurs.

Remarque
seuls les postes de travail Windows peuvent être protégés automatiquement. Les ordinateurs exécutant des systèmes d'exploitation serveur Windows, Mac OS, Linux ou UNIX ne peuvent pas être protégés automatiquement. Protégez-les manuellement comme le décrit le *Guide de démarrage avancé de Sophos Enterprise Console*.

4.5.6 Synchronisation immédiate avec Active Directory

Avant d'exécuter cette tâche :

- Si vous utilisez l'administration déléguée, vous devez disposer du droit **Recherche d'ordinateurs, protection et groupes**. Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).
- Si vous voulez protéger automatiquement les ordinateurs dans les groupes synchronisés, assurez-vous d'avoir préparé les ordinateurs comme indiqué à la section Préparation de l'installation du logiciel de sécurité (page 45).
- Si vous avez une structure Active Directory complexe et souhaitez synchroniser des groupes locaux de domaine ou des groupes Active Directory imbriqués, veuillez activer cette fonctionnalité conformément aux instructions de l'article 122529 de la base de connaissances.

Vous pouvez synchroniser les groupes de l'Enterprise Console (points de synchronisation) avec les conteneurs Active Directory immédiatement, sans attendre la synchronisation planifiée suivante.

Pour synchroniser immédiatement avec Active Directory :

1. Dans le volet **Groupes**, sélectionnez le groupe (point de synchronisation) que vous voulez synchroniser avec Active Directory. Cliquez avec le bouton droit de la souris sur le groupe et sélectionnez **Propriétés de la synchronisation**.
2. Dans la boîte de dialogue **Propriétés de la synchronisation**, effectuez les modifications nécessaires et cliquez sur **OK**.

4.5.7 Activation ou désactivation de la synchronisation

Avant d'exécuter cette tâche :

- Si vous utilisez l'administration déléguée, vous devez disposer du droit **Recherche d'ordinateurs, protection et groupes**. Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).
- Si vous voulez protéger automatiquement les ordinateurs dans les groupes synchronisés, assurez-vous d'avoir préparé les ordinateurs comme indiqué à la section Préparation de l'installation du logiciel de sécurité (page 45).
- Si vous avez une structure Active Directory complexe et souhaitez synchroniser des groupes locaux de domaine ou des groupes Active Directory imbriqués, veuillez activer cette fonctionnalité conformément aux instructions de l'article 122529 de la base de connaissances.

Pour activer ou désactiver la synchronisation avec Active Directory :

- Pour activer la synchronisation, exécutez l'**Assistant de synchronisation avec Active Directory** comme indiqué à la section Synchronisation avec Active Directory (page 40).
- Pour désactiver la synchronisation, sélectionnez le groupe (point de synchronisation) que vous ne souhaitez plus synchroniser avec Active Directory, cliquez avec le bouton droit de la souris et sélectionnez **Supprimer la synchronisation**. Cliquez sur **Oui** pour confirmer.

4.6 Configuration de l'URL de Sophos Mobile

Sophos Mobile est une solution d'administration des appareils mobiles comme les smartphones et les tablettes. Sophos Mobile permet d'assurer la sécurité des données professionnelles en gérant les apps et les paramètres de sécurité.

Vous pouvez ouvrir la console Web Sophos Mobile à partir de l'Enterprise Console en cliquant sur le bouton **Sophos Mobile** de la barre d'outils. Veuillez d'abord configurer l'URL de Sophos Mobile.

1. Dans le menu **Outils**, cliquez sur **Configurer l'URL de Sophos Mobile**.
2. Dans la boîte de dialogue **URL de Sophos Mobile**, saisissez l'URL de la console Web Sophos Mobile Control et cliquez sur **OK**.

5 Protection des ordinateurs

Vous pouvez installer les logiciels de protection Sophos de l'une des manières suivantes :

- Pour protéger les ordinateurs automatiquement, utilisez l'assistant de protection des ordinateurs dans l'Enterprise Console. Retrouvez plus de renseignements à la section Protection automatique des ordinateurs (page 46).
- Autrement, vous pouvez protéger les ordinateurs automatiquement à l'aide de la synchronisation Active Directory. Retrouvez plus de renseignements à la section Synchronisation avec Active Directory (page 37).
- Pour protéger les ordinateurs manuellement, l'Enterprise Console recherche le logiciel le mieux adapté comme indiqué à la section Localisation des programmes d'installation pour la protection manuelle des ordinateurs (page 48). Puis allez sur l'ordinateur respectif et installez manuellement les logiciels de sécurité.

5.1 Préparation de l'installation du logiciel de sécurité

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

Remarque
L'installation automatique n'est pas possible sur les ordinateurs Mac, Linux et UNIX.

Si vous utilisez Active Directory, vous pouvez préparer vos ordinateurs à l'aide d'un Objet de stratégie de groupe (GPO ou Group Policy Object). Si vous utilisez des groupes de travail, configurez les ordinateurs localement.

Retrouvez plus d'instructions dans le *Guide de déploiement de Sophos pour terminaux*. Retrouvez des vidéos sur le déploiement dans l'article 111180 de la base de connaissances.

5.2 Suppression du logiciel de sécurité tiers

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

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

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

Remarque
HitmanPro.Alert sera peut-être déjà installé en tant que produit autonome ou administré à partir de Sophos Central. Veuillez désinstaller HitmanPro.Alert avant d'appliquer l'administration locale à partir de Sophos Enterprise Console.

Si l'outil de mise à jour d'un autre éditeur est installé sur les ordinateurs et si vous souhaitez le supprimer, vous allez devoir modifier le fichier de configuration avant de sélectionner l'option **Third-Party Security Software Detection** dans l'**Assistant de protection des ordinateurs**.

Remarque
si des ordinateurs utilisent le pare-feu ou le produit HIPS d'un autre éditeur, il est possible que vous soyez obligé de laisser intact l'outil de mise à jour de cet éditeur. Retrouvez plus de renseignements dans la documentation de l'éditeur.

Pour modifier le fichier de configuration :

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

Lorsque vous exécutez l'**Assistant de Protection des ordinateurs** et sélectionnez **Third-Party Security Software Detection**, le fichier de configuration modifié supprime alors tout outil de mise à jour tiers ainsi que tout logiciel de sécurité tiers.

5.3 Protection automatique des ordinateurs

Avant de protéger les ordinateurs depuis la console :

- Appliquez la stratégie de mise à jour au groupe avant de pouvoir protéger les ordinateurs dans ce groupe.
- Assurez-vous d'avoir préparé les ordinateurs pour l'installation automatique du logiciel de sécurité comme indiqué à la section Préparation de l'installation du logiciel de sécurité (page 45).
- Si vous utilisez l'administration déléguée, vous devez disposer du droit **Recherche d'ordinateurs, protection et groupes** pour protéger les ordinateurs. Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

L'installation automatique n'est pas possible sur les ordinateurs Mac, Linux et UNIX. Utilisez plutôt l'installation manuelle. Retrouvez plus d'instructions dans le *Guide de démarrage avancé de Sophos Enterprise Console*.

Si vous optez pour la synchronisation avec Active Directory et la protection automatique des ordinateurs, il n'est *pas* nécessaire de suivre les étapes ci-dessous. Retrouvez plus de

renseignements à la section Synchronisation avec Active Directory (page 37) et dans les rubriques associées.

Pour protéger les ordinateurs automatiquement :

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

   L'**Assistant de protection des ordinateurs** est lancé. Suivez les instructions de l'assistant.
2. Sur la page **Sélection des fonctions**, sélectionnez les fonctionnalités que vous désirez.

   Remarque
   Retrouvez une liste des configurations requises pour les fonctions sur la page des différentes configurations requises du site Web de Sophos (http://www.sophos.com/fr-fr/products/all-system-requirements).

   Certaines fonctionnalités, telle la protection antivirus, sont toujours sélectionnées et doivent être installées. Vous pouvez également choisir d'installer les fonctions ci-dessous. Certaines fonctions sont disponibles seulement si votre licence les inclut.

   - **Firewall**

     Avant d'installer le pare-feu sur les ordinateurs, assurez-vous que vous avez configuré le pare-feu pour autoriser le trafic, les applications et les processus que vous voulez utiliser. Par défaut, le pare-feu est activé et bloque tout le trafic non indispensable. Retrouvez plus de renseignements à la section Stratégie de pare-feu (page 115).
   - **Patch**
   - **Exploit Prevention, Sophos Clean**

     Cette fonction assure la protection contre les ransomwares et les exploits. Elle est sélectionnée par défaut si votre licence inclut cette fonction.

     Remarque
     Si vous procédez à la mise à niveau de votre licence pour y inclure la prévention des Exploits (avec Sophos Clean), celle-ci ne sera pas automatiquement installée sur les ordinateurs que vous administrez déjà. Vous devez protéger de nouveau les ordinateurs pour l'installer.

   - **Third-Party Security Software Detection**

     Laissez la case **Third-Party Security Software Detection** sélectionnée si vous voulez que le logiciel d'un autre éditeur soit supprimé automatiquement. La détection des logiciels de sécurité tiers consiste à désinstaller uniquement les produits ayant les mêmes fonctionnalités que ceux que vous installez. Retrouvez plus de renseignements sur la suppression de l'outil de mise à jour d'un autre éditeur à la section Suppression du logiciel de sécurité tiers (page 45).
3. Sur la page **Récapitulatif de la protection**, tout problème rencontré avec l'installation figure dans la colonne **Problèmes de protection**. Résolvez les problèmes relatifs à l'installation (section Échec d'installation de Sophos Endpoint Security and Control (page 228)), ou procédez à l'installation manuelle sur ces ordinateurs (*Guide de démarrage avancé de Sophos Enterprise Console*). Cliquez sur **Suivant**.

4. Sur la page **Codes d'accès**, saisissez les détails d'un compte qui peut être utilisé pour installer le logiciel.

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

   - Posséder les droits d'administrateur local sur les ordinateurs que vous souhaitez protéger.
   - Pouvoir se connecter à l'ordinateur sur lequel vous avez installé le serveur d'administration.
   - Avoir un accès en lecture à l'emplacement Serveur principal spécifié dans la stratégie de **Mise à jour**. Retrouvez plus de renseignements à la section Configuration des serveurs de mise à jour (page 71).

   Remarque
   Si vous utilisez un compte de domaine, vous *devez* saisir le nom utilisateur sous la forme `domaine\utilisateur`.

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

5.4 Localisation des programmes d'installation pour la protection manuelle des ordinateurs

Si l'Enterprise Console ne parvient pas à effectuer l'installation automatique des fonctions antivirus, de pare-feu ou d'évaluation des correctifs sur certains ordinateurs, effectuez l'installation manuellement.

Pour rechercher les programmes d'installation :

1. Dans le menu **Affichage**, cliquez sur **Emplacements des fichiers d'amorce**.
2. Dans la boîte de dialogue **Emplacements des fichiers d'amorce**, pour chaque abonnement logiciels, vous verrez les emplacements contenant les programmes d'installation des logiciels, ainsi que les plates-formes sur lesquelles les logiciels sont pris en charge et leurs versions. Notez l'emplacement du programme d'installation dont vous avez besoin.

Retrouvez plus de renseignements sur l'installation manuelle des logiciels de sécurité sur différents systèmes d'exploitation dans le *Guide de démarrage avancé de Sophos Enterprise Console*.

5.5 Vérification de la protection de votre réseau

Pour avoir un aperçu de l'état de sécurité du réseau, utilisez le Tableau de bord. Retrouvez plus de renseignements aux sections Volets du tableau de bord (page 4) et Configuration du tableau de bord (page 49).

Vous pouvez identifier les ordinateurs à problèmes en utilisant la liste des ordinateurs et les filtres de cette liste. Par exemple, vous pouvez voir les ordinateurs sur lesquels les fonctions de pare-feu ou de correctif ne sont pas installées ou ceux ayant des alertes nécessitant votre attention. Retrouvez plus de renseignements aux sections Vérification de la protection des ordinateurs (page 49), Vérification de l'état de mise à jour des ordinateurs (page 50) et Recherche d'ordinateurs avec problèmes (page 50).

Vous pouvez vérifier si tous les ordinateurs d'un groupe sont conformes aux stratégies de ce groupe comme indiqué à la section Vérification de l'utilisation de la stratégie de groupe par les ordinateurs (page 33).

5.5.1 Configuration du tableau de bord

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Configuration système** pour configurer le Tableau de bord. Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

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

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

1. Dans le menu **Outils**, cliquez sur **Configurer le tableau de bord**.
2. Dans la boîte de dialogue **Configuration du tableau de bord**, changez les valeurs de seuil dans les champs **Niveau d'alerte** et **Niveau critique** comme décrit ci-dessous.

    a) Sous **Ordinateurs avec des alertes à traiter**, **Ordinateurs avec des erreurs de produits Sophos** et **Stratégie et protection**, saisissez un pourcentage d'ordinateurs administrés affectés par un problème particulier et qui déclenchera le passage de l'indicateur respectif de l'état « alerte » à l'état « critique ».

    b) Sous **Ordinateurs avec événements**, saisissez le nombre d'événements ayant eu lieu dans une période de sept jours qui déclenchent une alerte affichée sur le Tableau de bord.

    c) Sous **Dernière protection depuis Sophos**, saisissez l'heure de la dernière mise à jour réussie depuis Sophos qui déclenchera la passage de l'indicateur « Mises à jour » à l'état « alerte » ou « critique ». Cliquez sur **OK**.

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

Vous pouvez aussi configurer l'envoi des alertes par courriel aux destinataires de votre choix lorsqu'un seuil d'alerte ou critique a été dépassé. Retrouvez plus d'instructions à la section Paramétrage des alertes et des messages (page 190).

5.5.2 Vérification de la protection des ordinateurs

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

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

Pour vérifier que les ordinateurs sont protégés :

1. Sélectionnez le groupe d'ordinateurs que vous désirez vérifier.
2. Si vous désirez vérifier les ordinateurs dans les sous-groupes du groupe, sélectionnez **À ce niveau et au-dessous** dans la liste déroulante.
3. Dans la liste des ordinateurs, sur l'onglet **État**, observez la colonne **Sur accès**.
   Si vous voyez « Actif », l'ordinateur exécute le contrôle sur accès. Si vous voyez un bouclier gris, il ne l'exécute pas.
4. Si vous avez installé le pare-feu, observez la colonne **Pare-feu activé**.

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

5. Si vous utilisez d'autres fonctions telles que le contrôle des applications, le contrôle des données ou l'évaluation des correctifs, vérifiez leur état dans la colonne respective.

Retrouvez plus de renseignements sur la procédure de vérification de mise à jour des ordinateurs à la section Vérification de l'état de mise à jour des ordinateurs (page 50).

Retrouvez plus de renseignements sur la recherche des ordinateurs à problèmes à l'aide de filtres de listes d'ordinateurs à la section Recherche d'ordinateurs avec problèmes (page 50).

5.5.3 Vérification de l'état de mise à jour des ordinateurs

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

Pour vérifier que les ordinateurs sont à jour :

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

Retrouvez plus de renseignements sur la mise à jour de ces ordinateurs obsolètes à la section Mise à jour des ordinateurs non à jour (page 80).

5.5.4 Recherche d'ordinateurs avec problèmes

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

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

   Vous pouvez aussi sélectionner une sous-entrée de cette entrée pour afficher les ordinateurs affectés par un problème spécifique (par exemple, les ordinateurs qui diffèrent de la stratégie de groupe ou lorsqu'une erreur sur un produit Sophos a lieu).
3. Si le groupe contient des sous-groupes, sélectionnez également si vous souhaitez rechercher les ordinateurs **À ce niveau seulement** ou **À ce niveau et au-dessous**.
   Tout ordinateur ayant des problèmes de protection sera répertorié.

Vous pouvez également filtrer la liste des ordinateurs en fonction du nom d'un élément détecté tel qu'un programme malveillant, une application potentiellement indésirable ou un fichier suspect. Retrouvez plus de renseignements à la section Filtrage des ordinateurs en fonction du nom d'un élément détecté (page 9).

Retrouvez plus de renseignements sur la gestion des problèmes de protection à la section Les ordinateurs n'utilisent pas le contrôle sur accès (page 226) ainsi que dans les autres rubriques de la section Résolution des problèmes (page 226).

5.6 Traitement des alertes et des erreurs

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

Retrouvez une légende des icônes d'alertes à la section Que signifient les icônes d'alertes ? (page 51) Les autres rubriques de cette section contiennent des conseils sur le traitement des alertes.

Remarque
Des avertissements apparaissent aussi dans la console si le logiciel est désactivé ou non à jour. Retrouvez plus de renseignements à ce sujet à la section Vérification de la protection de votre réseau (page 48).

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

Retrouvez plus de renseignements sur les alertes du gestionnaire de mise à jour à la section Surveillance du gestionnaire de mise à jour (page 78).

5.6.1 Que signifient les icônes d'alertes ?

Icône	Explication
	L'apparition d'un signal d'avertissement rouge dans la colonne **Alertes et erreurs** signifie qu'un virus, un ver, un cheval de Troie, un spyware ou un comportement suspect a été détecté.
	L'apparition d'un signal d'avertissement jaune dans la colonne **Alertes et erreurs** indique l'un des problèmes suivants : • Un fichier suspect a été détecté. • Un adware ou toute autre application potentiellement indésirable a été détecté. • Une erreur s'est produite. L'apparition d'un signal d'avertissement jaune dans la colonne **Conforme à la stratégie** indique que l'ordinateur n'utilise pas la même stratégie ou les mêmes stratégies que les autres ordinateurs de son groupe.

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

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

5.6.2 Traitement des alertes sur les éléments détectés

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Actualisation - nettoyage** pour nettoyer les éléments détectés ou effacer les alertes depuis la console. Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

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

1. Dans la vue **Terminaux**, sélectionnez le ou les ordinateurs dont vous souhaitez voir les alertes. Cliquez avec le bouton droit de la souris et sélectionnez **Résoudre les alertes et les erreurs**. La boîte de dialogue **Résolution des alertes et des erreurs** apparaît.
2. Les mesures que vous pouvez prendre contre une alerte dépendent de l'état du nettoyage de l'alerte. Observez la colonne **État du nettoyage** et décidez des mesures à prendre.

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

État du nettoyage	Description et mesures à prendre
Nettoyable	Vous pouvez supprimer l'élément. Pour cela, sélectionnez l'alerte ou les alertes et cliquez sur **Nettoyage**.
Type de menace non nettoyable	Ce type d'élément détecté, comme par exemple, un fichier suspect, un comportement suspect ou du trafic réseau malveillant, ne peut pas être nettoyé de la console. Vous devez décider si vous voulez autoriser ou bloquer l'élément. Si vous vous méfiez de cet élément, vous pouvez l'envoyer à Sophos pour analyse. Retrouvez plus de renseignements à la section Recherche d'informations sur les éléments détectés (page 53).
Non nettoyable	Cet élément ne peut pas être nettoyé de la console. Retrouvez plus de renseignements sur l'élément et sur les actions que vous pouvez prendre à la section Recherche d'informations sur les éléments détectés (page 53).
Contrôle intégral requis	Cet élément est nettoyable, mais un contrôle intégral du terminal est nécessaire avant que le nettoyage puisse être exécuté. Retrouvez plus d'instructions à la section Contrôle immédiat des ordinateurs (page 54).
Redémarrage requis	L'élément a été partiellement supprimé et le terminal n'a pas besoin d'être redémarré pour terminer le nettoyage. **Remarque** Les terminaux doivent être redémarrés localement et non pas depuis Enterprise Console.
Échec du nettoyage	L'élément n'a pas pu être supprimé. Un nettoyage manuel peut être nécessaire. Retrouvez plus de renseignements à la section Nettoyage immédiat des ordinateurs (page 55).

État du nettoyage	Description et mesures à prendre
Nettoyage en cours (démarré à <heure>)	Le nettoyage est en cours.
Délai d'attente dépassé pour le nettoyage (démarré à <heure>)	Le délai d'attente est dépassé pour le nettoyage. L'élément n'a peut-être pas été nettoyé. Ceci peut se produire, par exemple, lorsque le terminal est déconnecté du réseau ou lorsque le réseau est occupé. Vous pouvez essayer de nettoyer une nouvelle fois l'élément ultérieurement.

Si vous avez décidez d'autoriser un élément, veuillez consulter la section Autorisation des adwares et des PUA (page 111) ou Autorisation d'éléments suspects (page 113).

5.6.3 Recherche d'informations sur les éléments détectés

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

1. Dans la vue **Terminaux**, dans la liste des ordinateurs, cliquez deux fois sur l'ordinateur affecté.
2. Dans la boîte de dialogue **Détails de l'ordinateur**, défilez jusqu'à la section **Alertes et erreurs à traiter**. Dans la liste des éléments détectés, cliquez sur le nom de l'élément qui vous intéresse. Ceci vous connecte directement au site Web de Sophos où vous pouvez lire une description de l'élément et des conseils sur les mesures à prendre.

Remarque
Vous pouvez aussi vous rendre sur la page des **Analyses de sécurité** sur le site Web de Sophos (http://www.sophos.com/fr-fr/threat-center/threat-analyses/viruses-and-spyware.aspx) et sélectionner le type d'élément que vous recherchez, puis saisir le nom de l'élément dans le champ de recherche.

5.6.4 Traitement des alertes de ransomware

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Actualisation - nettoyage** pour nettoyer les éléments détectés ou effacer les alertes depuis la console. Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

CryptoGuard bloque le processus sur le terminal qui a généré l'alerte de ransomware. Le blocage demeure jusqu'à ce que vous confirmiez la réception de l'alerte.

Remarque
Si le terminal est redémarré, le blocage n'a plus lieu. Une nouvelle alerte de ransomware est générée si le processus infecté redémarre.

Mémo
Veuillez exécuter Sophos Clean manuellement sur l'ordinateur déclenchant la détection. En cas contraire, l'ordinateur va déclencher une alerte et le processus sera bloqué à chaque fois qu'il sera exécuté.

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

1. Dans la vue **Terminaux**, sélectionnez le ou les ordinateurs dont vous souhaitez voir les alertes. Cliquez avec le bouton droit de la souris et sélectionnez **Résoudre les alertes et les erreurs**. La boîte de dialogue **Résolution des alertes et des erreurs** apparaît.
2. Sélectionnez les alertes de ransomware que vous souhaitez effacer et cliquez sur **Approuver**. Les alertes approuvées (supprimées) n'apparaissent plus dans la console. Le processus est débloqué.

5.6.5 Effacement des alertes ou des erreurs depuis la console

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Actualisation - nettoyage** pour effacer les alertes ou les erreurs depuis la console. Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

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

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

1. Dans la vue **Terminaux**, sélectionnez le ou les ordinateurs pour lesquels vous souhaitez effacer les alertes. Cliquez avec le bouton droit de la souris et sélectionnez **Résoudre les alertes et les erreurs**.
   La boîte de dialogue **Résolution des alertes et des erreurs** apparaît.
2. Pour effacer les alertes ou les erreurs des produits Sophos depuis la console, allez respectivement sur l'onglet Alertes ou Erreurs, sélectionnez les alertes ou les erreurs que vous voulez effacer et cliquez sur **Approuver**.
   Les alertes approuvées (supprimées) n'apparaissent plus dans la console.

Retrouvez plus de renseignements sur la suppression des alertes du gestionnaire de mise à jour depuis la console à la section Effacement des alertes du gestionnaire de mise à jour depuis la console (page 79).

5.7 Contrôle et nettoyage immédiats des ordinateurs

5.7.1 Contrôle immédiat des ordinateurs

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

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Actualisation - mise à jour et contrôle** pour contrôler les ordinateurs. Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Remarque
seuls les ordinateurs Windows, Linux et UNIX peuvent faire l'objet d'un contrôle intégral du système demandé depuis la console.

Pour contrôler les ordinateurs immédiatement :

1. Sélectionnez les ordinateurs dans la liste des ordinateurs ou un groupe depuis le volet **Groupes**. Cliquez avec le bouton droit de la souris et sélectionnez **Contrôle intégral du système**.

   Autrement, dans le menu **Actions**, sélectionnez **Contrôle intégral du système**.
2. Dans la boîte de dialogue **Contrôle intégral du système**, vérifiez les détails des ordinateurs à contrôler et cliquez sur **OK** pour lancer le contrôle.

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

5.7.2 Nettoyage immédiat des ordinateurs

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

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Actualisation - nettoyage** pour nettoyer les ordinateurs. Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Remarque
pour nettoyer les ordinateurs Linux ou UNIX, vous pouvez soit configurer un nettoyage automatique depuis la console (comme indiqué à la section Paramétrage du nettoyage automatique pour le contrôle sur accès (page 86)), soit nettoyer les ordinateurs individuellement comme indiqué à section Gestion des éléments détectés en cas d'échec du nettoyage (page 56).

Si un élément (par exemple, un cheval de Troie ou une application potentiellement indésirable) a été « partiellement détecté », avant de nettoyer l'ordinateur affecté, exécutez un contrôle intégral de l'ordinateur pour trouver tous les composants de l'élément partiellement détecté. Dans la liste des ordinateurs, dans la vue **Terminaux**, cliquez avec le bouton droit de la souris sur l'ordinateur affecté et cliquez sur **Contrôle intégral du système**. Retrouvez plus de renseignements à la section Élément partiellement détecté (page 230).

Pour nettoyer les ordinateurs immédiatement :

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

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

Si une quelconque alerte demeure répertoriée, procédez à un nettoyage manuel des ordinateurs. Retrouvez plus de renseignements à la section Gestion des éléments détectés en cas d'échec du nettoyage (page 56).

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

5.7.3 Gestion des éléments détectés en cas d'échec du nettoyage

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

1. Dans la liste des ordinateurs, cliquez deux fois sur l'ordinateur infecté.
2. Dans la boîte de dialogue **Détails de l'ordinateur**, défilez jusqu'à la section **Alertes et erreurs à traiter**. Dans la liste des éléments détectés, cliquez sur le nom de l'élément que vous voulez supprimer de l'ordinateur.
   Cette opération vous connecte au site Web de Sophos sur lequel vous pouvez lire des conseils sur le nettoyage de votre ordinateur.
3. Rendez-vous sur l'ordinateur et effectuez le nettoyage manuellement.

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

6 Mise à jour des ordinateurs

6.1 Configuration du gestionnaire de mise à jour

Un gestionnaire de mise à jour vous permet de configurer la mise à jour automatique du logiciel de sécurité Sophos depuis un site Web de Sophos. Un gestionnaire de mise à jour est installé avec et administré depuis l'Enterprise Console.

Vous pouvez installer des gestionnaires de mise à jour supplémentaires. Par exemple, si vous avez un réseau complexe avec plusieurs emplacements, vous pouvez installer un gestionnaire de mise à jour supplémentaire dans un emplacement distant. Retrouvez plus de renseignements à la section Ajout d'un gestionnaire de mise à jour (page 63).

6.1.1 Comment fonctionne un gestionnaire de mise à jour ?

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

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

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

6.1.2 Affichage ou modification de la configuration du gestionnaire de mise à jour

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de la stratégie - mise à jour** pour configurer un gestionnaire de mise à jour. Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

1. Si vous êtes dans la vue **Terminaux**, cliquez sur le bouton **Gestionnaires de mise à jour** sur la barre d'outils pour afficher la vue **Gestionnaires de mise à jour**.
2. Dans la liste des gestionnaires de mise à jour, sélectionnez le gestionnaire de mise à jour dont vous voulez voir ou modifier la configuration. Cliquez avec le bouton droit de la souris, puis cliquez sur **Voir/Modifier la configuration**.

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

   La boîte de dialogue **Configuration du gestionnaire de mise à jour** apparaît.
3. Modifiez la configuration comme le décrivent les sections suivantes :

- Sélection d'une source de mise à jour pour un gestionnaire de mise à jour (page 58).
- Sélection des logiciels à télécharger (page 59).
- Indication de l'emplacement du logiciel (page 60).
- Création ou modification d'une planification des mises à jour (page 61).
- Configuration du journal du gestionnaire de mise à jour (page 62).
- Configuration de la mise à jour automatique d'un gestionnaire de mise à jour (page 62).

Retrouvez plus de renseignements sur la suppression des alertes du gestionnaire de mise à jour depuis la console à la section Effacement des alertes du gestionnaire de mise à jour depuis la console (page 79).

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

6.1.3 Sélection d'une source de mise à jour pour un gestionnaire de mise à jour

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de la stratégie - mise à jour** pour configurer un gestionnaire de mise à jour. Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

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

Vous pouvez sélectionner plusieurs sources. La première source de la liste est la source principale. Les autres sources de la liste sont des emplacements alternatifs et optionnels utilisés par le gestionnaire de mise à jour lorsqu'il n'est pas en mesure de récupérer une mise à jour depuis la source principale.

1. Si vous êtes dans la vue **Terminaux**, cliquez sur le bouton **Gestionnaires de mise à jour** sur la barre d'outils pour afficher la vue **Gestionnaires de mise à jour**.
2. Dans la liste des gestionnaires de mise à jour, sélectionnez le gestionnaire de mise à jour pour lequel vous voulez sélectionner une source de mise à jour. Cliquez avec le bouton droit de la souris, puis cliquez sur **Voir/Modifier la configuration**.
3. Dans la boîte de dialogue **Configuration du gestionnaire de mise à jour**, sur l'onglet **Sources**, cliquez sur **Ajouter**.
4. Dans la boîte de dialogue **Détails de la source**, dans le champ **Adresse**, saisissez l'adresse de la source. L'adresse peut être un chemin UNC ou HTTP.

   Si vous souhaitez télécharger les logiciels et les mises à jour directement depuis Sophos, sélectionnez **Sophos**.
5. Si nécessaire, dans les champs **Nom utilisateur** et **Mot de passe**, saisissez le nom utilisateur et le mot de passe du compte qui sera utilisé pour accéder à la source de mise à jour.
   - Si la source de mise à jour est Sophos, saisissez les codes d'accès de téléchargement fournis par Sophos.
   - Si la source de mise à jour est le partage de mise à jour par défaut créé par un gestionnaire de mise à jour placé plus haut dans la hiérarchie de mise à jour, les champs **Nom d'utilisateur** et **Mot de passe** seront pré-remplis.

     L'emplacement de mise à jour par défaut est un partage UNC `\\<NomOrdinateur>\SophosUpdate`, où NomOrdinateur est le nom de l'ordinateur sur lequel le gestionnaire de mise à jour est installé.

- Si la source de mise à jour est un partage de mise à jour autre que celui par défaut sur votre réseau, saisissez les codes d'accès du compte qui a les droits en lecture du partage. Si le **Nom d'utilisateur** doit être qualifié pour indiquer le domaine, utilisez la forme domaine \nomutilisateur.

6. Si vous accédez à la source de mise à jour via un serveur proxy, sélectionnez **Utiliser un serveur proxy pour se connecter**. Puis saisissez l'**Adresse** et le numéro du **Port** du serveur proxy. Saisissez un **Nom d'utilisateur** et un **Mot de passe** qui donnent accès au serveur proxy. Si le nom d'utilisateur doit être qualifié pour indiquer le domaine, utilisez la forme domaine \nomutilisateur. Cliquez sur OK.
   La nouvelle source apparaît dans la liste de la boîte de dialogue **Configuration du gestionnaire de mise à jour**.

Si vous avez déjà installé un gestionnaire de mise à jour sur un ordinateur différent, le partage sur lequel ce gestionnaire téléchargera les logiciels et les mises à jour apparaîtra dans la liste d'adresses. Vous pouvez le sélectionner en tant que source pour le gestionnaire de mise à jour que vous configurez. Vous pouvez ensuite déplacer l'adresse que vous souhaitez voir apparaître au début de la liste, à l'aide des boutons **Monter** et **Descendre** situés à droite de la liste.

6.1.4 Sélection des logiciels à télécharger

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de la stratégie - mise à jour** pour configurer un gestionnaire de mise à jour. Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

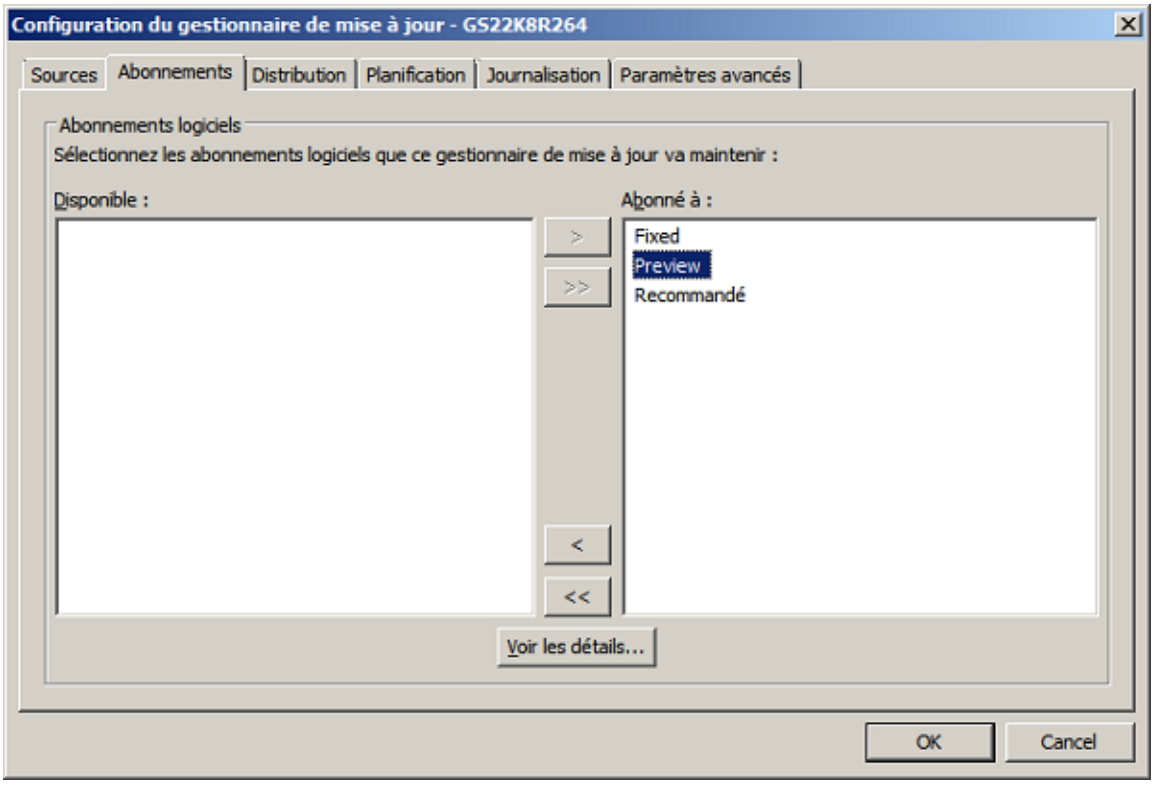
Sélectionnez les abonnements que le gestionnaire de mise à jour va mettre à jour.

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

   Pour déplacer tous les abonnements dans la liste « Abonné à », cliquez sur le bouton « Tout ajouter ».



6.1.5 Indication de l'emplacement du logiciel

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de la stratégie - mise à jour** pour configurer un gestionnaire de mise à jour. Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Après avoir sélectionné les logiciels à télécharger, vous pouvez indiquer à quel endroit du réseau ils doivent être placés. Par défaut, les logiciels sont placés dans un partage UNC `\\<NomOrdinateur>\SophosUpdate`, où NomOrdinateur est le nom de l'ordinateur sur lequel le gestionnaire de mise à jour est installé.

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

Remarque
Vous avez créé le compte d'utilisateur Update Manager avant d'installer l'Enterprise Console. Retrouvez plus de renseignements sur le compte dans la documentation de démarrage de l'Enterprise Console.

Pour déterminer où les logiciels sont placés :

1. Si vous êtes dans la vue **Terminaux**, cliquez sur le bouton **Gestionnaires de mise à jour** sur la barre d'outils pour afficher la vue **Gestionnaires de mise à jour**.
2. Dans la liste des gestionnaires de mise à jour, sélectionnez celui pour lequel vous voulez sélectionner des partages réseau en vue d'une distribution des logiciels. Cliquez avec le bouton droit de la souris, puis cliquez sur **Voir/Modifier la configuration**.

3. Dans la boîte de dialogue **Configuration du gestionnaire de mise à jour**, sur l'onglet **Distribution**, sélectionnez un abonnement logiciels dans la liste.
4. Sélectionnez un partage dans la liste des partages « Disponibles » et déplacez-le dans la liste « Mettre à jour dans » en cliquant sur le bouton « Ajouter » (>).

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

   La liste des partages « Disponibles » inclut tous les partages connus par l'Enterprise Console et qui ne sont pas déjà utilisés par un autre gestionnaire de mise à jour.

   Vous pouvez ajouter un partage existant dans la liste des partages « Disponibles » ou en enlever un à l'aide du bouton « Ajouter » (>) ou « Supprimer » (<).
5. Si vous voulez saisir une description de partage ou les codes d'accès nécessaires pour écrire dans le partage, sélectionnez ce dernier et cliquez sur **Configurer**. Dans la boîte de dialogue **Gestionnaire des partages**, saisissez la description et les codes d'accès.

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

6.1.6 Création ou modification d'une planification des mises à jour

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de la stratégie - mise à jour** pour configurer un gestionnaire de mise à jour. Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

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

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

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

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

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

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

1. Si vous êtes dans la vue **Terminaux**, cliquez sur le bouton **Gestionnaires de mise à jour** sur la barre d'outils pour afficher la vue **Gestionnaires de mise à jour**.
2. Dans la liste des gestionnaires de mise à jour, sélectionnez le gestionnaire de mise à jour pour lequel vous voulez créer une planification des mises à jour. Cliquez avec le bouton droit de la souris, puis cliquez sur **Voir/Modifier la configuration**.

3. Dans la boîte de dialogue **Configuration du gestionnaire de mise à jour**, sur l'onglet **Planification**, saisissez l'intervalle entre les mises à jour des données de détection des menaces.
4. Saisissez l'intervalle entre les mises à jour des logiciels.
   - Si vous voulez spécifier un intervalle de mise à jour qui est utilisé toutes les heures chaque jour, sélectionnez l'option **Vérifier les mises à jour toutes les n minutes** et saisissez l'intervalle en minutes.
   - Si vous voulez créer une planification plus sophistiquée ou des planifications différentes suivant les jours de la semaine, sélectionnez l'option **Configurer et gérer les mises à jour planifiées** et cliquez sur **Ajouter**.

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

6.1.7 Configuration du journal du gestionnaire de mise à jour

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de la stratégie - mise à jour** pour configurer un gestionnaire de mise à jour. Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

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

6.1.8 Configuration de la mise à jour automatique d'un gestionnaire de mise à jour

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de la stratégie - mise à jour** pour configurer un gestionnaire de mise à jour. Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

1. Si vous êtes dans la vue **Terminaux**, cliquez sur le bouton **Gestionnaires de mise à jour** sur la barre d'outils pour afficher la vue **Gestionnaires de mise à jour**.
2. Dans la liste des gestionnaires de mise à jour, sélectionnez le gestionnaire de mise à jour pour lequel vous voulez configurer la mise à jour automatique. Cliquez avec le bouton droit de la souris, puis cliquez sur **Voir/Modifier la configuration**.
3. Dans la boîte de dialogue **Configuration du gestionnaire de mise à jour**, sur l'onglet **Avancés**, sélectionnez une version du gestionnaire de mise à jour avec laquelle vous voulez rester à jour. Par exemple, si vous sélectionnez « Recommended », le gestionnaire de mise à jour sera toujours mis à niveau à la version qui est identifiée comme telle pour Sophos. La version même du gestionnaire de mise à jour changera.

6.1.9 Demande de vérification immédiate des mises à jour au gestionnaire de mise à jour

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Actualisation - mise à jour et contrôle** pour effectuer cette tâche. Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

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

1. Si vous êtes dans la vue **Terminaux**, cliquez sur le bouton **Gestionnaires de mise à jour** sur la barre d'outils pour afficher la vue **Gestionnaires de mise à jour**.
2. Dans la liste des gestionnaires de mise à jour, sélectionnez celui que vous voulez mettre à jour. Cliquez avec le bouton droit de la souris, puis cliquez sur **Mettre à jour maintenant**.

6.1.10 Mise en conformité d'un gestionnaire de mise à jour aux paramètres de configuration

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de la stratégie - mise à jour** pour configurer un gestionnaire de mise à jour. Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

1. Si vous êtes dans la vue **Terminaux**, cliquez sur le bouton **Gestionnaires de mise à jour** sur la barre d'outils pour afficher la vue **Gestionnaires de mise à jour**.
2. Dans la liste des gestionnaires de mise à jour, sélectionnez le gestionnaire de mise à jour que vous voulez mettre en conformité avec les paramètres de configuration. Cliquez avec le bouton droit de la souris, puis cliquez sur **Mettre en conformité avec la configuration**.

6.1.11 Ajout d'un gestionnaire de mise à jour

Sophos Update Manager (SUM) est toujours installé sur l'ordinateur sur lequel vous installez l'Enterprise Console. Si vous avez sélectionné **Configuration personnalisée** lors de l'installation, il s'agit de l'ordinateur sur lequel le serveur d'administration est installé.

Vous pouvez ajouter un ou plusieurs gestionnaires de mise à jour supplémentaires sur votre réseau. Cela aide à réduire la charge sur le gestionnaire de mise à jour qui est déjà installé et à distribuer plus efficacement les mises à jour. Vous pouvez installer un gestionnaire de mise à jour supplémentaire sur un ordinateur sur lequel aucun n'est encore installé.

Important
ne supprimez pas le gestionnaire de mise à jour installé sur le même ordinateur que le serveur d'administration Enterprise Console. L'Enterprise Console ne peut pas entièrement protéger le réseau tant que le gestionnaire de mise à jour n'est pas configuré avec une source de mise à jour. Ceci permet à l'Enterprise Console de recevoir les mises à jour nécessaires (par exemple, les informations sur les versions des logiciels de sécurité que les terminaux devraient utiliser, les nouvelles listes de contrôle du contenu et celles mises à jour pour le contrôle des données ou la liste des nouveaux périphériques et applications contrôlés).

Pour permettre à un gestionnaire de mise à jour supplémentaire de télécharger les logiciels de sécurité depuis Sophos ou d'un autre gestionnaire de mise à jour via HTTP, ouvrez le port TCP 80 (sortant) sur l'ordinateur sur lequel vous voulez installer le gestionnaire de mise à jour supplémentaire. Pour permettre au gestionnaire de mise à jour de télécharger le logiciel de sécurité depuis un autre gestionnaire de mise à jour via un chemin UNC, ouvrez les ports sortants suivants sur l'ordinateur : port UDP 137, port UDP 138, port TCP 139 et port TCP 445.

Si l'ordinateur est en train d'exécuter une version de Windows qui inclut la fonction Découverte du réseau et que cette fonction est désactivée, activez-la et redémarrez l'ordinateur.

Si le Contrôle de compte d'utilisateur est activé sur le serveur, désactivez-le et redémarrez l'ordinateur. Après avoir installé le gestionnaire de mise à jour et vous être abonné aux mises à jour Sophos, vous pouvez réactiver le Contrôle de compte d'utilisateur.

Si l'ordinateur est dans un domaine, ouvrez une session en tant qu'administrateur de domaine.

Si l'ordinateur est dans un groupe de travail, ouvrez une session en tant qu'administrateur local.

Le programme d'installation du gestionnaire de mise à jour est placé sur l'ordinateur sur lequel le serveur d'administration de l'Enterprise Console est installé, dans le dossier partagé `\\Nom serveur\SUMInstallSet`. Pour voir l'emplacement du programme d'installation, choisissez le menu **Affichage** et cliquez sur **Emplacement du programme d'installation de Sophos Update Manager**.

Vous pouvez installer Sophos Update Manager à l'aide du Bureau à distance Windows.

Pour installer un gestionnaire de mise à jour supplémentaire :

1. Exécutez **Setup.exe**, le programme d'installation de Sophos Update Manager.
   Un assistant d'installation se lance.
2. Sur la page de **Bienvenue** de l'assistant, cliquez sur **Suivant**.
3. Sur la page **Contrat de licence**, lisez le contrat de licence et cliquez sur **J'accepte les termes de ce contrat de licence** si vous êtes d'accord avec les termes. Cliquez sur **Suivant**.
4. Sur la page **Dossier de destination**, validez la valeur par défaut ou cliquez sur **Changer** et saisissez un nouveau dossier de destination. Cliquez sur **Suivant**.
5. Sur la page **Compte Sophos Update Manager**, sélectionnez un compte que les terminaux utiliseront pour accéder au partage de mise à jour par défaut créé par le gestionnaire de mise à jour (le partage de mise à jour par défaut est un `\\<NomOrdinateur>\SophosUpdate`, où NomOrdinateur est le nom de l'ordinateur où le gestionnaire de mise à jour est installé). Ce compte doit avoir les droits en lecture du partage et n'a pas besoin d'avoir des droits administrateur.

   Vous pouvez sélectionner l'utilisateur par défaut, sélectionner un utilisateur existant ou en créer un nouveau.

   Par défaut, le programme d'installation crée le compte **SophosUpdateMgr** avec des droits en lecture du partage de mise à jour par défaut et aucun droit de connexion interactif.

   Si vous souhaitez ajouter plus de partages de mise à jour ultérieurement, sélectionnez un compte existant ou créez un nouveau compte qui a les droits en lecture sur ces partages. Autrement, assurez-vous que le compte **SophosUpdateMgr** dispose des droits en lecture sur ces partages.

6. Sur la page **Détails du compte Sophos Update Manager**, selon l'option que vous avez sélectionnée à la page précédente, saisissez un mot de passe pour l'utilisateur par défaut, les détails du nouvel utilisateur ou sélectionnez un compte existant.

   Le mot de passe du compte doit respecter votre politique d'utilisation des mots de passe.
7. Sur la page **Prêt à installer le programme**, cliquez sur **Installer**.
8. Une fois l'installation terminée, cliquez sur **Terminer**.

L'ordinateur sur lequel vous avez installé Sophos Update Manager doit maintenant apparaître dans la vue **Gestionnaires de mise à jour** de l'Enterprise Console (dans le menu **Affichage**, cliquez sur **Gestionnaires de mise à jour**).

Pour configurer le gestionnaire de mise à jour, sélectionnez-le, cliquez avec le bouton droit de la souris, puis cliquez sur **Voir/Modifier la configuration**.

6.1.12 Publication des logiciels de sécurité sur un serveur Web

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

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

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

   a) Dans le menu **Affichage** de Enterprise Console, cliquez sur **Emplacements des fichiers de démarrage**.
   Dans la boîte de dialogue **Emplacements des fichiers d'amorce**, la colonne **Emplacement** affiche le chemin de l'emplacement des fichiers d'amorce pour chaque plate-forme.

   b) Notez le chemin jusqu'au dossier `CID` mais sans l'inclure. Par exemple : `\\`*`nom serveur`*`\SophosUpdate`
2. Mettez l'emplacement des fichiers d'amorce, y compris les sous-dossiers, à disposition sur le serveur Web. Retrouvez plus d'instructions dans l'article 38238 de la base de connaissances Sophos.

6.2 Configuration des abonnements logiciels

Un abonnement logiciels permet de spécifier quelles versions des logiciels pour terminaux sont téléchargées depuis Sophos pour chaque plate-forme.

L'**Assistant de téléchargement des logiciels de sécurité** configure un abonnement par défaut appelé « Recommended ». Cet abonnement inclut les versions recommandées de tous les logiciels sélectionnés.

Si vous voulez ajouter un logiciel à votre abonnement ou vous abonner à une version différente de celle recommandée, configurez l'abonnement comme indiqué à la section Abonnement aux logiciels de sécurité (page 68).

Si vous n'avez pas effectué toutes les tâches de l'Assistant de téléchargement des logiciels de sécurité après avoir installé l'Enterprise Console, veuillez consulter la section Exécution de l'Assistant de téléchargement des logiciels de sécurité (page 69).

6.2.1 Quels types de mise à jour sont disponibles ?

Chaque plate-forme (par exemple, Windows), dispose de plusieurs packages logiciels représentant différents types de mise à jour et contenant différentes versions du logiciel pour terminaux. Vous pouvez choisir la version des logiciels à télécharger depuis Sophos pour un déploiement ultérieur sur les terminaux en sélectionnant l'un des types de mise à jour suivant dans l'abonnement.

Type de mise à jour	Description
Recommended	Il s'agit du package par défaut. Si vous utilisez ce package, Sophos procède régulièrement à la mise à jour de votre logiciel (généralement, tous les mois) avec : • Les corrections des problèmes rencontrés par les clients. • Les nouvelles fonctions disponibles. Si vous installez l'Enterprise Console pour la première fois et acceptez les paramètres par défaut, cette version sera utilisée.
Preview	Ce package est destiné à être utilisé par les administrateurs informatiques et de sécurité. Lorsque vous utilisez cette version, vous recevez les nouvelles fonctions avant qu'elles ne soient mise à disposition dans la version « Recommended ». Vous pouvez donc les tester et les évaluer préférablement sur un réseau de tests avant qu'elles soient mises à disposition sur le marché. **Remarque** Il arrive parfois que le package « Preview » vous propose le même logiciel que le package « Recommended ». Ceci arrive lorsqu'aucune nouvelle fonction n'est prête à être testée sur des environnements clients.
Extended	La version Extended s'adresse aux clients dont les procédures d'installation des logiciels mis à jour sur leur réseau sont strictes ou conventionnelles. Lorsque vous utilisez cette version, vous recevez les mêmes mises à jour que celles de la version « Recommended » mais plusieurs mois après leur mise à disposition. De cette manière, tous les problèmes rencontrés dans le produit ont été identifiés et corrigés bien avant que celui-ci ne soit installé sur votre réseau.
Previous Recommended	Il s'agit d'une version précédente du package « Recommended ». Cette version vous sera particulièrement utile si vous souhaitez disposer de plus de temps pour tester le nouveau logiciel avant de le déployer sur votre réseau.
Previous Extended	Il s'agit d'une version précédente du package « Extended ». Cette version vous sera particulièrement utile si vous souhaitez disposer de plus de temps pour tester le nouveau logiciel avant de le déployer sur votre réseau.

Type de mise à jour	Description
Versions fixes	Retrouvez plus de renseignements à la section Packages du logiciel de la version fixe (page 67).

Remarque
Les packages sont susceptibles d'être modifiés. Retrouvez plus de renseignements sur les packages logiciels actuellement disponible dans l'article 119216 de la base de connaissances Sophos.

L'**Assistant de téléchargement des logiciels de sécurité** configure un abonnement qui spécifie les versions conseillées (« Recommended ») de tous les logiciels sélectionnés.

Les versions actuellement téléchargées changent généralement chaque mois. Pour vérifier les versions du logiciel qui sont téléchargées, ouvrez la boîte de dialogue **Abonnement logiciels** et sélectionnez le package que vous souhaitez vérifier puis cliquez sur **Détails**.

6.2.2 Packages du logiciel de la version fixe

Une **version fixe** est une version mise à jour tous les mois avec les nouvelles données de détection des menaces, mais pas avec la dernière version du logiciel. Un exemple de version fixe de Sophos Endpoint Security and Control pour Windows peut être « 10.3.15 VE3.60.0 ». Le nom de la version est divisée en trois parties : le numéro d'identification de la version principale (10), le numéro d'identification de la version mineure (3), le numéro d'identification de la version de maintenance (15) et enfin le moteur de détection des menaces (VE3.60.0).

Utilisation des packages fixes

Par défaut, l'utilisation des packages du logiciel de la version fixe est désactivé (sous **Outils > Configurer l'utilisation de packages fixes**). Ils ne s'affichent pas dans la boîte de dialogue **Abonnement logiciels** et vous ne pouvez pas vous y abonner.

Conseil
Si vous êtes abonné à une version fixe du logiciel, nous vous conseillons de changer votre abonnement et d'opter pour un package « Recommended » qui vous fera bénéficier de la meilleure protection possible. Retrouvez plus de renseignements sur les packages logiciels à la section Quels types de mise à jour sont disponibles ? (page 66).

Si vous n'avez encore jamais utilisé de packages du logiciel de la version fixe et que vous souhaitez le faire, veuillez activer l'utilisation des packages fixes sous **Outils > Configurer l'utilisation de packages fixes**. Lorsque l'utilisation des packages fixes est activée, ceux-ci sont affichés dans la boîte de dialogue **Abonnement logiciels** et vous pouvez vous y abonner.

Remarque
Si vous utilisez l'administration déléguée, vous devez disposer du droit **Configuration système** pour configurer l'utilisation des packages fixes.

Si vous désactivez l'utilisation des packages fixes alors que vous êtes encore abonné à un package fixe, vous demeurerez abonné à ce package et il continuera à être téléchargé jusqu'à ce que vous

arrêtiez l'abonnement. Toutefois, vous ne serez pas en mesure de voir ou de vous réabonner à un autre package fixe.

Si vous utilisez des consoles à distance, la modification de cette option de configuration sur l'une d'entre elles s'appliquera à toutes les consoles. Si vous avez activé l'utilisation des packages fixes dans le registre conformément aux instructions de l'article 117348 de la base de connaissances Sophos, le paramètre du registre s'appliquera uniquement sur l'ordinateur sur lequel il a été configuré et remplacera l'option de configuration définie dans la console.

Cycle de vie des packages fixes

Les versions fixes sont téléchargées tant qu'elles sont disponibles depuis Sophos. Si une version fixe est en instance de retrait, une alerte apparaît dans la vue **Gestionnaires de mise à jour** près de tous les gestionnaires de mise à jour qui sont abonnés à cette version. Si l'alerte par email est activée, l'administrateur recevra aussi une alerte par email.

Lorsqu'une version fixe abonnée est retirée du marché, vous êtes automatiquement abonné à un nouveau package « Fixed Extended » si vous ne changez pas votre abonnement avant la fin du support. Retrouvez plus de renseignements dans l'article 121139 de la base de connaissances de Sophos.

Retrouvez plus de renseignements sur la politique de cycle de vie de Sophos Endpoint dans l'article 112580 de la base de connaissances Sophos.

6.2.3 Abonnement aux logiciels de sécurité

Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - mise à jour** pour modifier un abonnement logiciels.
- Vous ne pouvez pas modifier un abonnement s'il est appliqué à une stratégie de mise à jour elle-même appliquée hors de votre sous-parc actif.

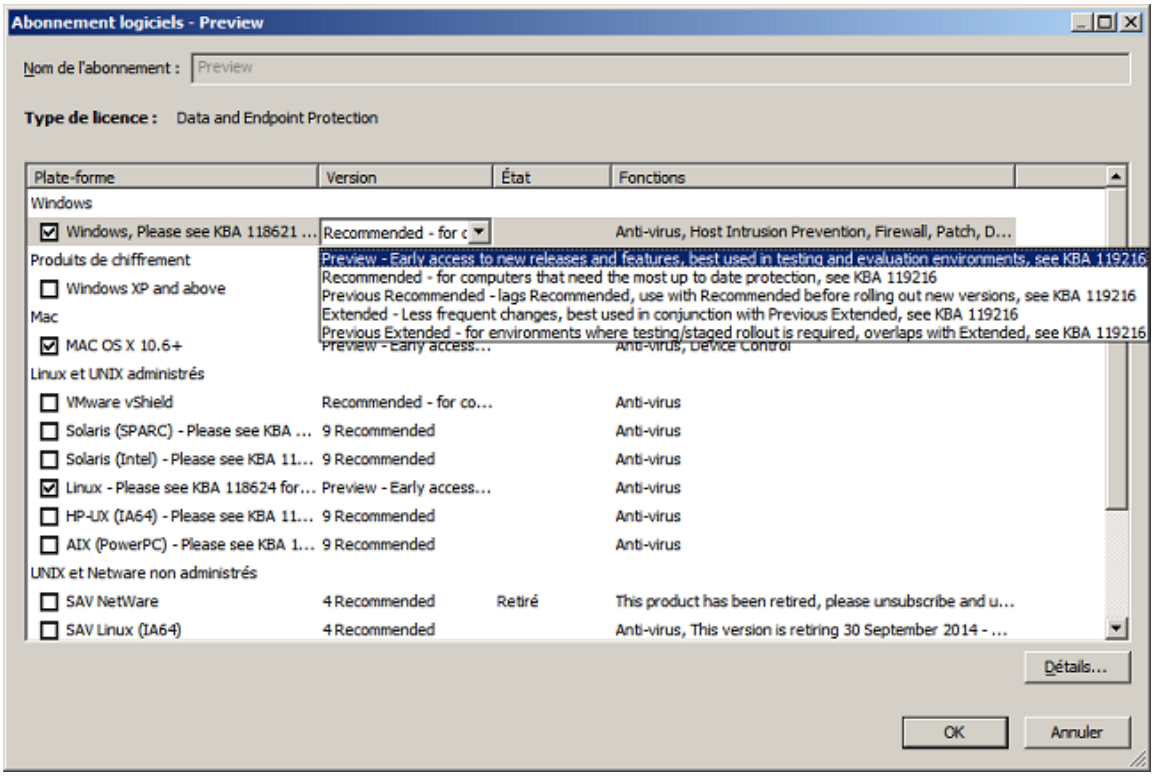
Retrouvez plus de renseignements sur l'administration déléguée à la section Gestion des rôles et des sous-parcs (page 14).

Pour vous abonner aux logiciels de sécurité :

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

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

   Sinon, si vous voulez créer une copie d'un abonnement existant, sélectionnez l'abonnement, cliquez dessus avec le bouton droit de la souris et cliquez sur **Dupliquer l'abonnement**. Saisissez un nouveau nom d'abonnement, puis cliquez deux fois dessus pour ouvrir la boîte de dialogue **Abonnement logiciels**.
3. Dans la boîte de dialogue **Abonnement logiciels**, modifiez le nom de l'abonnement, si vous le souhaitez.
4. Sélectionnez les plates-formes pour lesquelles vous souhaitez télécharger les logiciels.
5. Par défaut, vous êtes abonné au package « Recommended ». Vous avez également la possibilité de sélectionner un package différent (par exemple, si vous voulez découvrir les nouvelles fonctions en avant-première). Cliquez sur le champ **Version** situé à côté de la plate-forme pour laquelle vous voulez changer de package et cliquez de nouveau. Dans la liste du menu déroulant des versions disponibles, sélectionnez la version que vous souhaitez télécharger (par exemple « Preview »).



Retrouvez plus de renseignements sur les autres packages disponibles à la section Quels types de mise à jour sont disponibles ? (page 66)

Après vous être abonné aux logiciels de sécurité, vous pouvez paramétrer des alertes par email d'abonnement. Retrouvez plus de renseignements sur l'abonnement aux alertes par email à la section Configuration des alertes d'abonnement logiciels (page 190).

Si vous avez créé un nouvel abonnement logiciels, configurez le gestionnaire de mise à jour pour le maintenir à jour comme indiqué à la section Affichage ou modification de la configuration du gestionnaire de mise à jour (page 57).

6.2.4 Exécution de l'Assistant de téléchargement des logiciels de sécurité

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Paramétrage de la stratégie - mise à jour** pour exécuter l'**Assistant de téléchargement des logiciels de sécurité**. Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

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

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

  L'**Assistant de téléchargement des logiciels de sécurité** vous guide tout au long des opérations de sélection et de téléchargement des logiciels.

Remarque
Une fois que l'assistant a terminé toutes les opérations avec succès, l'option **Exécuter l'Assistant de téléchargement des logiciels de sécurité** disparaît du menu **Actions**.

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

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

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

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

6.3 Configuration de la stratégie de mise à jour

La mise à jour des stratégies vous permet de maintenir vos ordinateurs à jour avec votre logiciel de sécurité choisi. L'Enterprise Console vérifie les mises à jour et met à jour les ordinateurs, si nécessaire, dans un intervalle donné.

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

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

- Sélection d'un abonnement (page 70)
- Configuration des serveurs de mise à jour (page 71)
- Planification des mises à jour (page 76)
- Sélection d'une source différente pour l'installation initiale (page 77)
- Journalisation des mises à jour (page 78)

Remarque
Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - mise à jour** pour configurer une stratégie de mise à jour.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements sur l'administration déléguée à la section Gestion des rôles et des sous-parcs (page 14).

6.3.1 Sélection d'un abonnement

Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - mise à jour** pour configurer une stratégie de mise à jour.

- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

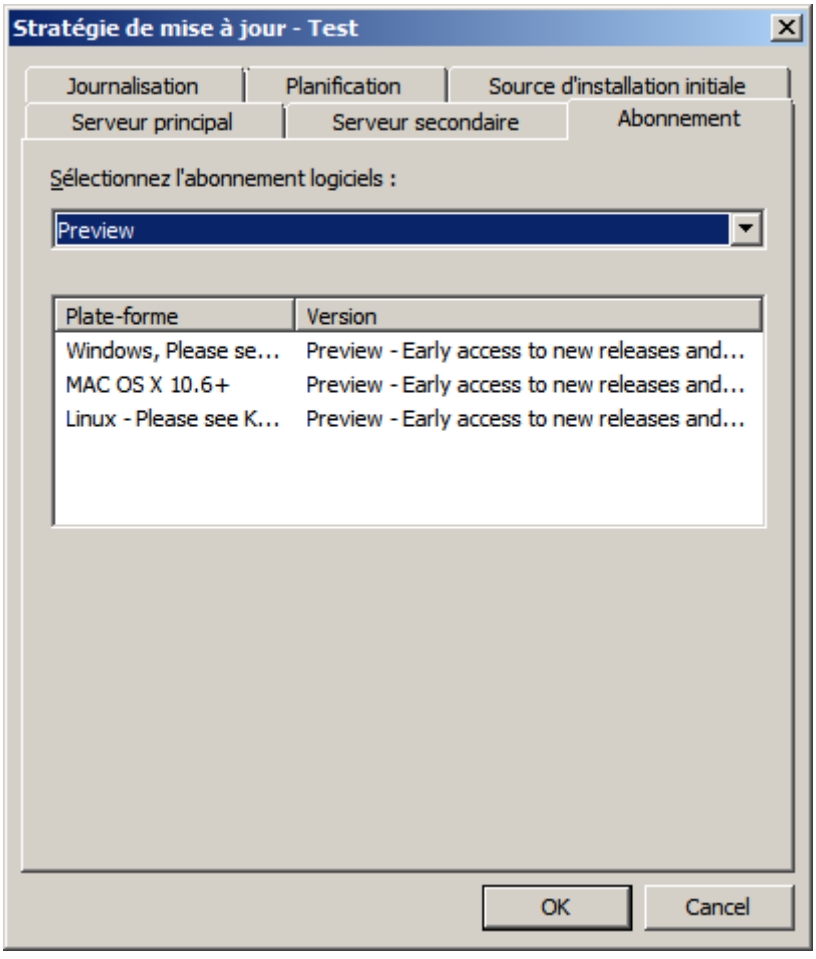
Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Un abonnement permet d'indiquer quelles versions des logiciels pour terminaux sont téléchargées depuis Sophos pour chaque plate-forme. L'abonnement par défaut inclut les logiciels les plus récents pour Windows.

Pour sélectionner un abonnement :

1. Vérifiez quelle stratégie de mise à jour est utilisée par le ou les groupes d'ordinateurs que vous désirez configurer.

   Retrouvez plus de renseignements à la section Vérification des stratégies utilisées par un groupe (page 27).
2. Dans le volet **Stratégies**, cliquez deux fois sur **Mise à jour**. Puis cliquez deux fois sur la stratégie que vous désirez changer.
3. Dans la boîte de dialogue **Stratégie de mise à jour**, cliquez sur l'onglet **Abonnement** et sélectionnez l'abonnement pour les logiciels que vous souhaitez maintenir à jour.



6.3.2 Configuration des serveurs de mise à jour

Par défaut, les ordinateurs se mettent à jour à partir d'une seule source principale de mise à jour dans un partage UNC, `\\<NomOrdinateur>\SophosUpdate`, où `<NomOrdinateur>` correspond au nom de l'ordinateur du gestionnaire de mise à jour. Vous pouvez indiquer une autre source secondaire pour les mises à jour, activer l'itinérance et activer la restriction de bande passante.

Si les terminaux ne sont pas en mesure de contacter leur source principale, ils tentent de se mettre à jour depuis leur source secondaire (si elle a été spécifiée). Nous vous conseillons de toujours spécifier une source secondaire.

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

Remarque
Les gestionnaires de mise à jour peuvent avoir plusieurs partages de distribution à disposition selon la manière dont vous les avez configurés.

Serveur principal

Le serveur principal est configuré automatiquement avec l'emplacement du serveur principal par défaut. Par défaut, les ordinateurs se mettent à jour à partir d'une seule source principale de mise à jour dans un partage UNC, `\\<NomOrdinateur>\SophosUpdate`, où `<NomOrdinateur>` correspond au nom de l'ordinateur sur lequel Sophos Update Manager est installé.

Pour accéder à ce partage, les ordinateurs utilisent les codes d'accès Sophos Update Manager que vous avez saisi au cours de l'installation de l'Enterprise Console. Si vous avez suivi les conseils du Guide de démarrage de l'Enterprise Console, le compte doit être nommé « SophosUpdateMgr ».

Retrouvez plus de renseignements sur la modification des codes d'accès à la section Changement des codes d'accès du serveur principal (page 74).

Si vous accédez à la source de mise à jour via un serveur proxy, cliquez sur **Détails du proxy** et saisissez les détails du serveur proxy.

Retrouvez plus de renseignements sur l'activation de l'itinérance à la section Itinérance pour les ordinateurs portables (page 72).

Vous pouvez également activer la restriction de la bande passante pour limiter la quantité de bande passante que les ordinateurs sont autorisés à utiliser lors de la mise à jour. Sur l'onglet **Serveur principal** de la stratégie de mise à jour, cliquez sur le bouton **Avancés**. Dans la boîte de dialogue **Paramètres avancés**, sélectionnez **Limiter la quantité de bande passante utilisée** et utilisez le curseur pour indiquer la bande passante maximum en Kbits/seconde.

Itinérance pour les ordinateurs portables

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

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

Remarque
Lorsque les ordinateurs fixes envoient les emplacements de mise à jour et les codes d'accès à l'ordinateur portable, les mots de passe sont brouillés lors de la transmission et du stockage. En revanche, les comptes définis pour les terminaux pour pouvoir lire les emplacements des serveurs de mise à jour doivent toujours être aussi restrictifs que possible et permettre uniquement un accès en lecture seule. Retrouvez plus de renseignements à la section Indication de l'emplacement du logiciel (page 60).

Retrouvez plus de renseignements sur l'itinérance à la section Comment fonctionne l'itinérance ? (page 73)

L'itinérance peut uniquement être utilisée lorsque :

- Il n'y a qu'une seule Enterprise Console commune aux terminaux itinérants et fixes.
- Les terminaux fixes utilisent le même abonnement logiciels que les ordinateurs portables itinérants.
- Il y a un emplacement de mise à jour principal spécifié dans la stratégie de mise à jour utilisée par les portables itinérants.
- Tous les pare-feu tiers sont configurés afin de permettre les demandes et les réponses de mise à jour des emplacements. Le port normalement utilisé est le port UDP 51235 mais il peut être configuré. Retrouvez plus de renseignements dans l'article 110371 de la base de connaissances Sophos.

Activez l'itinérance lorsque vous indiquez les sources de mises à jour. L'itinérance doit seulement être activée sur des groupes de machines qui sont fréquemment déplacées de bureau en bureau. Retrouvez plus de renseignements sur l'activation de l'itinérance à la section Changement des codes d'accès du serveur principal (page 74).

Retrouvez une foire aux questions sur l'itinérance dans l'article 112830 de la base de connaissances Sophos.

Comment fonctionne l'itinérance ?

L'itinérance est une méthode de mise à jour intelligente pour les portables itinérants. Les mises à jour sont exécutées à partir du « meilleur » emplacement de mise à jour, laquelle repose seulement sur les emplacements de mise à jour principal et secondaire spécifiés dans la stratégie de mise à jour des portables.

Lorsque l'itinérance est activée, voici ce qui se produit :

1. Lorsqu'un ordinateur portable change d'emplacement, le composant Sophos AutoUpdate de Enterprise Console installé sur celui-ci détermine que l'adresse MAC de la passerelle par défaut sur le réseau connecté a changé depuis la dernière mise à jour. Il envoie alors une émission ICMP via le sous-réseau local aux installations AutoUpdate avoisinantes à l'aide du port UDP 51235 par défaut.
2. Les installations AutoUpdate avoisinantes répondent avec leurs stratégies de mise à jour, à l'aide du même port. Seul l'emplacement de mise à jour principal est envoyé dans la réponse.

   Toutes les installations Enterprise Console surveillent les émissions, que l'itinérance soit activée ou non.

   Dans les réponses, les informations sensibles sont dissimulées et les champs sont hachurés pour préserver l'intégrité.

   Les messages de réponse ont un temps de réponse aléatoire, pour éviter l'afflux de messages. Les réponses sont aussi des émissions ICMP, ainsi tout autre machine qui répond avec les mêmes détails reçoit l'émission et sait qu'il ne faut pas répondre.

3. AutoUpdate choisit le « meilleur » emplacement à partir des emplacements reçus et vérifie si l'expéditeur est administré par la même Enterprise Console et si l'identifiant d'abonnement correspond à celui utilisé par AutoUpdate sur l'ordinateur portable.

   Le « meilleur » emplacement de mise à jour est déterminé par le nombre de bonds pour accéder à l'emplacement de mise à jour.

4. Une mise à jour est alors tentée et, si elle est réussie, l'emplacement est placé en mémoire cache.

   Un maximum de quatre emplacements de mise à jour accessibles avec le même ID d'abonnement et le nombre de bonds le plus faible sont stockés sur l'ordinateur portable (dans le fichier `iustatus.xml` à l'emplacement suivant : `C:\Program Files\Sophos\AutoUpdate\data\status\iustatus.xml`).

   Ces emplacements de mise à jour sont vérifiés chaque fois qu'AutoUpdate effectue une mise à jour.

Remarque
Si vous avez besoin de revenir à l'utilisation des emplacements de mise à jour principal et secondaire spécifiés dans la stratégie de mise à jour (par exemple, si vous souhaitez déployer des personnalisations à partir de l'emplacement de mise à jour spécifié dans la stratégie), vous devez désactiver l'itinérance.

Activation de l'itinérance

Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - mise à jour** pour configurer une stratégie de mise à jour.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Activez seulement l'itinérance sur des groupes de machines qui voyagent fréquemment de bureau en bureau.

Pour activer l'itinérance :

1. Dans le volet **Stratégies**, cliquez deux fois sur **Mise à jour**. Puis cliquez deux fois sur la stratégie de mise à jour que vous désirez changer.
2. Dans la boîte de dialogue **Stratégie de mise à jour**, sur l'onglet **Serveur principal**, sélectionnez la case à cocher **Autoriser l'itinérance**.
3. Dans le volet **Groupes**, sélectionnez un groupe qui utilise la stratégie de mise à jour que vous venez de changer. Cliquez avec le bouton droit de la souris et sélectionnez **Mettre en conformité avec**, **Stratégie de mise à jour du groupe**.

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

Remarque
Si vous avez ultérieurement besoin de revenir à l'utilisation des emplacements de mise à jour principal et secondaire spécifiés dans la stratégie de mise à jour, désactivez l'itinérance.

Changement des codes d'accès du serveur principal

Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - mise à jour** pour configurer une stratégie de mise à jour.

- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Pour changer les codes d'accès du serveur principal :

1. Dans le volet **Stratégies**, cliquez deux fois sur **Mise à jour**. Puis cliquez deux fois sur la stratégie de mise à jour que vous désirez changer.
2. Dans la boîte de dialogue **Stratégie de mise à jour**, sur l'onglet **Serveur principal**, saisissez les nouveaux codes d'accès qui seront utilisés pour accéder au serveur. Changez les autres détails, si besoin est.

   Remarque
   Si votre source de mise à jour principale est un dossier sur votre site Web et si vous utilisez Internet Information Services (IIS) avec l'authentification anonyme, vous devrez tout de même saisir des codes d'accès sur l'onglet **Serveur principal**. Utilisez les codes d'accès pour le partage UNC de la « source d'installation initiale », même si vous n'en avez pas besoin pour accéder au serveur Web. Si vous laissez vides les champs **Nom d'utilisateur** et **Mot de passe** sur l'onglet **Serveur principal**, vous ne pourrez pas protéger les terminaux depuis la console.

3. Dans le volet **Groupes**, sélectionnez un groupe qui utilise la stratégie de mise à jour que vous venez de changer. Cliquez avec le bouton droit de la souris et sélectionnez **Mettre en conformité avec**, **Stratégie de mise à jour du groupe**.

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

Paramétrage du serveur de mise à jour secondaire

Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - mise à jour** pour configurer une stratégie de mise à jour.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

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

1. Vérifiez quelle stratégie de mise à jour est utilisée par le ou les groupes d'ordinateurs que vous désirez configurer.

   Retrouvez plus de renseignements à la section Vérification des stratégies utilisées par un groupe (page 27).
2. Dans le volet **Stratégies**, cliquez deux fois sur **Mise à jour** puis cliquez deux fois sur la stratégie que vous souhaitez modifier.
3. Dans la boîte de dialogue **Stratégie de mise à jour**, cliquez sur l'onglet **Serveur secondaire** et sélectionnez la case à cocher **Indiquer les détails du serveur secondaire**.
4. Dans le champ **Adresse (HTTP ou UNC)**, procédez de la manière suivante :
   - Saisissez l'URL HTTP ou le chemin du réseau UNC du partage du serveur de mise à jour.
   - Sélectionnez **Sophos**.

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

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

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

   Remarque
   Si le nom d'utilisateur doit être qualifié pour indiquer le domaine, utilisez la forme domaine \nomutilisateur. Retrouvez plus de renseignements sur la vérification d'un compte utilisateur Windows dans l'article 11637 de la base de connaissances Sophos.

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

   Remarque
   Sachez que certains fournisseurs de service Internet exigent que les requêtes HTPP soient envoyées au serveur proxy.

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

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

6.3.3 Planification des mises à jour

Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - mise à jour** pour configurer une stratégie de mise à jour.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Par défaut, les terminaux vérifient les mises à jour dans le partage réseau toutes les 5 minutes.

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

Pour indiquer l'intervalle de mise à jour :

1. Vérifiez quelle stratégie de mise à jour est utilisée par le ou les groupes d'ordinateurs que vous désirez configurer.

   Retrouvez plus de renseignements à la section Vérification des stratégies utilisées par un groupe (page 27).
2. Dans le volet **Stratégies**, cliquez deux fois sur **Mise à jour**. Puis cliquez deux fois sur la stratégie que vous désirez changer.
3. Dans la boîte de dialogue **Stratégie de mise à jour**, sur l'onglet **Planification**, laissez **Permettre l'utilisation automatique des mises à jour aux ordinateurs** sélectionné. Saisissez l'intervalle entre les mises à jour logicielles (en minutes).
4. Si les ordinateurs se mettent à jour via une connexion modem à Internet, sélectionnez **Vérifier les mises à jour à la connexion**.
   Les ordinateurs tenteront alors d'effectuer la mise à jour chaque fois qu'ils se connecteront à Internet.

6.3.4 Sélection d'une source différente pour l'installation initiale

Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - mise à jour** pour configurer une stratégie de mise à jour.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

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

Remarque
Ce paramètre s'applique uniquement à Windows.

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

Pour effectuer l'installation initiale depuis une source différente :

1. Vérifiez quelle stratégie de mise à jour est utilisée par le ou les groupes d'ordinateurs que vous désirez configurer.

   Retrouvez plus de renseignements à la section Vérification des stratégies utilisées par un groupe (page 27).
2. Dans le volet **Stratégies**, cliquez deux fois sur **Mise à jour**. Puis cliquez deux fois sur la stratégie que vous désirez changer.
3. Dans la boîte de dialogue **Stratégie de mise à jour**, sur l'onglet **Source d'installation initiale**, dessélectionnez la case à cocher **Utiliser l'adresse du serveur principal**. Puis saisissez l'adresse de la source que vous souhaitez utiliser.

6.3.5 Journalisation des mises à jour

Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - mise à jour** pour configurer une stratégie de mise à jour.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

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

Pour changer les paramètres de journalisation :

1. Vérifiez quelle stratégie de mise à jour est utilisée par le ou les groupes d'ordinateurs que vous désirez configurer.

   Retrouvez plus de renseignements à la section Vérification des stratégies utilisées par un groupe (page 27).
2. Dans le volet **Stratégies**, cliquez deux fois sur **Mise à jour**. Puis cliquez deux fois sur la stratégie que vous désirez changer.
3. Dans la boîte de dialogue **Stratégie de mise à jour**, sur l'onglet **Journalisation**, laissez **Enregistrer l'activité de Sophos AutoUpdate** sélectionné. Dans le champ **Taille maximale du journal** , indiquez une taille maximale du journal en Mo.
4. Dans le champ **Niveau du journal**, sélectionnez **Normal** ou **Détaillé**.

   La journalisation détaillée fournit des informations sur beaucoup plus d'activités que le journal normal c'est pourquoi il prend du volume plus rapidement. Utilisez ce paramétrage uniquement lorsqu'une journalisation détaillée est nécessaire pour la résolution des problèmes.

6.4 Surveillance du gestionnaire de mise à jour

Vérification de l'état du gestionnaire de mise à jour sur le Tableau de bord

L'état des gestionnaires de mise à jour apparaît dans le volet **Mises à jour** sur le **Tableau de bord**. Ceci vous indique quand la dernière mise à jour a été téléchargée depuis Sophos et affiche un avertissement si le temps écoulé depuis la dernière mise à jour dépasse le seuil d'avertissement ou critique.

Remarque
La section **Mises à jour** du tableau de bord ne signale pas d'alerte ou d'erreur si un gestionnaire de mise à jour est temporairement incapable de mettre à jour. Des alertes et des erreurs sont générées seulement si la durée écoulée depuis la dernière mise à jour du gestionnaire de mise à jour dépasse le seuil d'alerte ou critique défini à la section Configuration du tableau de bord (page 49).

Vérification des alertes et des erreurs du gestionnaire de mise à jour

Les alertes et les erreurs du gestionnaire de mise à jour apparaissent dans la vue **Gestionnaires de mise à jour**, les colonnes **Alertes** et **Erreurs** respectivement.

Si vous vous êtes abonné à une version fixe des logiciels, une alerte apparaîtra lorsque cette version sera en instance de retrait ou retirée. Une alerte apparaîtra également si la licence de votre produit a changé.

Pour voir les alertes et les erreurs du gestionnaire de mise à jour :

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

   Dans la boîte de dialogue **Détails du gestionnaire de mise à jour**, vous pouvez voir l'heure des dernières mises à jour des données de détection des menaces et des logiciels, l'état de l'abonnement ou des abonnements que le gestionnaire de mise à jour maintient à jour ainsi que l'état de ce dernier.
4. Pour en savoir plus sur l'état d'un gestionnaire de mise à jour donné et pour avoir plus d'informations sur les moyens de l'exploiter, suivez le lien dans la colonne **Description**.

Si vous devez vérifier ou changer votre abonnement, par exemple, si le produit auquel vous vous êtes abonné est sur le point d'être retiré, ou si la licence de votre produit a changé et la nouvelle licence n'inclut pas ce produit, veuillez consulter la section Abonnement aux logiciels de sécurité (page 68).

Si de nouvelles fonctionnalités deviennent disponibles suite à un changement de licence, vous pouvez avoir besoin de configurer de nouvelles stratégies avant de pouvoir utiliser ces fonctionnalités.

Abonnement aux alertes par email

Vous pouvez paramétrer des alertes par email à envoyer à vos destinataires choisis lorsque la version du produit auquel vous vous êtes abonné est sur le point d'être retiré ou est retiré, ou bien lorsque les fonctionnalités de votre produit Sophos changent suite à un changement de licence. Retrouvez plus de renseignements à la section Configuration des alertes d'abonnement logiciels (page 190).

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

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Actualisation - nettoyage** pour effacer les alertes depuis la console. Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

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

1. Dans la vue **Gestionnaires de mise à jour**, sélectionnez le ou les gestionnaires de mise à jour pour lequel ou lesquels vous souhaitez effacer les alertes. Cliquez avec le bouton droit de la souris et sélectionnez **Approuver les alertes**.
   La boîte de dialogue **Alertes du gestionnaire de mise à jour** apparaît.
2. Pour effacer les alertes depuis la console, sélectionnez les alertes que vous souhaitez effacer et cliquez sur **Approuver**.
   Les alertes approuvées (supprimées) n'apparaissent plus dans la console.

6.5 Mise à jour des ordinateurs non à jour

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Actualisation - mise à jour et contrôle** pour mettre à jour les ordinateurs. Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

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

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

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

- L'ordinateur ne parvient pas à récupérer une mise à jour depuis le serveur.
- Le serveur ne dispose pas du logiciel Sophos le plus récent.

Pour diagnostiquer le problème et mettre à jour les ordinateurs :

1. Dans la vue **Terminaux**, sélectionnez le groupe qui contient les ordinateurs non à jour.
2. Sur l'onglet **État**, cliquez sur la colonne **A jour** pour trier les ordinateurs par leur état de mise à jour le plus récent.
3. Cliquez sur l'onglet **Détails de la mise à jour** et observez la colonne **Serveur principal**.
   Le répertoire à partir duquel chaque ordinateur se met à jour apparaît.
4. A présent, observez les ordinateurs qui se mettent à jour à partir d'un répertoire particulier.
   - *Si certains ne sont pas à jour alors que d'autres le sont*, le problème provient des ordinateurs individuels. Sélectionnez-les, cliquez dessus avec le bouton droit de la souris, puis cliquez sur **Mettre les ordinateurs à jour maintenant**.
   - *Si tous ne sont pas à jour*, le problème peut provenir du répertoire. Dans le menu **Affichage**, cliquez sur **Gestionnaires de mise à jour**. Sélectionnez le gestionnaire de mise à jour qui gère le répertoire que vous soupçonnez de ne pas être à jour, cliquez dessus avec le bouton droit de la souris et cliquez sur **Mettre à jour maintenant**. Dans le menu **Affichage**, cliquez sur **Terminaux**. Sélectionnez les ordinateurs non à jour, cliquez avec le bouton droit de la souris et cliquez sur **Mettre les ordinateurs à jour maintenant**.

   Si vous avez plusieurs gestionnaires de mise à jour et ne savez pas lequel gère le répertoire non à jour, utilisez le rapport Hiérarchie des mises à jour pour voir quels partages sont gérés par chaque gestionnaire de mise à jour. Pour consulter le rapport Hiérarchie des mises à jour, dans le menu **Outils**, cliquez sur **Gérer les rapports**. Dans la boîte de dialogue **Gestionnaire des rapports**, sélectionnez **Hiérarchie des mises à jour** et cliquez sur **Exécuter**. Retrouvez plus de renseignements à la section « Partages gérés par les gestionnaires de mise à jour » du rapport.

7 Configuration des stratégies

7.1 Stratégie antivirus et HIPS

Une stratégie antivirus et HIPS vous permet de réaliser les opérations suivantes :

- Détecter automatiquement les virus, les chevaux de Troie, les vers et les spywares connus et inconnus dès que les utilisateurs tentent de copier, de déplacer ou d'ouvrir des fichiers qui les contiennent.
- Contrôler les ordinateurs à la recherche des adwares et autres applications potentiellement indésirables.
- Contrôler les ordinateurs à la recherche des fichiers suspects et des rootkits.
- Détecter le trafic réseau malveillant, c'est-à-dire les communications entre les terminaux et les serveurs de commande et de contrôle impliqués dans des attaques par botnet ou par autre programme malveillant.
- Nettoyer automatiquement les ordinateurs dès la découverte d'un virus ou de toute autre menace.

  Retrouvez plus de renseignements sur la modification des paramètres du nettoyage automatique à la section Paramétrage du nettoyage automatique pour le contrôle sur accès (page 86).
- Analyser également le comportement des programmes s'exécutant sur le système.

  Retrouvez plus de renseignements à la section Surveillance des comportements (page 97).
- Contrôler les ordinateurs à des heures définies.

  Retrouvez plus de renseignements à la section Création d'un contrôle planifié (page 90).

Vous pouvez utiliser différents paramètres de contrôle pour chaque groupe d'ordinateurs. Retrouvez plus de renseignements sur la configuration des paramètres de contrôle aux sections suivantes :

- Configuration du contrôle sur accès (page 83)
- Configuration des paramètres de contrôle pour un contrôle planifié (page 91)

Remarque
Les SophosLabs peut suivre les fichiers qui sont contrôlés de manière indépendante. Ils peuvent ajouter ou supprimer le contrôle de certains types de fichier afin d'assurer une protection optimale.

Retrouvez plus de renseignements sur les options de contrôle et de nettoyage qui n'affectent pas Mac, Linux ou UNIX à la section Paramètres non applicables sous Mac, Linux ou UNIX (page 82).

Retrouvez plus de renseignements sur les options de contrôle et de nettoyage qui ne s'appliquent pas à Sophos Anti-Virus pour VMware vShield dans l'article 121745 de la base de connaissances de Sophos. Pour la version 2.x de Sophos Anti-Virus pour VMware vShield, veuillez également consulter le *Guide de configuration de Sophos Anti-Virus pour VMware vShield* sur www.sophos.com/fr-fr/support/documentation/sophos-anti-virus-for-vmware-vshield.

7.1.1 Paramètres non applicables sous Mac, Linux ou UNIX

Tous les types de contrôle et de nettoyage sur les ordinateurs Windows peuvent être entièrement administrés à partir de l'Enterprise Console. Toutefois, un certain nombre de paramètres ne s'appliquent pas aux ordinateurs Mac, Linux ou UNIX.

Mac OS X

Retrouvez plus de renseignements sur les paramètres de la stratégie antivirus et HIPS s'appliquant aux ordinateurs Mac dans l'article 118859 de la base de connaissances Sophos.

Linux

Les options de nettoyage automatique suivantes ne s'appliquent pas aux ordinateurs Linux et seront ignorées par ceux-ci.

Options de nettoyage automatique pour le contrôle sur accès :

- **Refuser l'accès et déplacer dans l'emplacement par défaut**
- **Refuser l'accès et déplacer dans**

Options de nettoyage automatique pour le contrôle planifié :

- **Déplacer dans l'emplacement par défaut**
- **Déplacer dans**

Retrouvez plus de renseignements sur les paramètres de nettoyage automatique aux sections Paramétrage du nettoyage automatique pour le contrôle planifié (page 93) et Paramètres de nettoyage automatique pour le contrôle planifié (page 94).

Retrouvez plus de renseignements sur les paramètres de la stratégie antivirus et HIPS s'appliquant aux ordinateurs Linux dans l'article 117344 de la base de connaissances Sophos.

UNIX

- L'Enterprise Console ne peut pas effectuer de contrôles sur accès sur les ordinateurs UNIX.

  Vous pouvez configurer les contrôles planifiés, les alertes, la journalisation et la mise à jour de manière centralisée depuis l'Enterprise Console.

  Remarque
  Ces fonctions incluent également certains paramètres qui ne peuvent pas être définis à l'aide de l'Enterprise Console. Vous pouvez définir ces paramètres localement sur chaque ordinateur UNIX à partir de l'interface de ligne de commande de Sophos Anti-Virus. L'Enterprise Console les ignore.

  Vous pouvez aussi configurer les contrôles à la demande localement sur chaque ordinateur UNIX à partir de l'interface de ligne de commande de Sophos Anti-Virus.

  Retrouvez plus de renseignements sur la configuration des paramètres supplémentaires ou sur la configuration locale de Sophos Anti-Virus pour UNIX dans le *Guide de configuration de Sophos Anti-Virus pour UNIX*.

- Les options de nettoyage automatique suivantes pour le contrôle planifié ne s'appliquent pas aux ordinateurs UNIX et seront ignorées par ceux-ci.
  - **Déplacer dans l'emplacement par défaut**
  - **Déplacer dans**

  Retrouvez plus de renseignements sur les options de nettoyage automatique pour le contrôle planifié à la section Paramètres de nettoyage automatique pour le contrôle planifié (page 94).

Retrouvez plus de renseignements sur les paramètres de la stratégie antivirus et HIPS s'appliquant aux ordinateurs UNIX dans l'article 117344 de la base de connaissances Sophos.

7.1.2 Contrôle sur accès

À propos de la meilleure protection par contrôle sur accès

Cette section vous donne des conseils utiles qui vous permettront d'utiliser le contrôle sur accès de manière optimale.

Nous vous conseillons d'utiliser les paramètres par défaut du contrôle sur accès car ils vous garantissent le meilleur compromis entre la protection contre les menaces et de bonnes performances de tout votre système. Retrouvez plus de renseignements sur les paramètres conseillés du contrôle sur accès dans l'article 114345 de la base de connaissances du support Sophos (http://www.sophos.com/fr-fr/support/knowledgebase/114345.aspx).

Nous vous conseillons de consulter le *Guide de configuration des stratégies de Sophos Enterprise Console* pour obtenir des conseils pratiques en matière d'utilisation et d'administration des logiciels de sécurité Sophos. Retrouvez toute la documentation Sophos sur http://www.sophos.com/fr-fr/support/documentation.

Configuration du contrôle sur accès

Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - antivirus et HIPS** pour réaliser cette tâche.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Attention
Le contrôle sur accès ne détecte pas les virus lorsque certains logiciels de chiffrement sont installés. Modifiez les processus de démarrage afin de vous assurer que ces fichiers sont déchiffrés lorsque le contrôle sur accès commence. Retrouvez plus de renseignements sur l'utilisation de la stratégie antivirus et HIPS avec un logiciel de chiffrement dans l'article 12790 de la base de connaissances Sophos.

Pour configurer le contrôle sur accès :

1. Vérifiez quelle stratégie antivirus et HIPS est utilisée par le(s) groupe(s) d'ordinateurs que vous voulez configurer.

   Retrouvez plus de renseignements à la section Vérification des stratégies utilisées par un groupe (page 27).
2. Dans le volet **Stratégies**, cliquez deux fois sur **Antivirus et HIPS**.
3. Cliquez deux fois sur la stratégie que vous désirez modifier.

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

4. Dans le volet **Contrôle sur accès**, près de **Activer le contrôle sur accès**, cliquez sur **Configurer**.
5. Pour changer le moment où le contrôle sur accès doit avoir lieu, sous **Vérifier les fichiers**, paramétrez les options comme décrit ci-dessous.

Option	Description
À la lecture	• Contrôle des fichiers lorsqu'ils sont copiés, déplacés ou ouverts. • Contrôle des programmes lorsqu'ils sont démarrés.
Au moment de renommer	Contrôle des fichiers lorsqu'ils sont renommés.
À l'écriture	Contrôle des fichiers lorsqu'ils sont enregistrés ou créés.

6. Sous **Rechercher les**, paramétrez les options comme décrit ci-dessous.

Option	Description
Adwares et PUA	• Un adware affiche de la publicité (par exemple, des messages intempestifs), qui affecte la productivité des utilisateurs et les performances du système. • Une application potentiellement indésirable ou PUA (Potentially Unwanted Application) n'est pas malveillante mais sa présence sur les réseaux d'entreprise est généralement considérée comme inappropriée.
Fichiers suspects	Les fichiers suspects affichent certaines caractéristiques (par exemple, du code de décompression dynamique) qui sont fréquemment, mais pas exclusivement, trouvées dans les malwares. Par contre, ces caractéristiques ne sont pas suffisamment solides pour que le fichier soit identifié comme un nouvel élément de malware. **Remarque** Cette option s'applique uniquement à Sophos Endpoint Security and Control pour Windows.

7. Sous **Autres options de contrôle**, paramétrez les options comme décrit ci-dessous.

Option	Description
Autoriser l'accès aux lecteurs aux secteurs de démarrage infectés	Autorisez l'accès à un support ou périphérique amovible dont le secteur de démarrage est infecté tel qu'un CD-ROM

Option	Description
	d'initialisation, une disquette ou un lecteur flash USB. Utilisez uniquement cette option après avoir demandé conseil auprès du support technique de Sophos.
Contrôler dans les fichiers archive	Contrôlez le contenu d'une archive ou de fichiers compressés avant qu'ils ne soient téléchargés ou envoyés par email depuis des ordinateurs administrés. Nous vous conseillons de conserver cette option **désactivée** car elle ralentit considérablement le contrôle. L'utilisateur sera quand même protégé contre les menaces présentes dans les archives ou dans les fichiers compressés car tous les composants d'une archive ou d'un fichier compressé caractéristiques d'un programme malveillant seront bloqués par le contrôle sur accès : • Lorsque l'utilisateur ouvre un fichier extrait du fichier archive, le fichier extrait est contrôlé. • Les fichiers compressés avec des utilitaires de compression dynamiques tels que PKLite, LZEXE et Diet sont contrôlés.
Contrôler la mémoire système	Exécutez un contrôle en tâche de fond toutes les heures afin de détecter les programmes malveillants cachés dans la mémoire système de l'ordinateur (la mémoire utilisée par le système d'exploitation).

Activation ou désactivation du contrôle sur accès

Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - antivirus et HIPS** pour réaliser cette tâche.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Par défaut, Sophos Endpoint Security and Control contrôle les fichiers au moment où l'utilisateur tente d'y accéder et refuse leur accès sauf s'ils sont sains.

Vous avez la possibilité de désactiver le contrôle sur accès sur les serveurs Exchange ou sur d'autres serveurs dont les performances pourraient être affectées. Dans ce cas, placez les serveurs dans un groupe spécial et changez la stratégie antivirus et HIPS de ce groupe comme indiqué ci-dessous.

Pour activer ou désactiver le contrôle sur accès :

1. Vérifiez quelle stratégie antivirus et HIPS est utilisée par le ou les groupes d'ordinateurs que vous voulez configurer.

   Retrouvez plus de renseignements à la section Vérification des stratégies utilisées par un groupe (page 27).
2. Dans le volet **Stratégies**, cliquez deux fois sur **Antivirus et HIPS**. Puis cliquez deux fois sur la stratégie que vous désirez changer.
   La boîte de dialogue **Stratégie antivirus et HIPS** apparaît.
3. Dans le volet **Contrôle sur accès**, sélectionnez ou dessélectionnez la case à cocher **Activer le contrôle sur accès**.

Important
si vous désactivez le contrôle sur accès sur un serveur, nous vous conseillons de paramétrer les contrôles planifiés sur les ordinateurs appropriés. Retrouvez plus d'instructions sur la manière de créer des contrôles planifiés à la section Création d'un contrôle planifié (page 90)

Paramétrage du nettoyage automatique pour le contrôle sur accès

Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - antivirus et HIPS** pour réaliser cette tâche.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Par défaut, Sophos Endpoint Security and Control nettoie automatiquement les ordinateurs dès la découverte d'un virus ou de toute autre menace. Vous pouvez changer les paramètres du nettoyage automatique comme décrit ci-dessous.

1. Vérifiez quelle stratégie antivirus et HIPS est utilisée par le(s) groupe(s) d'ordinateurs que vous voulez configurer.

   Retrouvez plus de renseignements à la section Vérification des stratégies utilisées par un groupe (page 27).
2. Dans le volet **Stratégies**, cliquez deux fois sur **Antivirus et HIPS**.
3. Cliquez deux fois sur la stratégie que vous désirez modifier.
   La boîte de dialogue **Stratégie antivirus et HIPS** apparaît.
4. Dans le volet **Contrôle sur accès**, près de **Activer le contrôle sur accès**, cliquez sur **Configurer**.
5. Dans la boîte de dialogue **Paramètres de contrôle sur accès**, cliquez sur l'onglet **Nettoyage**.
6. Configurez les options comme indiqué à la section Paramètres de nettoyage automatique pour le contrôle sur accès (page 86).

Paramètres de nettoyage automatique pour le contrôle sur accès

Virus/spywares

Sélectionnez ou dessélectionnez la case à cocher **Nettoyer automatiquement les éléments contenant un virus/spyware**.

Vous pouvez aussi spécifier ce que vous souhaitez faire des éléments en cas d'échec du nettoyage :

- **Refuser l'accès uniquement**

- **Supprimer**
- **Refuser l'accès et déplacer dans l'emplacement par défaut**
- **Refuser l'accès et déplacer dans (saisir un chemin UNC complet)**

Remarque
Les paramètres **Refuser l'accès et déplacer dans l'emplacement par défaut** et **Refuser l'accès et déplacer dans** ne s'appliquent pas aux ordinateurs Linux ou UNIX et seront ignorés par ceux-ci.

Fichiers suspects

Remarque
Ces paramètres s'appliquent uniquement aux ordinateurs Windows.

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

- **Refuser l'accès uniquement**
- **Supprimer**
- **Refuser l'accès et déplacer dans l'emplacement par défaut**
- **Refuser l'accès et déplacer dans (saisir un chemin UNC complet)**

Extensions de fichier pour le contrôle sur accès

Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - antivirus et HIPS** pour réaliser cette tâche.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

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

1. Vérifiez quelle stratégie antivirus et HIPS est utilisée par le(s) groupe(s) d'ordinateurs que vous voulez configurer.

   Retrouvez plus de renseignements à la section Vérification des stratégies utilisées par un groupe (page 27).
2. Dans le volet **Stratégies**, cliquez deux fois sur **Antivirus et HIPS**.
3. Cliquez deux fois sur la stratégie que vous désirez modifier.
   La boîte de dialogue **Stratégie antivirus et HIPS** apparaît.
4. Dans le volet **Contrôle sur accès**, près de **Activer le contrôle sur accès**, cliquez sur **Configurer**.
5. Cliquez sur l'onglet **Extensions** et configurez les options comme décrit ci-dessous.

Option	Description
Contrôler tous les fichiers	Contrôlez tous les fichiers quelle que soit l'extension du fichier. Si vous activez cette option, les autres options de l'onglet **Extensions** sont désactivées.

Option	Description
	Le contrôle de tous les fichiers affecte les performances de l'ordinateur, nous vous conseillons donc d'activer cette option seulement dans le cadre d'un contrôle planifié hebdomadaire.
Contrôler uniquement les exécutables et autres fichiers vulnérables	• Vérifiez tous les fichiers avec des extensions d'exécutables (par exemple, .exe, .bat, .pif) ou les fichiers qui sont susceptibles d'être infectés (par exemple, .doc, .chm, .pdf). • Vérifiez rapidement la structure de tous les fichiers, puis contrôlez-les si leur format est celui d'un fichier exécutable.
Extensions des types de fichiers supplémentaires à contrôler	Pour contrôler des types de fichiers supplémentaires, cliquez sur **Ajouter**, puis saisissez l'extension du fichier, par exemple PDF, dans le champ **Extension**. Vous pouvez utiliser le caractère ? pour remplacer tout caractère. Pour arrêter le contrôle d'un type de fichier, sélectionnez son extension dans la liste, puis cliquez sur **Supprimer**. Pour changer un type de fichier, sélectionnez son extension dans la liste, puis cliquez sur **Modifier**.
Contrôler les fichiers sans extension	Les fichiers sans extension peuvent être du malware, nous vous conseillons donc de laisser cette option activée.
Exclure	Pour exclure des types de fichiers spécifiques du contrôle sur accès, cliquez sur **Ajouter**, puis saisissez l'extension du fichier, par exemple PDF, dans le champ **Extension**. Pour démarrer le contrôle d'un type de fichier, sélectionnez son extension dans la liste, puis cliquez sur **Supprimer**. Pour changer un type de fichier, sélectionnez son extension dans la liste, puis cliquez sur **Renommer**.

Exclusion d'éléments du contrôle sur accès

Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - antivirus et HIPS** pour réaliser cette tâche.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Vous pouvez exclure des éléments du contrôle sur accès.

Remarque
Ces options s'appliquent uniquement aux ordinateurs Windows, Mac OS X et Linux.

L'Enterprise Console ne peut pas effectuer de contrôles sur accès sur les ordinateurs UNIX.

1. Vérifiez quelle stratégie antivirus et HIPS est utilisée par le(s) groupe(s) d'ordinateurs que vous voulez configurer.

   Retrouvez plus de renseignements à la section Vérification des stratégies utilisées par un groupe (page 27).
2. Dans le volet **Stratégies**, cliquez deux fois sur **Antivirus et HIPS**. Puis cliquez deux fois sur la stratégie que vous désirez changer.

   La boîte de dialogue **Stratégie antivirus et HIPS** apparaît.
3. Dans le volet **Contrôle sur accès**, cliquez sur le bouton **Configurer**.
4. Cliquez sur l'onglet **Exclusions Windows**, **Exclusions Mac** ou **Exclusions Linux/UNIX**. Pour ajouter des éléments dans la liste, cliquez sur **Ajouter** et saisissez le chemin complet dans la boîte de dialogue **Exclusion d'un élément**.

   Les éléments que vous pouvez exclure du contrôle diffèrent selon chaque type d'ordinateur. Retrouvez plus de renseignements à la section Éléments pouvant être exclus du contrôle (page 107).

   Pour exclure des fichiers qui ne sont pas stockés sur les lecteurs locaux, sélectionnez la case à cocher **Exclure les fichiers distants**. Vous pouvez sélectionnez cette option si vous voulez augmenter la vitesse d'accès à ces fichiers et si vous faites confiance aux emplacements de fichiers distants disponibles.

Important
Si vous sélectionnez **Exclure les fichiers distants** sur l'onglet **Exclusions Windows**, le contrôle des données n'effectue pas le contrôle des fichiers téléchargés ou joints à partir d'un emplacement réseau à l'aide d'une application surveillée, par exemple, un client de messagerie, un navigateur web ou un client de messagerie instantanée (IM). En effet, le contrôle des données utilise la même série d'exclusions que le contrôle sur accès de Sophos Anti-Virus (InterCheck ™). Ainsi, si le contrôle des fichiers distants est désactivé, il n'envoie aucun fichier distant au contrôle des données. Cette restriction ne s'applique pas à la surveillance des périphériques de stockage.

Vous pouvez exporter la liste des exclusions Windows dans un fichier, puis l'importer dans une autre stratégie. Retrouvez plus de renseignements à la section Importation ou exportation des exclusions du contrôle sur accès (page 89).

Importation ou exportation des exclusions du contrôle sur accès

Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - antivirus et HIPS** pour réaliser cette tâche.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Vous pouvez exporter dans un fichier la liste des exclusions Windows pour le contrôle sur accès, puis l'importer dans une autre stratégie.

1. Vérifiez quelle stratégie antivirus et HIPS est utilisée par le(s) groupe(s) d'ordinateurs que vous voulez configurer.

   Retrouvez plus de renseignements à la section Vérification des stratégies utilisées par un groupe (page 27).
2. Dans le volet **Stratégies**, cliquez deux fois sur **Antivirus et HIPS**.
3. Cliquez deux fois sur la stratégie que vous désirez modifier.
   La boîte de dialogue **Stratégie antivirus et HIPS** apparaît.
4. Dans le volet **Contrôle sur accès**, près de **Activer le contrôle sur accès**, cliquez sur **Configurer**.
5. Sur l'onglet **Exclusions Windows**, cliquez soit sur **Exporter**, soit sur **Importer**.

7.1.3 Contrôles à la demande et planifié

Dans le volet **Contrôle à la demande** de la stratégie **Antivirus et HIPS**, vous pouvez :

- Configurer des contrôles planifiés
- Configurer les options de contrôle telles que les extensions et les exclusions pour tous les types de contrôle à la demande et planifié, pour le contrôle intégral du système et pour les contrôles à la demande par défaut sur des ordinateurs individuels.

Création d'un contrôle planifié

Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - antivirus et HIPS** pour réaliser cette tâche.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Pour que Sophos Endpoint Security and Control contrôle certains ordinateurs à des heures définies, vous pouvez créer un contrôle planifié.

1. Vérifiez quelle stratégie antivirus et HIPS est utilisée par le(s) groupe(s) d'ordinateurs que vous voulez configurer.

   Retrouvez plus de renseignements à la section Vérification des stratégies utilisées par un groupe (page 27).
2. Dans le volet **Stratégies**, cliquez deux fois sur **Antivirus et HIPS**.
3. Cliquez deux fois sur la stratégie que vous désirez modifier.
   La boîte de dialogue **Stratégie antivirus et HIPS** apparaît.
4. Dans le volet **Contrôle à la demande**, sous **Paramétrer et gérer les contrôles planifiés**, cliquez sur **Ajouter**.
   La boîte de dialogue des **Paramètres du contrôle planifié** apparaît.
5. Dans la zone de texte **Nom du contrôle**, saisissez un nom de contrôle.
6. Sous **Éléments à contrôler**, sélectionnez les cases à cocher des éléments à contrôler. Par défaut, tous les disques durs locaux et systèmes de fichiers montés UNIX sont contrôlés.
7. Sous **Planification du contrôle**, sélectionnez les cases à cocher du ou des jours où le contrôle doit s'exécuter.
8. Pour indiquer l'heure à laquelle le contrôle doit s'exécuter, cliquez sur **Ajouter**.
   - Pour changer une heure, sélectionnez-la dans la liste **Heures d'exécution du contrôle**, puis cliquez sur **Modifier**.

- Pour supprimer une heure, sélectionnez-la dans la liste **Heures d'exécution du contrôle**, puis cliquez sur **Supprimer**.

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

Retrouvez plus de renseignements sur la modification des paramètres de contrôle et de nettoyage aux sections suivantes :

- Configuration des paramètres de contrôle pour un contrôle planifié (page 91)
- Paramétrage du nettoyage automatique pour le contrôle sur accès (page 86)

Configuration des paramètres de contrôle pour un contrôle planifié

Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - antivirus et HIPS** pour réaliser cette tâche.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Pour configurer les paramètres de contrôle pour un contrôle planifié :

1. Vérifiez quelle stratégie antivirus et HIPS est utilisée par le(s) groupe(s) d'ordinateurs que vous voulez configurer.

   Retrouvez plus de renseignements à la section Vérification des stratégies utilisées par un groupe (page 27).
2. Dans le volet **Stratégies**, cliquez deux fois sur **Antivirus et HIPS**.
3. Cliquez deux fois sur la stratégie que vous désirez modifier.
   La boîte de dialogue **Stratégie antivirus et HIPS** apparaît.
4. Dans la liste **Configurer et gérer les contrôles planifiés**, sélectionnez le contrôle, puis cliquez sur **Modifier**.
5. Dans la boîte de dialogue **Paramètres du contrôle planifié**, cliquez sur **Configurer**.
6. Sous **Contrôler les fichiers à la recherche de**, configurez les paramètres comme décrit ci-dessous.

Option	Description
Adwares et PUA	• Un adware affiche de la publicité (par exemple, des messages intempestifs), qui affecte la productivité des utilisateurs et les performances du système. • Une application potentiellement indésirable ou PUA (Potentially Unwanted Application) n'est pas malveillante mais sa présence sur les réseaux d'entreprise est généralement considérée comme inappropriée.

Option	Description
Fichiers suspects	Les fichiers suspects affichent certaines caractéristiques (par exemple, du code de décompression dynamique) qui sont fréquemment, mais pas exclusivement, trouvées dans les malwares. Par contre, ces caractéristiques ne sont pas suffisamment solides pour que le fichier soit identifié comme un nouvel élément de malware. **Remarque** Ce paramètre s'applique uniquement à Sophos Endpoint Security and Control pour Windows.
Rootkits	Un rootkit est un cheval de Troie ou une technologie utilisée pour dissimuler la présence d'un objet malveillant (processus, fichier, clé de registre ou port réseau) à l'utilisateur de l'ordinateur ou à l'administrateur.

7. Sous **Autres options de contrôle**, paramétrez les options comme décrit ci-dessous.

Option	Description
Contrôler dans les fichiers archive	Contrôle le contenu des archives et des autres fichiers compressés. Nous déconseillons le contrôle dans les fichiers archives lors d'un contrôle planifié, car cette opération rallonge énormément le temps de contrôle. Nous vous conseillons plutôt d'utiliser le contrôle sur accès (en lecture et en écriture) pour protéger votre réseau. Tous les composants de malware d'une archive décompressée seront bloqués par les utilitaires de contrôle en lecture et en écriture au moment de leur accès. Si vous voulez contrôler toutes les archives sur quelques ordinateurs à l'aide d'un contrôle planifié, nous vous conseillons de procéder comme suit : • Créez un contrôle planifié supplémentaire. • Dans la boîte de dialogue **Configurer > Paramètres du contrôle à la demande**, sur l'onglet **Extensions**, ajoutez uniquement les extensions de fichiers à la liste des extensions à contrôler. • Assurez-vous que **Contrôler tous les fichiers** est désactivé.

Option	Description
	Vous pourrez ainsi contrôler les fichiers archive tout en réduisant au maximum la durée du contrôle.
Contrôler la mémoire système	Détectez les programmes malveillants cachés dans la mémoire système de l'ordinateur (la mémoire utilisée par le système d'exploitation).
Exécuter le contrôle avec une priorité inférieure	Sous Windows Vista et supérieur, exécutez le contrôle planifié avec une priorité plus faible afin que l'impact soit minimal sur les applications de l'utilisateur.

Retrouvez plus de conseils sur le réglage des paramètres de contrôle par défaut dans l'article 63985 de la base de connaissances Sophos.

Paramétrage du nettoyage automatique pour le contrôle planifié

Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - antivirus et HIPS** pour réaliser cette tâche.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Par défaut, Sophos Endpoint Security and Control nettoie automatiquement les ordinateurs dès la découverte d'un virus ou de toute autre menace. Vous pouvez changer les paramètres du nettoyage automatique comme décrit ci-dessous.

1. Vérifiez quelle stratégie antivirus et HIPS est utilisée par le(s) groupe(s) d'ordinateurs que vous voulez configurer.

   Retrouvez plus de renseignements à la section Vérification des stratégies utilisées par un groupe (page 27).
2. Dans le volet **Stratégies**, cliquez deux fois sur **Antivirus et HIPS**.
3. Cliquez deux fois sur la stratégie que vous désirez modifier.
   La boîte de dialogue **Stratégie antivirus et HIPS** apparaît.
4. Dans la liste **Configurer et gérer les contrôles planifiés**, sélectionnez le contrôle, puis cliquez sur **Modifier**.
5. Près de **Changer les paramètres de contrôle et de nettoyage**, cliquez sur **Configurer**.
   La boîte de dialogue **Paramètres de contrôle et de nettoyage** apparaît.
6. Cliquez sur l'onglet **Nettoyage**.
7. Configurez les options comme indiqué à la section Paramètres de nettoyage automatique pour le contrôle sur accès (page 86).

Paramètres de nettoyage automatique pour le contrôle planifié

Virus/spywares

Sélectionnez ou dessélectionnez la case à cocher **Nettoyer automatiquement les éléments contenant un virus/spyware**.

Vous pouvez aussi spécifier ce que vous souhaitez faire des éléments en cas d'échec du nettoyage :

- **Consigner dans le journal uniquement**
- **Supprimer**
- **Déplacer dans l'emplacement par défaut**
- **Déplacer dans (saisir un chemin UNC complet)**

Remarques

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

Adwares et PUA

Sélectionnez **Nettoyer automatiquement les adwares et les PUA**.

Remarque

- Ce paramètre s'applique uniquement aux ordinateurs Windows.

Fichiers suspects

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

- **Consigner dans le journal uniquement**
- **Supprimer**
- **Déplacer dans l'emplacement par défaut**
- **Déplacer dans (saisir un chemin UNC complet)**

Remarques

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

Extensions de fichier pour les contrôles à la demande et planifié

Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - antivirus et HIPS** pour réaliser cette tâche.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Vous pouvez indiquer les extensions de fichier à contrôler au cours des contrôles à la demande et planifiés.

1. Vérifiez quelle stratégie antivirus et HIPS est utilisée par le(s) groupe(s) d'ordinateurs que vous voulez configurer.

   Retrouvez plus de renseignements à la section Vérification des stratégies utilisées par un groupe (page 27).
2. Dans le volet **Stratégies**, cliquez deux fois sur **Antivirus et HIPS**.
3. Cliquez deux fois sur la stratégie que vous désirez modifier.
   La boîte de dialogue **Stratégie antivirus et HIPS** apparaît.
4. Dans le volet **Contrôle à la demande**, cliquez sur **Configurer**.
   La boîte de dialogue **Paramètres du contrôle à la demande** apparaît.
5. Sur l'onglet **Extensions**, configurez les options comme décrit ci-dessous :

Option	Description
Contrôler tous les fichiers	Contrôlez tous les fichiers quelle que soit l'extension du fichier. Si vous activez cette option, les autres options de l'onglet **Extensions** sont désactivées. Le contrôle de tous les fichiers affecte les performances de l'ordinateur, nous vous conseillons donc d'activer cette option seulement dans le cadre d'un contrôle planifié hebdomadaire.
Contrôler uniquement les exécutables et autres fichiers vulnérables	• Vérifiez tous les fichiers avec des extensions d'exécutables (par exemple, .exe, .bat, .pif) ou les fichiers qui sont susceptibles d'être infectés (par exemple, .doc, .chm, .pdf). • Vérifiez rapidement la structure de tous les fichiers, puis contrôlez-les si leur format est celui d'un fichier exécutable.
Extensions des types de fichiers supplémentaires à contrôler	Pour contrôler des types de fichiers supplémentaires, cliquez sur **Ajouter**, puis saisissez l'extension du fichier, par exemple PDF, dans le champ **Extension**. Vous pouvez utiliser le caractère ? pour remplacer tout caractère. Pour arrêter le contrôle d'un type de fichier, sélectionnez son extension dans la liste, puis cliquez sur **Supprimer**. Pour changer un type de fichier, sélectionnez son extension dans la liste, puis cliquez sur **Modifier**.
Contrôler les fichiers sans extension	Les fichiers sans extension peuvent être du malware, nous vous conseillons donc de laisser cette option activée.

Option	Description
Exclure	Pour exclure des types de fichiers spécifiques du contrôle planifié, cliquez sur **Ajouter**, puis saisissez l'extension du fichier, par exemple PDF, dans le champ **Extension**. Pour démarrer le contrôle d'un type de fichier, sélectionnez son extension dans la liste, puis cliquez sur **Supprimer**. Pour changer un type de fichier, sélectionnez son extension dans la liste, puis cliquez sur **Renommer**.

Retrouvez plus de conseils sur la configuration des paramètres d'extension pour le contrôle planifié dans l'article 63985 de la base de connaissances Sophos.

Exclusion d'éléments des contrôles à la demande et planifié

Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - antivirus et HIPS** pour réaliser cette tâche.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Vous pouvez exclure des éléments des contrôles à la demande et planifié.

Remarque
Les paramètres des « éléments exclus » des contrôles planifiés s'appliquent aussi aux contrôles intégraux du système exécutés depuis la console et aux contrôles « Contrôler cet ordinateur » exécutés sur les ordinateurs en réseau. Retrouvez plus de renseignements à la section Contrôle immédiat des ordinateurs (page 54).

1. Vérifiez quelle stratégie antivirus et HIPS est utilisée par le(s) groupe(s) d'ordinateurs que vous voulez configurer.

   Retrouvez plus de renseignements à la section Vérification des stratégies utilisées par un groupe (page 27).
2. Dans le volet **Stratégies**, cliquez deux fois sur **Antivirus et HIPS**. Puis cliquez deux fois sur la stratégie que vous désirez changer.
3. La boîte de dialogue **Stratégie antivirus et HIPS** apparaît. Dans le volet **Contrôle à la demande**, cliquez sur **Configurer**.
4. Cliquez sur l'onglet **Exclusions Windows**, **Exclusions Linux/UNIX** ou **Exclusions Mac**. Pour ajouter des éléments dans la liste, cliquez sur **Ajouter** et saisissez le chemin complet dans la boîte de dialogue **Exclusion d'un élément**.

   Les éléments que vous pouvez exclure du contrôle diffèrent selon chaque type d'ordinateur. Retrouvez plus de renseignements à la section Éléments pouvant être exclus du contrôle (page 107).

Vous pouvez exporter la liste des exclusions Windows dans un fichier, puis l'importer dans une autre stratégie. Retrouvez plus de renseignements à la section Importation ou exportation des exclusions du contrôle sur accès (page 89).

Importation ou exportation des exclusions Windows pour les contrôles à la demande et planifié

Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - antivirus et HIPS** pour réaliser cette tâche.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Vous pouvez exporter la liste des exclusions Windows pour les contrôles à la demande et planifié dans un fichier, puis l'importer dans une autre stratégie.

1. Vérifiez quelle stratégie antivirus et HIPS est utilisée par le(s) groupe(s) d'ordinateurs que vous voulez configurer.

   Retrouvez plus de renseignements à la section Vérification des stratégies utilisées par un groupe (page 27).
2. Dans le volet **Stratégies**, cliquez deux fois sur **Antivirus et HIPS**.
3. Cliquez deux fois sur la stratégie que vous désirez modifier.
   La boîte de dialogue **Stratégie antivirus et HIPS** apparaît.
4. Dans le volet **Contrôle à la demande**, cliquez sur **Configurer**.
5. Sur l'onglet **Exclusions Windows**, cliquez soit sur **Exporter**, soit sur **Importer**.

7.1.4 Surveillance des comportements

Dans le cadre du contrôle sur accès, la surveillance des comportements Sophos assure la protection des ordinateurs Windows contre les menaces du jour zéro ou non identifiées et contre les comportements suspects.

La détection à l'exécution (runtime) intercepte les menaces qui ne peuvent pas être détectées avant exécution. La surveillance des comportements utilise les méthodes de détection à l'exécution (runtime) suivantes pour intercepter les menaces :

- Détection des comportements malveillants et suspects
- Détection du trafic malveillant
- Détection des dépassements de la mémoire tampon

Détection des comportements malveillants et suspects

La détection des comportements suspects utilise le système de prévention d'intrusion sur l'hôte (HIPS) de Sophos et effectue une analyse dynamique du comportement de tous les programmes en cours d'exécution sur l'ordinateur pour détecter et bloquer toute activité qui semble malveillante. Un comportement suspect peut inclure des changements apportés au registre qui pourrait entraîner l'exécution automatique d'un virus lors du redémarrage de l'ordinateur.

La détection des comportements suspects surveille tous les processus système à la recherche de signes d'activité de programmes malveillants comme l'écriture suspecte dans le registre ou des actions suspectes de copie de fichiers. Elle peut être paramétrée pour avertir l'administrateur et/ou bloquer le processus.

La détection des comportements malveillants procède à une analyse dynamique de tous les programmes fonctionnant sur l'ordinateur pour détecter et bloquer toute activité qui semble malveillante.

Détection du trafic malveillant

La détection du trafic malveillant détecte les communications entre les terminaux et les serveurs de commande et de contrôle impliqués dans des attaques par botnet ou par autre programme malveillant.

Remarque
Sophos Live Protection doit être activé pour pouvoir utiliser la détection du trafic malveillant afin de rechercher et de récupérer les données les plus récentes. (Sophos Live Protection est activé par défaut).

Détection des dépassements de la mémoire tampon

La détection des dépassements de la mémoire tampon est importante pour traiter les exploits du jour zéro.

Elle procède à une analyse dynamique du comportement de tous les programmes s'exécutant sur le système afin de détecter toute tentative d'attaque par saturation de la mémoire tampon sur des processus en cours d'exécution. Elle intercepte les attaques ciblant les vulnérabilités de sécurité à la fois dans les logiciels et dans les applications des systèmes d'exploitation.

Activation ou désactivation de la surveillance des comportements

Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - antivirus et HIPS** pour réaliser cette tâche.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Par défaut, la surveillance des comportements est activée.

Pour activer ou désactiver la surveillance des comportements :

1. Vérifiez quelle stratégie antivirus et HIPS est utilisée par le ou les groupes d'ordinateurs que vous voulez configurer.

   Retrouvez plus de renseignements à la section Vérification des stratégies utilisées par un groupe (page 27).
2. Dans le volet **Stratégies**, cliquez deux fois sur **Antivirus et HIPS**.
3. Cliquez deux fois sur la stratégie que vous désirez modifier.
   La boîte de dialogue **Stratégie antivirus et HIPS** apparaît.
4. Dans le volet **Contrôle sur accès**, sélectionnez ou dessélectionnez la case à cocher **Activer la surveillance des comportements**.

Détection des comportements malveillants

Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - antivirus et HIPS** pour réaliser cette tâche.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

La détection des comportements malveillants est l'analyse dynamique de tous les programmes fonctionnant sur l'ordinateur pour détecter et bloquer toute activité qui semble malveillante.

Par défaut, la détection des comportements malveillants est activée.

Pour changer les paramètres de détection et de signalement des comportements malveillants :

1. Vérifiez quelle stratégie antivirus et HIPS est utilisée par le ou les groupes d'ordinateurs que vous voulez configurer.

   Retrouvez plus de renseignements à la section Vérification des stratégies utilisées par un groupe (page 27).
2. Dans le volet **Stratégies**, cliquez deux fois sur **Antivirus et HIPS**.
3. Cliquez deux fois sur la stratégie que vous désirez modifier.
   La boîte de dialogue **Stratégie antivirus et HIPS** apparaît.
4. Dans le volet **Contrôle sur accès**, assurez-vous que la case à cocher **Activer la surveillance des comportements** est sélectionnée.
5. À côté de **Activer la surveillance des comportements**, cliquez sur **Configurer**.
6. Dans la boîte de dialogue **Configuration de la surveillance des comportements** :
   - Pour alerter l'administrateur et bloquer les comportements malveillants, sélectionnez la case **Détecter les comportements malveillants**.
   - Pour désactiver la détection des comportements malveillants, dessélectionnez la case à cocher **Détecter les comportements malveillants**.

   Remarque
   Si vous désactivez la détection des comportements malveillants, la détection des comportements suspects sera également désactivée. Veuillez noter que la détection du trafic malveillant ne sera **pas** désactivée.

Détection du trafic malveillant

Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - antivirus et HIPS** pour réaliser cette tâche.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

  Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).
- Sophos Live Protection doit être activé pour pouvoir utiliser la détection du trafic malveillant. (Sophos Live Protection est activé par défaut).

La détection du trafic malveillant détecte les communications entre les terminaux et les serveurs de commande et de contrôle impliqués dans des attaques par botnet ou par autre programme malveillant.

Remarque
La détection du trafic malveillant utilise la même série d'exclusions que le contrôle sur accès de Sophos Anti-Virus (InterCheck ™). Retrouvez plus de renseignements sur la configuration des exclusions du contrôle sur accès à la section Exclusion d'éléments du contrôle sur accès (page 88).

Par défaut, la détection du trafic malveillant est activée pour les nouvelles installations de Enterprise Console à partir de la version 5.3. Si vous avez procédé à la mise à niveau vers une version antérieure de Enterprise Console, vous allez devoir activer la détection du trafic malveillant afin de bénéficier de cette fonction.

Pour changer les paramètres de détection du trafic malveillant :

1. Vérifiez quelle stratégie antivirus et HIPS est utilisée par le ou les groupes d'ordinateurs que vous voulez configurer.

   Retrouvez plus de renseignements à la section Vérification des stratégies utilisées par un groupe (page 27).
2. Dans le volet **Stratégies**, cliquez deux fois sur **Antivirus et HIPS**.
3. Cliquez deux fois sur la stratégie que vous désirez modifier.
   La boîte de dialogue **Stratégie antivirus et HIPS** apparaît.
4. Dans le volet **Contrôle sur accès**, assurez-vous que la case à cocher **Activer la surveillance des comportements** est sélectionnée.
5. À côté de **Activer la surveillance des comportements**, cliquez sur **Configurer**.
6. Dans la boîte de dialogue **Configuration de la surveillance des comportements**, assurez-vous que la case **Détecter les comportements malveillants** est sélectionnée.
7. Pour activer ou désactiver la détection du trafic malveillant, sélectionnez ou dessélectionnez la case **Détecter le trafic malveillant**.

Détection des comportements suspects

Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - antivirus et HIPS** pour réaliser cette tâche.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

La détection des comportements suspects surveille tous les processus système à la recherche de signes d'activité de programmes malveillants comme l'écriture suspecte dans le registre ou des actions suspectes de copie de fichiers. Elle peut être paramétrée pour avertir l'administrateur et/ou bloquer le processus.

Par défaut, les comportements malveillants sont détectés et signalés. En revanche, ils ne sont pas bloqués.

Pour changer les paramètres de détection et de signalement des comportements suspects :

1. Vérifiez quelle stratégie antivirus et HIPS est utilisée par le ou les groupes d'ordinateurs que vous voulez configurer.

   Retrouvez plus de renseignements à la section Vérification des stratégies utilisées par un groupe (page 27).
2. Dans le volet **Stratégies**, cliquez deux fois sur **Antivirus et HIPS**.
3. Cliquez deux fois sur la stratégie que vous désirez modifier.
   La boîte de dialogue **Stratégie antivirus et HIPS** apparaît.

4. Dans le volet **Contrôle sur accès**, assurez-vous que la case à cocher **Activer la surveillance des comportements** est sélectionnée.
5. À côté de **Activer la surveillance des comportements**, cliquez sur **Configurer**.
6. Dans la boîte de dialogue **Configuration de la surveillance des comportements**, assurez-vous que la case **Détecter les comportements malveillants** est sélectionnée.
   - Pour alerter l'administrateur et bloquer les processus suspects, sélectionnez la case à cocher **Détecter les comportements suspects** et dessélectionnez la case à cocher **Alerter uniquement, ne pas bloquer les comportements suspects**.
   - Pour alerter l'administrateur sans bloquer les processus suspects, sélectionnez les cases à cocher **Détecter les comportements suspects** et **Alerter uniquement, ne pas bloquer les comportements suspects**.

Pour une protection renforcée, nous vous conseillons d'activer la détection des fichiers suspects. Retrouvez plus de renseignements à la section Configuration du contrôle sur accès (page 83).

Détection des dépassements de la mémoire tampon

Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - antivirus et HIPS** pour réaliser cette tâche.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

La détection des dépassements de la mémoire tampon procède à une analyse dynamique du comportement de tous les programmes s'exécutant sur le système afin de détecter toute tentative d'attaque par saturation de la mémoire tampon sur des processus en cours d'exécution.

Par défaut, les dépassements de la mémoire tampon sont détectés et bloqués.

Pour changer les paramètres de détection et de signalement des attaques par dépassement de la mémoire tampon :

1. Vérifiez quelle stratégie antivirus et HIPS est utilisée par le ou les groupes d'ordinateurs que vous voulez configurer.

   Retrouvez plus de renseignements à la section Vérification des stratégies utilisées par un groupe (page 27).
2. Dans le volet **Stratégies**, cliquez deux fois sur **Antivirus et HIPS**.
3. Cliquez deux fois sur la stratégie que vous désirez modifier.
   La boîte de dialogue **Stratégie antivirus et HIPS** apparaît.
4. Dans le volet **Contrôle sur accès**, assurez-vous que la case à cocher **Activer la surveillance des comportements** est sélectionnée.
5. À côté de **Activer la surveillance des comportements**, cliquez sur **Configurer**. Dans la boîte de dialogue **Configuration de la surveillance des comportements** :
   - Pour alerter l'administrateur et bloquer les dépassements de la mémoire tampon, sélectionnez la case à cocher **Détecter les dépassements de mémoire tampon** et dessélectionnez la case à cocher **Alerter uniquement, ne pas bloquer**.
   - Pour alerter l'administrateur sans bloquer les dépassements de la mémoire tampon, sélectionnez les deux cases à cocher **Détecter les dépassements de mémoire tampon** et **Alerter uniquement, ne pas bloquer**.

7.1.5 Sophos Live Protection

Sophos Live Protection utilise la technologie Cloud pour décider instantanément si un fichier suspect est une menace et prendre les mesures spécifiées dans la stratégie antivirus et HIPS.

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

Pour une utilisation optimale de Sophos Live Protection, assurez-vous que les options suivantes sont activées.

- **Activer Sophos Live Protection**

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

  Important
  Les fonctions de Détection du trafic malveillant et de Réputation des téléchargements nécessite l'activation de Sophos Live Protection afin de pouvoir effectuer des recherches instantanées dans la base de données en ligne des SophosLabs et récupérer les données les plus récentes sur les menaces ou sur la réputation des téléchargements.

- **Activer Sophos Live Protection pour le contrôle à la demande**

  Si vous voulez que les contrôles sur accès utilisent la même vérification dans le Cloud que le contrôle sur accès, veuillez sélectionner cette option.

- **Envoyer automatiquement des fichiers échantillons à Sophos**

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

  L'envoi d'échantillons de fichiers aide Sophos à améliorer en permanence la détection des malwares sans aucun risque de faux positifs.

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

Important
Vous devez vous assurer que le domaine Sophos auquel les données des fichiers sont envoyées est fiable dans votre solution de filtrage web. Retrouvez plus de renseignements dans l'article 62637 de la base de connaissances du support (http://www.sophos.com/fr-fr/support/knowledgebase/62637.aspx).

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

Activation ou désactivation de Sophos Live Protection

Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - antivirus et HIPS** pour réaliser cette tâche.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Sophos Live Protection vérifie les fichiers suspects en les comparant aux informations les plus récentes fournies par la base de données des SophosLabs.

Par défaut, Sophos Live Protection envoie des données de fichiers telles que les sommes de contrôle à Sophos, mais n'envoie pas d'échantillons de fichiers. Pour une utilisation optimale de Sophos Live Protection, veuillez sélectionner l'option d'envoi d'échantillons de fichiers.

Pour activer ou désactiver les options de Sophos Live Protection :

1. Vérifiez quelle stratégie antivirus et HIPS est utilisée par le ou les groupes d'ordinateurs que vous voulez configurer.

   Retrouvez plus de renseignements à la section Vérification des stratégies utilisées par un groupe (page 27).
2. Dans le volet **Stratégies**, cliquez deux fois sur **Antivirus et HIPS**. Puis cliquez deux fois sur la stratégie que vous désirez changer.
3. Dans la boîte de dialogue **Stratégie antivirus et HIPS**, cliquez sur le bouton **Sophos Live Protection**.
4. Dans la boîte de dialogue **Sophos Live Protection** :
   - Sélectionnez ou dessélectionnez la case **Activer Sophos Live Protection**. Cette opération active ou désactive Sophos Live Protection lors du lancement du contrôle sur accès.

     Important
     Les fonctions de Détection du trafic malveillant et de Réputation des téléchargements nécessite l'activation de Sophos Live Protection afin de pouvoir effectuer des recherches instantanées dans la base de données en ligne des SophosLabs et récupérer les données les plus récentes sur les menaces ou sur la réputation des téléchargements.

   - Sélectionnez ou dessélectionnez la case **Activer Sophos Live Protection pour le contrôle à la demande**. Cette opération active ou désactive Sophos Live Protection lors du lancement de contrôles à la demande.
   - Sélectionnez ou dessélectionnez la case **Envoyer automatiquement les échantillons de fichiers à Sophos**.

     Les échantillons peuvent uniquement être envoyés lorsque Sophos Live Protection est activée.

Remarque
Lorsqu'un échantillon de fichier est envoyé à Sophos en vue d'un contrôle en ligne, les données de fichiers (somme de contrôle, etc...) sont toujours envoyées avec l'échantillon.

7.1.6 Protection Web

La protection Web offre une protection renforcée contre les menaces provenant du Web. Il offre les fonctions suivantes :

- Filtrage instantané d'URL
- Contrôle du contenu téléchargé
- Vérification de la réputation des fichiers téléchargés

Filtrage instantané d'URL

Le filtrage instantané d'URL bloque l'accès aux sites Web réputés pour héberger des malwares. Cette fonction consulte en temps réel la base de données en ligne de Sophos répertoriant les sites Web infectés.

Remarque
Si vous voulez avoir plus de contrôle sur les sites Web auxquels les utilisateurs ont la permission d'accéder, par exemple, si vous voulez empêcher les utilisateurs de visiter des sites Web à propos desquels votre entreprise pourrait être légalement responsable, utilisez la fonctionnalité de contrôle du Web. Retrouvez plus de renseignements à la section Stratégie de contrôle du Web (page 178).

Contrôle du contenu

Le contrôle du contenu effectue le contrôle des données et des fichiers téléchargés à partir d'Internet (ou d'intranet) et détecte de manière proactive le contenu malveillant. Cette fonction contrôle le contenu, quel que soit l'emplacement où il est hébergé, notamment les emplacements qui ne figurent pas dans la base de données des sites Web infectés.

Réputation des téléchargements

La réputation des téléchargements est calculée en fonction de l'ancienneté, de la source, de la prévalence, de l'analyse détaillée et d'autres caractéristiques du fichier.

Remarque
La réputation des téléchargements est uniquement prise en charge sur Windows 7 et version supérieure.

Par défaut, une alerte s'affiche lorsque vous tentez de télécharger un fichier de mauvaise réputation ou inconnu. Nous déconseillons le téléchargement de ce genre de fichiers. Si la source et l'éditeur de ce fichier sont fiables, vous pouvez choisir de télécharger le fichier. Cette action et l'URL du fichier seront consignées dans le journal du contrôle.

Remarque
La réputation des téléchargements est calculée en fonction des données de la base de données Cloud des SophosLabs et nécessite l'activation de Sophos Live Protection pour pouvoir effectuer les consultations et obtenir les données. (Sophos Live Protection est activé par défaut).

Retrouvez plus de renseignements sur la réputation des téléchargements dans l'article 121319 de la base de connaissances.

Paramètres de configuration de la protection Web

La protection Web est activée par défaut : l'accès aux sites Web malveillants est bloqué, le contenu téléchargé est contrôlé et la réputation des fichiers téléchargés est vérifiée.

Retrouvez plus de renseignements sur les paramètres de la protection Web et sur leur modification à la section Configuration des options de protection Web (page 105).

Navigateurs Web pris en charge

La protection Web est compatible avec les navigateurs Web suivants :

- Internet Explorer
- Edge
- Google Chrome
- Firefox (hormis la réputation des téléchargements)
- Safari (hormis la réputation des téléchargements)
- Opera

Le contenu Web accédé via un navigateur non compatible n'est pas filtré et ne sera pas bloqué.

Événements de protection Web

Lorsque l'accès à un site malveillant est bloqué, un événement journalisé est visible dans l'Observateur d'événements Web et dans les **Détails de l'ordinateur** du terminal où s'est produit l'événement. Si vous utilisez la fonctionnalité de contrôle du Web, les événements de protection Web et de contrôle du Web apparaissent dans l'Observateur d'événements Web et dans les **Détails de l'ordinateur**. Retrouvez plus de renseignements aux sections Affichage des événements Web (page 208) et Affichage des derniers événements Web sur un ordinateur (page 209).

Configuration des options de protection Web

Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - antivirus et HIPS** pour réaliser cette tâche.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Pour activer ou désactiver la protection Web :

1. Vérifiez quelle stratégie antivirus et HIPS est utilisée par le ou les groupes d'ordinateurs que vous voulez configurer.

   Retrouvez plus de renseignements à la section Vérification des stratégies utilisées par un groupe (page 27).
2. Dans le volet **Stratégies**, cliquez deux fois sur **Antivirus et HIPS**.
3. Cliquez deux fois sur la stratégie que vous désirez modifier.
4. Dans la boîte de dialogue de la **Stratégie antivirus et HIPS**, cliquez sur le bouton **Protection Web**.
5. Dans la boîte de dialogue **Protection Web**, sous **Protection antimalwares**, près du champ **Bloquer l'accès aux sites Web malveillants**, sélectionnez **Activé** ou **Désactivé** pour bloquer ou débloquer l'accès aux sites Web malveillants. Cette option est activée par défaut.
   Retrouvez plus de renseignements sur l'autorisation des sites Web spécifiques à la section Autorisation de sites Web (page 114).
6. Pour activer ou désactiver le contrôle des données et des fichiers téléchargés, sélectionnez **Avec le contrôle sur accès**, **Actif** ou **Inactif** dans le menu déroulant du champ **Contrôle du contenu**.

   L'option **Avec le contrôle sur accès** est sélectionnée par défaut, ce qui signifie que le contrôle du contenu est désactivé ou activé simultanément avec le contrôle sur accès.
7. Pour modifier les actions à prendre lorsqu'un utilisateur tente de télécharger un fichier de mauvaise réputation ou inconnu, sous **Réputation des téléchargements**, sélectionnez soit **Demander à l'utilisateur** (par défaut) soit **Journaliser uniquement** dans le menu déroulant du champ **Action**.

   Remarque
   Sophos Live Protection doit être activé pour pouvoir utiliser la réputation des téléchargements. (Sophos Live Protection est activé par défaut).

   - Si vous sélectionnez **Demander à l'utilisateur**, une alerte s'affichera à chaque fois qu'un utilisateur tentera de télécharger un fichier de mauvaise réputation pour l'avertir et lui demander s'il souhaite bloquer ou autoriser le téléchargement. Nous déconseillons aux utilisateurs de télécharger ce genre de fichiers. S'ils considèrent la source et l'éditeur du fichier fiables, ils peuvent choisir de télécharger le fichier. Votre décision de bloquer ou d'autoriser le téléchargement ainsi que l'URL du fichier sera consignée en tant qu'événement Web dans le journal du contrôle de Enterprise Console.
   - Si vous sélectionnez **Journaliser uniquement**, aucune alerte ne sera affichée. Le téléchargement sera autorisé et consigné en tant qu'événement Web dans le journal du contrôle de Enterprise Console.
8. Pour choisir le niveau de sévérité du contrôle de réputation, sélectionnez **Conseillé** (par défaut) ou **Strict** dans le menu déroulant du champ **Niveau**.
   - Si vous sélectionnez **Conseillé**, une alerte s'affichera et/ou un enregistrement et un événement seront consignés dans le journal à chaque fois qu'un utilisateur essaiera de télécharger un fichier de mauvaise réputation ou inconnu.
   - Si vous sélectionnez **Strict**, une alerte s'affichera et/ou un enregistrement et un événement seront consignés dans le journal à chaque fois qu'un utilisateur essaiera de télécharger un fichier de mauvaise ou moyenne réputation ou inconnu.

7.1.7 Types de fichiers et exclusions contrôlés

Par défaut, Sophos Endpoint Security and Control contrôle les types de fichiers vulnérables aux virus. Les types de fichiers qui sont contrôlés par défaut non seulement diffèrent d'un système d'exploitation à l'autre, mais changent aussi au fur et à mesure de la mise à jour du produit.

Pour consulter une liste des types de fichiers qui sont contrôlés par défaut, rendez-vous sur un ordinateur possédant le système d'exploitation approprié, ouvrez la fenêtre Sophos Endpoint Security and Control ou Sophos Anti-Virus et recherchez la page de configuration des extensions.

Vous pouvez aussi choisir de contrôler des types de fichiers supplémentaires ou exempter certains types de fichiers du contrôle.

Windows

Pour voir une liste des types de fichiers contrôlés par défaut sur un ordinateur Windows :

1. Ouvrez Sophos Endpoint Security and Control.
2. Sous **Antivirus et HIPS**, cliquez sur **Configurer l'antivirus et HIPS**, puis cliquez sur **Extensions et exclusions à la demande**.

Retrouvez plus de renseignements sur le contrôle des types de fichiers supplémentaires ou sur l'exemption de certains types de fichiers du contrôle sur un ordinateur Windows aux sections suivantes :

- Extensions de fichier pour le contrôle sur accès (page 87)
- Extensions de fichier pour les contrôles à la demande et planifié (page 94)

Mac OS X

Sophos Anti-Virus pour Mac OS X contrôle toutes les extensions de fichier pendant le contrôle sur accès. Retrouvez plus de renseignements sur la modification des paramètres du contrôle planifié à la section Extensions de fichier pour les contrôles à la demande et planifié (page 94).

Linux ou UNIX

Pour apporter des changements sur un ordinateur Linux, utilisez les commandes `savconfig` et `savscan` conformément aux instructions du *Guide de configuration de Sophos Anti-Virus pour Linux*.

Pour apporter des changements sur un ordinateur UNIX, utilisez la commande `savscan` conformément aux instructions du *Guide de configuration de Sophos Anti-Virus pour UNIX*.

Éléments pouvant être exclus du contrôle

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

Windows

Sous Windows, vous pouvez exclure des lecteurs, des dossiers, les fichiers et les processus.

Vous pouvez utiliser les caractères de remplacement * et ?

Le caractère de remplacement ? peut seulement être utilisé dans un nom ou dans une extension de fichier. Il permet généralement de retrouver n'importe quel caractère. En revanche, lorsqu'il est utilisé à la fin d'un nom de fichier ou d'une extension, il ne retrouve que les caractères uniques ou n'en retrouve pas. Par exemple, fichier??.txt permet de retrouver fichier.txt, fichier1.txt et fichier12.txt, mais pas fichier123.txt.

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

Mac OS X

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

Vous pouvez spécifier quels éléments sont exclus en préfixant ou suffixant l'exclusion avec une barre oblique ou en la suffixant avec une double barre oblique.

Retrouvez plus de renseignements dans l'*Aide de Sophos Anti-Virus pour Mac OS X*.

Linux ou UNIX

Sous Linux et UNIX, vous pouvez exclure des répertoires et des fichiers.

Vous pouvez spécifier n'importe quel chemin POSIX, qu'il s'agisse d'un fichier ou d'un répertoire, par exemple, /dossier/fichier. Vous pouvez utiliser les caractères de remplacement ? et *.

Remarque
L'Enterprise Console prend uniquement en charge les exclusions Linux et UNIX basées sur des chemins. Vous pouvez aussi configurer d'autres types d'exclusions directement sur des ordinateurs administrés. Ensuite, vous pouvez utiliser des expressions régulières et exclure des types de fichiers et des systèmes de fichiers. Retrouvez plus de renseignements sur la manière de procéder dans le *Guide de configuration de Sophos Anti-Virus pour Linux* ou dans le *Guide de configuration de Sophos Anti-Virus pour UNIX*.

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

Retrouvez plus de renseignements sur l'exclusion d'éléments du contrôle aux sections suivantes :

- Exclusion d'éléments du contrôle sur accès (page 88)
- Exclusion d'éléments des contrôles à la demande et planifié (page 96)

Spécification des exclusions de contrôle pour Windows

Conventions d'appellation standard

Sophos Anti-Virus valide les chemins et les noms de fichier des éléments d'exclusion du contrôle en les comparant aux conventions d'appellation standard de Windows. Par exemple, un nom de dossier peut contenir des espaces mais ne peut pas contenir ***uniquement*** des espaces.

Plusieurs extensions de fichier

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

`MonExemple.txt.doc` = nom de fichier `MonExemple.txt` + extension `.doc`.

Exclusion de fichiers, dossiers ou lecteurs spécifiques

Type d'exclusion	Description	Exemples	Commentaires

Fichier spécifique	Indiquez à la fois le chemin et le nom du fichier pour exclure un fichier spécifique. Le chemin peut inclure une lettre de lecteur ou un nom de partage réseau.	`C:\Documents \CV.doc`
		`\\Serveur \Utilisateurs \Documents \CV.doc`
			Pour vous assurer que les exclusions sont toujours appliquées correctement, ajoutez le fichier conforme au format 8.3 et les noms de dossier :
			`C:\Program Files \Sophos \Sophos Anti-Virus`
			`C: \Progra~1\Sophos \Sophos~1`
			Retrouvez plus de renseignements dans l'article 13045 de la base de connaissances.

Tous les fichiers du même nom	Indiquez un nom de fichier sans son chemin afin d'exclure tous les fichiers du même nom sur tout le système de fichiers.	`spacer.gif`	
Tout le contenu du lecteur ou du partage réseau	Indiquez une lettre de lecteur ou un nom de partage réseau pour exclure tout le contenu présent sur ce lecteur ou ce partage réseau.	`D:` `\\Serveur \<nom du partage>\`	Lorsque vous indiquez un partage réseau, veuillez inclure une barre oblique finale après le nom du partage.

Type d'exclusion	Description	Exemples	Commentaires
Dossier spécifique	Indiquez un chemin de dossier en incluant une lettre de lecteur ou un nom de partage réseau afin d'exclure tout le contenu de ce dossier et de ses sous-dossiers.	`D:\Outils\logs\`	Veuillez inclure une barre oblique finale après le nom du dossier.
Tous les dossiers du même nom	Indiquez un chemin de dossier sans aucune lettre de lecteur ou de nom de partage réseau afin d'exclure tout le contenu de ce dossier et de ses sous-dossiers sur *tous* les lecteurs ou partages réseau.	`\Outils\logs\` (exclut les dossiers suivants : `C:\Outils\logs\`, `\\Server\Outils\logs\`)	Vous devez indiquer le chemin complet jusqu'à la lettre du lecteur ou du nom de partage réseau. Dans cet exemple, la spécification simple de `\logs` n'exclut aucun fichier.

Caractères de remplacement

Vous pouvez utiliser les caractères de remplacement ? et *.

Utilisez le caractère ? dans un nom de fichier ou une extension pour remplacer un seul caractère.

À la fin d'un nom de fichier ou d'une extension, le caractère ? correspond à un caractère unique ou à aucun caractère. Par exemple, `fichier??.txt` permet de retrouver `fichier.txt`, `fichier1.txt` et `fichier12.txt`, mais pas `fichier123.txt`.

Utilisez le caractère * dans un nom de fichier ou une extension au format `[nom de fichier].*` ou `*.[extension]`:

Correct

`fichier.*`

`*.txt`

Incorrect

`fichier.txt*`

`fichier.*txt`

Il est également possible d'exclure les fichiers commençant par un nom de fichier spécifique ou avec une extension spécifique :

`fichier*.txt`

L'exemple ci-dessus exclut les fichiers suivants du contrôle :

`fichier.txt`

`fichier1.txt`

```
fichier12.txt
fichier.1.txt
fichier.12.txt
fichier12.12.txt
```

Les fichiers suivants ne sont pas exclus si l'exclusion définie ci-dessus est appliquée :

```
fichier.1txt
fichier.12txt
fichier.txt1
fichier.txt12
1fichier.txt
1fichier.txt1
```

7.1.8 Autorisation d'utilisation d'éléments

Autorisation des adwares et des PUA

Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - antivirus et HIPS** pour réaliser cette tâche.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Si vous avez activé Sophos Endpoint Security and Control pour détecter les adwares et autres applications potentiellement indésirables (PUA), vous risquez de ne pas pouvoir utiliser une application dont vous avez besoin.

Pour autoriser un adware ou une PUA :

1. Vérifiez quelle stratégie antivirus et HIPS est utilisée par le(s) groupe(s) d'ordinateurs que vous voulez configurer.

   Retrouvez plus de renseignements à la section Vérification des stratégies utilisées par un groupe (page 27).
2. Dans le volet **Stratégies**, cliquez deux fois sur **Antivirus et HIPS**.
3. Cliquez deux fois sur la stratégie que vous désirez modifier.
   La boîte de dialogue **Stratégie antivirus et HIPS** apparaît.
4. Cliquez sur **Autorisation**.
   La boîte de dialogue **Gestionnaire d'autorisation** apparaît.
5. Dans l'onglet **Adwares et PUA**, dans la liste **Adwares et PUA connus**, sélectionnez l'application que vous voulez autoriser.

   Si vous ne voyez pas l'application que vous voulez autoriser, vous pouvez l'ajouter vous-même dans la liste des adwares et des PUA connus. Retrouvez plus de renseignements sur la manière de procéder à la section Préautorisation des adwares et des PUA (page 112).
6. Cliquez sur **Ajouter**.

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

Préautorisation des adwares et des PUA

Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - antivirus et HIPS** pour réaliser cette tâche.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Si vous voulez autoriser l'utilisation d'une application que Sophos Endpoint Security and Control n'a pas encore classée comme adware ou comme PUA, vous pouvez la préautoriser en l'ajoutant vous-même à la liste des adwares et des PUA autorisés.

1. Rendez-vous sur la page **Adwares et PUA** du site Web de Sophos (http://www.sophos.com/fr-fr/threat-center/threat-analyses/adware-and-puas.aspx).
2. Recherchez, puis copiez le nom de l'application que vous voulez préautoriser.
3. Vérifiez quelle stratégie antivirus et HIPS est utilisée par le(s) groupe(s) d'ordinateurs que vous voulez configurer.

   Retrouvez plus de renseignements à la section Vérification des stratégies utilisées par un groupe (page 27).
4. Dans le volet **Stratégies**, cliquez deux fois sur **Antivirus et HIPS**.
5. Cliquez deux fois sur la stratégie que vous désirez modifier.
   La boîte de dialogue **Stratégie antivirus et HIPS** apparaît.
6. Cliquez sur **Autorisation**.
   La boîte de dialogue **Gestionnaire d'autorisation** apparaît.
7. Sur l'onglet **Adwares et PUA**, cliquez sur **Nouvelle entrée**.
8. Dans la boîte de dialogue **Ajout d'un nouvel adware ou PUA**, collez le nom de l'application que vous avez copié à l'étape 2.

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

Si vous vous êtes trompé ou voulez simplement supprimer une application du **Gestionnaire d'autorisation**, supprimez-la de la liste des adwares et des PUA connus :

1. Dans la liste **Adwares et PUA autorisés**, sélectionnez l'application.
2. Cliquez sur **Supprimer**.
3. Dans la liste **Adwares ou PUA connus**, sélectionnez l'application.
4. Cliquez sur **Supprimer**.

Blocage des adwares et des PUA autorisés

Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - antivirus et HIPS** pour réaliser cette tâche.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Pour empêcher l'exécution des adwares et des PUA actuellement autorisés sur les ordinateurs :

1. Vérifiez quelle stratégie antivirus et HIPS est utilisée par le(s) groupe(s) d'ordinateurs que vous voulez configurer.

Retrouvez plus de renseignements à la section Vérification des stratégies utilisées par un groupe (page 27).

2. Dans le volet **Stratégies**, cliquez deux fois sur **Antivirus et HIPS**. Puis cliquez deux fois sur la stratégie que vous désirez changer.
3. Dans la boîte de dialogue **Stratégie antivirus et HIPS**, cliquez sur le bouton **Autorisation**.
4. Dans l'onglet **Adwares ou PUA**, dans la liste **Adwares et PUA autorisés**, sélectionnez l'application que vous voulez bloquer.
5. Cliquez sur **Supprimer**.

Autorisation d'éléments suspects

Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - antivirus et HIPS** pour réaliser cette tâche.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

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

1. Vérifiez quelle stratégie antivirus et HIPS est utilisée par le ou les groupes d'ordinateurs que vous voulez configurer.

   Retrouvez plus de renseignements à la section Vérification des stratégies utilisées par un groupe (page 27).
2. Dans le volet **Stratégies**, cliquez deux fois sur **Antivirus et HIPS**.
3. Cliquez deux fois sur la stratégie que vous désirez modifier.
   La boîte de dialogue **Stratégie antivirus et HIPS** apparaît.
4. Cliquez sur **Autorisation**.
   La boîte de dialogue **Gestionnaire d'autorisation** apparaît.
5. Cliquez sur l'onglet correspondant au type de comportement qui a été détecté.

   Dans cet exemple, nous utiliserons **Dépassement de la mémoire tampon**.
6. Dans la liste **Applications connues**, sélectionnez l'application que vous voulez autoriser.

   Si vous voyez pas l'application que vous voulez autoriser, vous pouvez l'ajouter vous-même dans la liste des applications autorisées. Retrouvez plus de renseignements sur la manière de procéder à la section Préautorisation des adwares et des PUA (page 112).
7. Cliquez sur **Ajouter**.

L'application suspecte apparaît dans la liste **Applications autorisées**.

Préautorisation d'éléments potentiellement suspects

Si vous voulez autoriser l'utilisation d'une application ou d'un fichier que Sophos Endpoint Security and Control n'a pas encore classé comme suspect, vous pouvez pré-autoriser cette application ou ce fichier en l'ajoutant vous-même à la liste des éléments autorisés.

1. Vérifiez quelle stratégie antivirus et HIPS est utilisée par le ou les groupes d'ordinateurs que vous voulez configurer.

   Retrouvez plus de renseignements à la section Vérification des stratégies utilisées par un groupe (page 27).
2. Dans le volet **Stratégies**, cliquez deux fois sur **Antivirus et HIPS**.

3. Cliquez deux fois sur la stratégie que vous désirez modifier.
   La boîte de dialogue **Stratégie antivirus et HIPS** apparaît.
4. Cliquez sur **Autorisation**.
   La boîte de dialogue **Gestionnaire d'autorisation** apparaît.
5. Cliquez sur l'onglet correspondant au type de comportement qui a été détecté.

   Dans cet exemple, nous utiliserons **Dépassement de la mémoire tampon**.
6. Cliquez sur **Nouveau**.
   La boîte de dialogue **Ouverture** apparaît.
7. Naviguez vers l'application et cliquez deux fois dessus.

L'application suspecte apparaît dans la liste **Applications autorisées**.

Si vous vous êtes trompé ou voulez simplement supprimer une application du **Gestionnaire d'autorisation**, supprimez-la de la liste des fichiers connus :

1. Dans la boîte de dialogue **Gestionnaire d'autorisation**, cliquez sur l'onglet correspondant au type de comportement ayant été détecté.

   Dans cet exemple, nous utiliserons **Fichiers suspects**.
2. Dans la liste **Fichiers autorisés**, sélectionnez le fichier.
3. Cliquez sur **Supprimer**.
4. Dans la liste **Fichiers connus**, sélectionnez le fichier.
5. Cliquez sur **Supprimer**.

Autorisation de sites Web

Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - antivirus et HIPS** pour réaliser cette tâche.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

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

Attention
L'autorisation d'un site Web classé comme malveillant par Sophos peut exposer vos utilisateurs à des menaces. Assurez-vous que la visite du site Web est sûre avant de l'autoriser.

Pour autoriser un site Web :

1. Vérifiez quelle stratégie antivirus et HIPS est utilisée par le(s) groupe(s) d'ordinateurs que vous voulez configurer.

   Retrouvez plus de renseignements à la section Vérification des stratégies utilisées par un groupe (page 27).
2. Dans le volet **Stratégies**, cliquez deux fois sur **Antivirus et HIPS**.
3. Cliquez deux fois sur la stratégie que vous désirez modifier.
   La boîte de dialogue **Stratégie antivirus et HIPS** apparaît.
4. Cliquez sur **Autorisation**.
   La boîte de dialogue **Gestionnaire d'autorisation** apparaît.
5. Sur l'onglet **Sites Web**, cliquez sur **Ajouter**.

- Pour modifier une entrée de site Web, sélectionnez-la dans la liste **Sites Web autorisés**, puis cliquez sur **Modifier**.
- Pour supprimer une entrée de site Web, sélectionnez-la dans la liste **Sites Web autorisés**, puis cliquez sur **Supprimer**.

Le site Web apparaît dans la liste **Sites Web autorisés**.

Remarques

- Si le contrôle des téléchargements est activé et si vos utilisateurs visitent un site Web contenant une menace, l'accès à ce site sera bloqué même s'il est répertorié en tant que site Web autorisé.
- Si vous utilisez la fonctionnalité de contrôle du Web, lorsque vous autorisez un site Web bloqué par votre stratégie de **Contrôle du Web**, le site Web restera tout de même bloqué. Pour autoriser l'accès à ce site Web, vous devrez l'exempter de filtrage par contrôle du Web mais aussi l'autoriser dans la stratégie antivirus et HIPS. Retrouvez plus de renseignements sur le contrôle du Web à la section Stratégie de contrôle du Web (page 178).

7.2 Stratégie de pare-feu

La stratégie de **Pare-feu** définit la manière dont le pare-feu assure la protection des ordinateurs.

Par défaut, Sophos Client Firewall est activé et bloque tout le trafic non indispensable. Avant de l'utiliser sur votre réseau, configurez-le pour autoriser les applications que vous désirez utiliser. Retrouvez plus de renseignements à la section Configuration d'une stratégie de pare-feu (page 115).

Retrouvez une liste complète des paramètres du pare-feu par défaut dans l'article 57757 de la base de connaissances.

Remarque
Un nombre de fonctions ont été retirées de la version 3.0 de Sophos Client Firewall 3.0 pour Windows 8 et versions supérieures et sont uniquement disponibles sur les ordinateurs sous Windows 7 ou versions antérieures. Ces fonctions sont :

- Mode interactif
- Détection des processus cachés
- Détection de mémoire modifiée
- Applications rawsocket (les rawsockets sont traitées de la même manière que les autres connexions)
- Règles non dynamiques
- L'option **Connexions simultanées** pour les règles TCP
- L'option **Où le port local correspond au port distant**

7.2.1 Configuration de base du pare-feu

Configuration d'une stratégie de pare-feu

Par défaut, le pare-feu est activé et bloque tout le trafic non indispensable. Par conséquent, vous devez le configurer pour qu'il autorise les applications que vous souhaitez utiliser puis le tester avant

de procéder à son installation sur tous les ordinateurs. Retrouvez plus de renseignements dans le *Guide de configuration des stratégies de Sophos Enterprise Console*.

Retrouvez plus de renseignements sur les paramètres par défaut du pare-feu dans l'article 57757 de la base de connaissances Sophos.

Retrouvez plus de renseignements sur la prévention des ponts entre réseaux à la section Stratégie de contrôle des périphériques (page 165).

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

Remarque
Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - pare-feu** pour configurer une stratégie de pare-feu.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements sur l'administration déléguée à la section Gestion des rôles et des sous-parcs (page 14).

Pour configurer une stratégie de pare-feu :

1. Dans le volet **Stratégies**, cliquez deux fois sur **Pare-feu**.
2. Cliquez deux fois sur la stratégie **Par défaut** pour la modifier.
   L'assistant de **Stratégie de pare-feu** apparaît. Suivez les instructions à l'écran. Retrouvez ci-dessous des informations supplémentaires sur certaines des options.
3. Sur la page **Configuration du pare-feu**, sélectionnez le type d'emplacement :
   - Sélectionnez **Emplacement unique** pour les ordinateurs qui sont toujours sur le réseau, par exemple, les stations de travail.
   - Sélectionnez **Emplacement double** si vous voulez que le pare-feu utilise des paramètres différents en fonction de l'emplacement où les ordinateurs sont utilisés, par exemple, au bureau (connecté au réseau) et en dehors du bureau (déconnecté du réseau). Il peut être judicieux de paramétrer un emplacement double pour les ordinateurs portables.
4. Sur la page **Mode de fonctionnement**, sélectionnez la manière dont le pare-feu va gérer le trafic entrant et sortant.

Mode	Description
Bloquer le trafic entrant et sortant	• Niveau par défaut. Offre le plus haut niveau de sécurité. • Autorise uniquement le trafic essentiel via le pare-feu et authentifie les applications grâce aux sommes de contrôle. • Pour autoriser les applications les plus fréquemment utilisées au sein de votre entreprise à communiquer par le biais du pare-feu, cliquez sur **Accepter**. Retrouvez plus de renseignements à la section À

Mode	Description
	propos des applications fiables (page 124).
Bloquer le trafic entrant et autoriser le trafic sortant	• Offre un niveau de sécurité inférieur à **Bloquer le trafic entrant et sortant**. • Autorise vos ordinateurs à accéder au réseau et à Internet sans qu'il vous soit nécessaire de créer de règles spéciales. • Toutes les applications sont autorisées à communiquer par le biais du pare-feu.
Surveiller	• Applique toutes les règles que vous avez définies au trafic réseau. Si le trafic n'a aucune règle de correspondance, il est signalé à la console, et il est autorisé uniquement s'il est sortant. • Ce mode vous permet de collecter des informations sur votre réseau et, par la suite, de créer des règles appropriées avant de déployer le pare-feu sur tous vos ordinateurs. Retrouvez plus de renseignements à la section À propos du mode surveillance (page 117).

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

Après avoir paramétré le pare-feu, vous pouvez consulter les événements de pare-feu (par exemple, les applications bloquées par le pare-feu) dans **Pare-feu - Observateur d'événements**. Retrouvez plus de renseignements à la section Affichage des événements du pare-feu (page 203).

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

À propos du mode surveillance

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

Vous pouvez ensuite utiliser l'Observateur d'événements pour créer des règles qui autorisent ou bloquent le trafic, les applications et les processus signalés comme indiqué à la section Création d'une règle d'événement de pare-feu (page 121).

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

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

En mode interactif, le pare-feu demande à l'utilisateur d'autoriser ou de bloquer toutes les applications et tout le trafic pour lesquels ne s'appliquent aucune règle. Retrouvez plus de renseignements à la section Mode interactif (page 123).

Ajout et acceptation d'une application

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

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

1. Sur la page **Mode de fonctionnement** de l'assistant **Stratégie de pare-feu**, cliquez sur **Accepter**. La boîte de dialogue **Stratégie de pare-feu** apparaît.
2. Cliquez sur **Ajouter**.
   La boîte de dialogue **Stratégie de pare-feu - Ajouter une application fiable** apparaît.
3. Dans le champ **Période de recherche**, cliquez sur la flèche du menu déroulant et sélectionnez la période pour laquelle vous souhaitez afficher les événements d'applications.

   Vous pouvez sélectionner soit une période fixe, par exemple, **Depuis 24 heures**, soit **Personnalisée** et spécifiez votre propre période en sélectionnant les dates de début et de fin.
4. Si vous voulez consulter les événements d'applications d'un certain type, dans le champ **Type d'événement**, cliquez sur la flèche du menu déroulant et sélectionnez le type d'événement.
5. Si vous voulez consulter les événements d'applications pour un certain fichier, saisissez le nom du fichier dans le champ **Nom du fichier**.

   Si vous laissez ce champ vide, les événements d'applications de tous les fichiers apparaîtront.

   Vous pouvez utiliser des caractères génériques dans ce champ. Utilisez ? pour remplacer un seul caractère du nom et * pour remplacer une chaîne de caractères quelconque.
6. Cliquez sur **Rechercher** pour afficher une liste d'événements d'applications.
7. Sélectionnez un événement d'applications, puis cliquez sur **OK**.

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

Administration déléguée

Remarque
Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - pare-feu** pour configurer une stratégie de pare-feu.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

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

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

1. Vérifiez quelle stratégie de pare-feu est utilisée par le ou les groupes d'ordinateurs que vous désirez configurer.

   Retrouvez plus de renseignements à la section Vérification des stratégies utilisées par un groupe (page 27).
2. Dans le volet **Stratégies**, cliquez deux fois sur **Pare-feu** puis cliquez deux fois sur la stratégie que vous souhaitez changer.
3. Sur la page **Partage de fichiers et d'imprimantes** de l'assistant **Stratégie de pare-feu**, sélectionnez **Utiliser les paramètres personnalisés**, puis cliquez sur **Personnaliser**.

4. Dans la liste **Paramètres du réseau local**, sélectionnez la case **Fiable** pour un réseau.

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

Administration déléguée

Remarque
Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - pare-feu** pour configurer une stratégie de pare-feu.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Autorisation du partage de fichiers et d'imprimantes

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

1. Vérifiez quelle stratégie de pare-feu est utilisée par le ou les groupes d'ordinateurs que vous désirez configurer.

   Retrouvez plus de renseignements à la section Vérification des stratégies utilisées par un groupe (page 27).
2. Dans le volet **Stratégies**, cliquez deux fois sur **Pare-feu** puis cliquez deux fois sur la stratégie que vous souhaitez changer.
3. Sur la page **Partage de fichiers et d'imprimantes** de l'assistant **Stratégie de pare-feu**, sélectionnez **Autoriser le partage de fichiers et d'imprimantes**.

Administration déléguée

Remarque
Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - pare-feu** pour configurer une stratégie de pare-feu.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Contrôle plus souple du partage de fichiers et d'imprimantes

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

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

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

1. Vérifiez quelle stratégie de pare-feu est utilisée par le ou les groupes d'ordinateurs que vous désirez configurer.

   Retrouvez plus de renseignements à la section Vérification des stratégies utilisées par un groupe (page 27).
2. Dans le volet **Stratégies**, cliquez deux fois sur **Pare-feu** puis cliquez deux fois sur la stratégie que vous souhaitez changer.
3. Sur la page **Partage de fichiers et d'imprimantes** de l'assistant **Stratégie de pare-feu**, sélectionnez **Utiliser les paramètres personnalisés**, puis cliquez sur **Personnaliser**.
4. Dessélectionnez la case à cocher **Bloquer le partage de fichiers et d'imprimantes pour d'autres réseaux**.

Administration déléguée

Remarque
Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - pare-feu** pour configurer une stratégie de pare-feu.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Blocage du partage de fichiers et d'imprimantes non désiré

Remarque
Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - pare-feu** pour configurer une stratégie de pare-feu.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

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

1. Vérifiez quelle stratégie de pare-feu est utilisée par le ou les groupes d'ordinateurs que vous désirez configurer.

   Retrouvez plus de renseignements à la section Vérification des stratégies utilisées par un groupe (page 27).
2. Dans le volet **Stratégies**, cliquez deux fois sur **Pare-feu** puis cliquez deux fois sur la stratégie que vous souhaitez changer.
3. Sur la page **Partage de fichiers et d'imprimantes** de l'assistant **Stratégie de pare-feu**, sélectionnez **Utiliser les paramètres personnalisés**, puis cliquez sur **Personnaliser**.
4. Sélectionnez la case à cocher **Bloquer le partage de fichiers et d'imprimantes pour d'autres réseaux**.

Création d’une règle d’événement de pare-feu

Remarque
Si vous utilisez l’administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - pare-feu** pour configurer une stratégie de pare-feu.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Vous pouvez créer des règles pour tous les événements de pare-feu à l’exception des événements de « mémoire modifiée ».

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

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

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

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

   Remarque
   Vous ne pouvez pas ajouter une règle à une stratégie appliquée hors de votre sous-parc actif.

Remarque
Pour créer une règle d’applications directement depuis une stratégie de pare-feu à l’aide des pages de configuration de la stratégie de pare-feu avancée, veuillez consulter la section Création d’une règle d’applications depuis une stratégie de pare-feu (page 139).

Désactivation temporaire du pare-feu

Remarque
Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - pare-feu** pour configurer une stratégie de pare-feu.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

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

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

1. Vérifiez quelle stratégie de pare-feu est utilisée par le ou les groupes d'ordinateurs que vous désirez configurer.

   Retrouvez plus de renseignements à la section Vérification des stratégies utilisées par un groupe (page 27).
2. Dans le volet **Stratégies**, cliquez deux fois sur **Pare-feu**. Puis cliquez deux fois sur la stratégie que vous désirez changer.
   L'assistant de **Stratégie de pare-feu** apparaît.
3. Sur la page de bienvenue de l'assistant, procédez de la manière suivante :
   - Si vous souhaitez désactiver le pare-feu pour tous les emplacements que vous avez configuré (emplacement principal et emplacement secondaire, si vous en avez un de configuré), cliquez sur **Suivant**. Sur la page **Configuration du pare-feu**, sélectionnez **Autoriser tout le trafic (le pare-feu est désactivé)**. Fermez l'assistant.
   - Si vous souhaitez désactiver le pare-feu pour l'un des emplacements (principal ou secondaire), cliquez sur le bouton **Stratégie de pare-feu avancée**. Dans la boîte de dialogue **Stratégie de pare-feu** qui apparaît, sélectionnez la case **Autoriser tout le trafic** à côté de l'**Emplacement principal** ou de l'**Emplacement secondaire**. Cliquez sur **OK**. Fermez l'assistant de **Stratégie de pare-feu**.

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

7.2.2 Configuration avancée du pare-feu

Ouverture des pages de configuration avancée

Remarque
Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - pare-feu** pour configurer une stratégie de pare-feu.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

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

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

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

Mode interactif

Sous Windows 7 ou versions antérieures, vous pouvez activer le mode interactif. Le pare-feu affiche une boîte de dialogue d'apprentissage à chaque fois qu'une application inconnue ou qu'un service inconnu demande l'accès au réseau. La boîte de dialogue d'apprentissage demande à l'utilisateur d'autoriser ou de bloquer le trafic ou de créer une règle pour ce type de trafic.

Remarque
Le mode interactif n'est pas disponible à partir de Windows 8. Vous devez ajouter des règles de stratégies spécifiques pour autoriser ou bloquer les applications. Vous pouvez utiliser le **Pare-feu - Observateur d'événements** pour gérer les règles d'applications de manière interactive comme indiqué à la section Création d'une règle d'événement de pare-feu (page 121).

Activation du mode interactif

Remarque
Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - pare-feu** pour configurer une stratégie de pare-feu.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Le pare-feu peut fonctionner en mode interactif en demandant à l'utilisateur comment il doit traiter le trafic détecté. Retrouvez plus de renseignements à la section Mode interactif (page 123).

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

1. Vérifiez quelle stratégie de pare-feu est utilisée par le ou les groupes d'ordinateurs que vous désirez configurer.

   Retrouvez plus de renseignements à la section Vérification des stratégies utilisées par un groupe (page 27).
2. Sur la page de **Bienvenue** de l'assistant **Stratégie de pare-feu**, cliquez sur **Stratégie de pare-feu avancée**.
3. Sous **Configurations**, cliquez sur le bouton **Configurer** correspondant à l'emplacement que vous souhaitez configurer.
4. Sur l'onglet **Général**, sous **Mode de fonctionnement**, cliquez sur **Interactif**.

Passage en mode non interactif

Remarque
Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - pare-feu** pour configurer une stratégie de pare-feu.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Il existe deux modes non interactifs :

- Autoriser par défaut
- Bloquer par défaut

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

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

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

Configuration du pare-feu

À propos des applications fiables

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

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

Remarque
Pour une sécurité renforcée, vous pouvez appliquer une ou plusieurs règles d'applications afin de spécifier les conditions d'exécution de l'application. Retrouvez plus de renseignements sur la manière de procéder à la section Création d'une règle d'applications depuis une stratégie de pare-feu (page 139).

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

Remarque
Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - pare-feu** pour configurer une stratégie de pare-feu.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

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

1. Sous **Configurations**, cliquez sur le bouton **Configurer** correspondant à l'emplacement que vous souhaitez configurer.
2. Cliquez sur l'onglet **Applications**.
3. Cliquez sur **Ajouter**.
   La boîte de dialogue **Stratégie de pare-feu - Ajouter une application** apparaît.
4. Dans le champ **Période de recherche**, cliquez sur la flèche du menu déroulant et sélectionnez la période pour laquelle vous souhaitez afficher les événements d'applications.

   Vous pouvez sélectionner soit une période fixe, par exemple, **Depuis 24 heures**, soit **Personnalisée** et spécifiez votre propre période en sélectionnant les dates de début et de fin.
5. Si vous voulez consulter les événements d'applications d'un certain type, dans le champ **Type d'événement**, cliquez sur la flèche du menu déroulant et sélectionnez le type d'événement.
6. Si vous voulez consulter les événements d'applications pour un certain fichier, saisissez le nom du fichier dans le champ **Nom du fichier**.

   Si vous laissez ce champ vide, les événements d'applications de tous les fichiers apparaîtront.

   Vous pouvez utiliser des caractères joker dans ce champ. Utilisez ? pour remplacer un seul caractère du nom et * pour remplacer une chaîne de caractères quelconque.
7. Cliquez sur **Rechercher** pour afficher une liste d'événements d'applications.
8. Sélectionnez un événement d'applications, puis cliquez sur **OK**.

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

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

Remarque
Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - pare-feu** pour configurer une stratégie de pare-feu.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

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

1. Sous **Configurations**, cliquez sur le bouton **Configurer** correspondant à l'emplacement que vous souhaitez configurer.
2. Cliquez sur l'onglet **Applications**.
3. Sélectionnez l'application dans la liste et cliquez sur **Supprimer**.

Acceptation d'une application

Remarque
Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - pare-feu** pour configurer une stratégie de pare-feu.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Pour accepter une application sur un groupe d'ordinateurs :

1. Sous **Configurations**, cliquez sur le bouton **Configurer** correspondant à l'emplacement que vous souhaitez configurer.
2. Cliquez sur l'onglet **Applications**.
   Si l'application ne figure pas dans la liste, veuillez suivre les instructions de la section Ajout d'une application dans une stratégie de pare-feu (page 125) pour l'ajouter.
3. Sélectionnez l'application dans la liste et cliquez sur **Accepter**.

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

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

- Création d'une règle d'applications (page 138)
- Application de règles d'applications prédéfinies (page 140)

Acceptation d'une application à l'aide de l'Observateur d'événements du pare-feu

Remarque
Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - pare-feu** pour configurer une stratégie de pare-feu.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Si le pare-feu signale une application inconnue ou bloque une application sur vos ordinateurs en réseau, un événement apparaît dans l'Observateur d'événements du pare-feu. Cette rubrique vous décrit comment accepter une application depuis l'Observateur d'événements du pare-feu et comment appliquer la nouvelle règle aux stratégies de pare-feu de votre choix.

Pour retrouver plus de détails sur les applications signalées ou bloquées dans l'Observateur d'événements du pare-feu et pour les accepter ou créer de nouvelles règles pour ces applications :

1. Dans le menu **Événements**, cliquez sur **Événements du pare-feu**.
2. Dans la boîte de dialogue **Pare-feu - Observateur d'événements**, sélectionnez l'entrée de l'application pour laquelle vous voulez accepter ou créer une règle et cliquez ensuite sur **Créer une règle**.
3. Dans la boîte de dialogue qui apparaît, indiquez si vous voulez accepter l'application ou lui créer une règle à l'aide d'une option prédéfinie existante.

4. A partir de la liste des stratégies de pare-feu, sélectionnez celles auxquelles vous voulez appliquer la règle. Pour appliquer la règle à toutes les stratégies, cliquez sur **Tout sélectionner**, puis cliquez sur **OK**.

- Si vous utilisez des sommes de contrôle, ajoutez la somme de contrôle de l'application à la liste des sommes de contrôle autorisées. Retrouvez plus de renseignements à la section Ajout d'une somme de contrôle d'application (page 129).
- Vous pouvez aussi ajouter une application comme fiable directement dans une stratégie de pare-feu à l'aide des pages de configuration de la stratégie de pare-feu avancée. Retrouvez plus de renseignements à la section Création d'une règle d'applications depuis une stratégie de pare-feu (page 139).

Blocage d'une application

Remarque
Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - pare-feu** pour configurer une stratégie de pare-feu.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Pour bloquer une application sur un groupe d'ordinateurs :

1. Vérifiez quelle stratégie de pare-feu est utilisée par le ou les groupes d'ordinateurs que vous désirez configurer.

   Retrouvez plus de renseignements à la section Vérification des stratégies utilisées par un groupe (page 27).
2. Dans le volet **Stratégies**, cliquez deux fois sur **Pare-feu** puis cliquez deux fois sur la stratégie que vous souhaitez changer.
3. Sur la page de **Bienvenue** de l'assistant **Stratégie de pare-feu**, cliquez sur **Stratégie de pare-feu avancée**.
4. Sous **Configurations**, cliquez sur le bouton **Configurer** correspondant à l'emplacement que vous souhaitez configurer.
5. Cliquez sur l'onglet **Applications**.

   Si l'application ne figure pas dans la liste, veuillez suivre les instructions de la section Ajout d'une application dans une stratégie de pare-feu (page 125) pour l'ajouter.
6. Sélectionnez l'application dans la liste et cliquez sur **Bloquer**.

Autorisation de lancement des processus cachés aux applications

Remarque
Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - pare-feu** pour configurer une stratégie de pare-feu.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

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

Des applications malveillantes peuvent utiliser cette technique pour échapper aux pare-feu : au lieu de le faire elles-mêmes, elles lancent une application fiable pour qu'elle accède au réseau.

Pour autoriser des applications à lancer des processus cachés, procédez comme indiqué ci-dessous.

Remarque
Cette option n'est pas disponible sous Windows 8 et versions supérieures car elle est gérée automatiquement par la technologie HIPS de Sophos Anti-Virus.

1. Sur la page de **Bienvenue** de l'assistant **Stratégie de pare-feu**, cliquez sur **Stratégie de pare-feu avancée**.
2. Sous **Configurations**, cliquez sur **Configurer** près de l'emplacement pour lequel vous voulez configurer le pare-feu.
3. Cliquez sur l'onglet **Processus**.
4. Dans la zone supérieure, cliquez sur le bouton **Ajouter**.
   La boîte de dialogue **Stratégie de pare-feu - Ajouter une application** apparaît.
5. Dans le champ **Période de recherche**, cliquez sur la flèche du menu déroulant et sélectionnez la période pour laquelle vous souhaitez afficher les événements d'applications.

   Vous pouvez sélectionner soit une période fixe, par exemple, **Depuis 24 heures**, soit **Personnalisée** et spécifiez votre propre période en sélectionnant les dates de début et de fin.
6. Si vous voulez consulter les événements d'applications pour un certain fichier, saisissez le nom du fichier dans le champ **Nom du fichier**.

   Si vous laissez ce champ vide, les événements d'applications de tous les fichiers apparaîtront.

   Vous pouvez utiliser des caractères de remplacement dans ce champ. Utilisez ? pour remplacer un seul caractère du nom et * pour remplacer une chaîne de caractères quelconque.
7. Cliquez sur **Rechercher** pour afficher une liste d'événements d'applications.
8. Sélectionnez un événement d'applications, puis cliquez sur **OK**.

Si vous activez le mode interactif, le pare-feu peut afficher une boîte de dialogue d'apprentissage sur le terminal lorsqu'il détecte un nouveau programme de lancement. Retrouvez plus de renseignements à la section Activation du mode interactif (page 123). Le mode interactif n'est pas disponible à partir de Windows 8.

Autorisation d'utilisation des rawsockets aux applications

Remarque
Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - pare-feu** pour configurer une stratégie de pare-feu.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Certaines applications peuvent accéder au réseau par le biais des rawsockets, et ainsi avoir le contrôle sur tous les aspects des données qu'elles envoient sur le réseau.

Les applications malveillantes exploitent les rawsockets en contrefaisant leur adresse IP ou en envoyant des messages corrompus.

Pour autoriser les applications à accéder au réseau par le biais des rawsockets, procédez comme indiqué ci-dessous.

Remarque
Cette option n'est pas disponible à partir de Windows 8. Le pare-feu traite les rawsockets de la même manière qu'il traite les sockets ordinaires.

1. Cliquez deux fois sur la stratégie de pare-feu que vous désirez modifier.
2. Sur la page de **Bienvenue** de l'assistant **Stratégie de pare-feu**, cliquez sur **Stratégie de pare-feu avancée**.
3. Sous **Configurations**, cliquez sur **Configurer** près de l'emplacement pour lequel vous voulez configurer le pare-feu.
4. Cliquez sur l'onglet **Processus**.
5. Dans la zone inférieure, cliquez sur le bouton **Ajouter**.
   La boîte de dialogue **Stratégie de pare-feu - Ajouter une application** apparaît.
6. Dans le champ **Période de recherche**, cliquez sur la flèche du menu déroulant et sélectionnez la période pour laquelle vous souhaitez afficher les événements d'applications.

   Vous pouvez sélectionner soit une période fixe, par exemple, **Depuis 24 heures**, soit **Personnalisée** et spécifiez votre propre période en sélectionnant les dates de début et de fin.
7. Si vous voulez consulter les événements d'applications pour un certain fichier, saisissez le nom du fichier dans le champ **Nom du fichier**.

   Si vous laissez ce champ vide, les événements d'applications de tous les fichiers apparaîtront.

   Vous pouvez utiliser des caractères de remplacement dans ce champ. Utilisez ? pour remplacer un seul caractère du nom et * pour remplacer une chaîne de caractères quelconque.
8. Cliquez sur **Rechercher** pour afficher une liste d'événements d'applications.
9. Sélectionnez un événement d'applications, puis cliquez sur **OK**.

Si vous activez le mode interactif, le pare-feu peut afficher une boîte de dialogue d'apprentissage sur le terminal lorsqu'une rawsocket est détectée. Retrouvez plus de renseignements à la section Activation du mode interactif (page 123).

Ajout d'une somme de contrôle d'application

Remarque
Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - pare-feu** pour configurer une stratégie de pare-feu.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Chaque version d'une application a une somme de contrôle unique. Le pare-feu peut utiliser cette somme de contrôle pour décider si une application est autorisée ou non.

Par défaut, le pare-feu vérifie la somme de contrôle de chaque application qui s'exécute. Si la somme de contrôle est inconnue ou a changé, le pare-feu la bloque.

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

1. Cliquez deux fois sur la stratégie de pare-feu que vous désirez modifier.
2. Sur la page de **Bienvenue** de l'assistant **Stratégie de pare-feu**, cliquez sur **Stratégie de pare-feu avancée**.
3. Cliquez sur l'onglet **Sommes de contrôle**.
4. Cliquez sur **Ajouter**.

La boîte de dialogue **Stratégie de pare-feu - Ajouter une somme de contrôle de l'application** apparaît.

5. Dans le champ **Période de recherche**, cliquez sur la flèche du menu déroulant et sélectionnez la période pour laquelle vous souhaitez afficher les événements d'applications.

   Vous pouvez sélectionner soit une période fixe, par exemple, **Depuis 24 heures**, soit **Personnalisée** et spécifiez votre propre période en sélectionnant les dates de début et de fin.
6. Dans le champ **Type d'événement**, cliquez sur la flèche du menu déroulant et indiquez si vous voulez ajouter une somme de contrôle pour une application modifiée ou pour une nouvelle application.
7. Si vous voulez consulter les événements d'applications pour un certain fichier, saisissez le nom du fichier dans le champ **Nom du fichier**.

   Si vous laissez ce champ vide, les événements d'applications de tous les fichiers apparaîtront.

   Vous pouvez utiliser des caractères génériques dans ce champ. Utilisez ? pour remplacer un seul caractère du nom et * pour remplacer une chaîne de caractères quelconque.
8. Cliquez sur **Rechercher** pour afficher une liste d'événements d'applications.
9. Sélectionnez l'événement d'application pour lequel vous voulez ajouter une somme de contrôle, puis cliquez sur **OK**.

La somme de contrôle d'une application est ajoutée à la liste des sommes de contrôle autorisées dans la boîte de dialogue **Stratégie de pare-feu**.

Si vous activez le mode interactif, le pare-feu peut afficher une boîte de dialogue d'apprentissage sur le terminal lorsqu'il détecte une nouvelle application ou une application modifiée. Retrouvez plus de renseignements à la section Activation du mode interactif (page 123).

Activation ou désactivation du blocage des processus modifiés

Remarque
Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - pare-feu** pour configurer une stratégie de pare-feu.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Certains programmes malveillants tentent de contourner le pare-feu en modifiant un processus en mémoire lancé par un programme de confiance et en utilisant ensuite ce processus modifié pour accéder au réseau.

Vous pouvez configurer le pare-feu pour détecter et bloquer les processus qui ont été modifiés en mémoire.

Pour activer ou désactiver le blocage des processus modifiés :

1. Cliquez deux fois sur la stratégie de pare-feu que vous désirez modifier.
2. Sur la page de **Bienvenue** de l'assistant **Stratégie de pare-feu**, cliquez sur **Stratégie de pare-feu avancée**.
3. Sous **Configurations**, cliquez sur **Configurer** près de l'emplacement pour lequel vous voulez configurer le pare-feu.
4. Sur l'onglet **Général**, sous **Blocage**, dessélectionnez la case **Bloquer les processus si la mémoire est modifiée par une autre application** pour désactiver le blocage des processus modifiés.

   Pour activer le blocage des processus modifiés, sélectionnez cette case à cocher.

Si le pare-feu détecte un processus modifié dans la mémoire, il ajoute une règle pour empêcher l'accès au réseau à ce processus modifié.

Remarques

- Nous déconseillons la désactivation permanente du blocage des processus modifiés. Désactivez cette option uniquement lorsque cela est nécessaire.
- Le blocage des processus modifiés n'est pas pris en charge sur les versions 64 bits de Windows et à partir de Windows 8. À partir de Windows 8, la technologie HIPS de Sophos Anti-Virus effectue l'opération automatiquement.
- Seul le processus modifié est bloqué. Le programme effectuant la modification n'est pas bloqué et a donc accès au réseau.

Activation et désactivation de l'utilisation des sommes de contrôle

Par défaut, le pare-feu utilise les sommes de contrôle pour authentifier les applications. Lorsque vous faites confiance ou bloquer des applications, elles sont automatiquement identifiées par leurs sommes de contrôle (vous pouvez également ajouter ces sommes de contrôle manuellement). Une application sera bloquée si elle ne correspond pas à une somme de contrôle.

Si vous désactivez cette option, les applications sont identifiées par leur nom de fichier.

Pour activer ou désactiver l'utilisation des sommes de contrôle pour authentifier les applications :

1. Cliquez deux fois sur la stratégie de pare-feu que vous désirez modifier.
2. Sur la page de **Bienvenue** de l'assistant **Stratégie de pare-feu**, cliquez sur **Stratégie de pare-feu avancée**.
3. Sous **Configurations**, cliquez sur **Configurer** près de l'emplacement pour lequel vous voulez configurer le pare-feu.
4. Dans l'onglet **Général**, sous **Blocage**, sélectionnez ou décochez la case **Utiliser les sommes de contrôle pour authentifier les applications**.

Autorisation ou blocage de paquets IPv6

Pour autoriser ou bloquer les paquets IPv6 :

1. Cliquez deux fois sur la stratégie de pare-feu que vous désirez modifier.
2. Sur la page de **Bienvenue** de l'assistant **Stratégie de pare-feu**, cliquez sur **Stratégie de pare-feu avancée**.
3. Sous **Configurations**, cliquez sur **Configurer** près de l'emplacement pour lequel vous voulez configurer le pare-feu.
4. Sur l'onglet **Général**, sous **Blocage**, décochez ou sélectionnez la case **Bloquer les paquets IPv6**.

Filtrage des messages ICMP

Remarque
Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - pare-feu** pour configurer une stratégie de pare-feu.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Les messages ICMP (Internet Control Message Protocol) autorisent les ordinateurs d'un réseau à partager les informations sur les erreurs et sur leur état. Vous pouvez autoriser ou bloquer des types spécifiques de messages ICMP entrants ou sortants.

Filtrez uniquement les messages ICMP si vous êtes familier avec les protocoles réseau. Retrouvez plus de renseignements sur les types de message ICMP à la section Explication des types de message ICMP (page 132).

Pour filtrer les messages ICMP :

1. Cliquez deux fois sur la stratégie de pare-feu que vous désirez modifier.
2. Sur la page de **Bienvenue** de l'assistant **Stratégie de pare-feu**, cliquez sur **Stratégie de pare-feu avancée**.
3. Sous **Configurations**, cliquez sur **Configurer** près de l'emplacement pour lequel vous voulez configurer le pare-feu.
4. Sur l'onglet **ICMP**, sélectionnez la case **Entrant** ou **Sortant** pour autoriser les types de messages entrants ou sortants spécifiés.

Explication des types de message ICMP

Demande d'écho, Réponse d'écho	Utilisées pour tester l'accessibilité et l'état de la destination. Un hôte envoie une **Demande d'écho** et attend de recevoir la **Réponse d'écho** correspondante. Ces opérations sont généralement effectuées en utilisant la commande `ping`.
Destination injoignable, Réponse d'écho	Envoyé par un routeur lorsqu'il ne peut pas transmettre un datagramme IP. Un datagramme est l'unité de données ou le paquet transmis dans un réseau TCP/IP.
Source éteinte	Envoyé par un hôte ou un routeur lorsqu'il est saturé par le volume de données qu'il reçoit. Ce message demande à la source de réduire sa vitesse de transmission des datagrammes.
Rediriger les messages	Envoyé par un routeur lorsqu'il reçoit un datagramme devant être envoyé à un routeur différent. Le message contient l'adresse vers laquelle la source doit rediriger les prochains datagrammes. Cette opération est utilisée pour optimiser l'acheminement du trafic réseau.
Annonce routeur, Sollicitation routeur	Autorise les hôtes à découvrir l'existence des routeurs. Les routeurs diffusent régulièrement leurs adresses IP via les messages d'**Annonce routeur**. Les hôtes peuvent aussi demander l'adresse d'un routeur en diffusant un message **Sollicitation routeur** auquel un routeur répond par une **Annonce routeur**.
Temps dépassé	Envoyé par un routeur si le datagramme a atteint la limite maximum de routeurs par le biais desquels il est transporté.
Problème de paramétrage	Envoyé par un routeur en cas de problème de transmission d'un datagramme entraînant l'impossibilité d'achever l'opération. L'origine de ce genre de problème peut être un en-tête de datagramme incorrect.
Demande d'horodatage, Réponse d'horodatage	Utilisé pour synchroniser les horloges entre les hôtes et pour estimer la durée d'acheminement.
Demande Informations, Réponse Informations	Obsolète. Ces messages étaient auparavant utilisés par les hôtes pour déterminer leurs adresses inter-réseau mais sont désormais obsolètes et ne doivent pas être utilisés.

Demande masque d'adresse, Réponse masque d'adresse	Utilisé pour retrouver le masque du sous-réseau (c'est-à-dire quels bits de l'adresse définissent le réseau). Un hôte envoie une **Demande masque d'adresse** à un routeur et reçoit une **Réponse masque d'adresse** en retour.

Règles de pare-feu

Règles globales

Les règles globales s'appliquent à toutes les communications réseau et aux applications même si elles ont des règles d'applications.

Règles d'applications

Vous pouvez avoir une ou plusieurs règles pour une application. Vous pouvez soit utiliser des règles prédéfinies créées par Sophos soit créer des règles personnalisées qui vous procureront un contrôle précis sur l'accès autorisé à une application.

Retrouvez plus de renseignements sur les paramètres des règles globales et d'applications par défaut dans l'article 57757 de la base de connaissances Sophos.

Ordre dans lequel les règles sont appliquées

Pour les connexions qui utilisent les rawsockets, seules les règles globales sont vérifiées.

Pour les connexions qui n'utilisent *pas* les rawsockets, de nombreuses règles sont vérifiées selon que la connexion est établie ou non sur une adresse réseau figurant sur l'onglet **Réseau local**.

Si l'adresse réseau figure dans la liste sur l'onglet **Réseau local**, les règles suivantes sont vérifiées :

- Si l'adresse a été marquée comme **Fiable**, tout le trafic sur la connexion est autorisé sans vérifications supplémentaires.
- Si l'adresse a été marquée comme **NetBIOS**, le partage de fichiers et d'imprimantes sur toute connexion satisfaisant aux critères demandés est autorisé :

Connexion	Port	Plage
TCP	Distant	137-139 ou 445
TCP	Local	137-139 ou 445
UDP	Distant	137 ou 138
UDP	Local	137 ou 138

Si l'adresse réseau ne figure *pas* dans la liste sur l'onglet **Réseau local**, d'autres règles de pare-feu sont vérifiées dans l'ordre suivant :

1. Tout le trafic **NetBIOS** qui n'a pas été autorisé via l'onglet **Réseau local** est géré selon que la case **Bloquer le partage de fichiers et d'imprimantes pour d'autres réseaux** ait été sélectionnée ou non :
    - Si la case est sélectionnée, le trafic est bloqué.
    - Si la case est dessélectionnée, le trafic est traité par les règles restantes.

2. Les règles globales à priorité élevée sont vérifiées dans l'ordre où elles apparaissent dans la liste.
3. Si aucune règle n'a encore été appliquée à la connexion, les règles d'applications sont vérifiées.
4. Si la connexion n'a pas encore été traitée, les règles globales à priorité normale sont vérifiées dans l'ordre où elles apparaissent dans la liste.
5. Si aucune règle n'a été trouvée pour traiter la connexion :
   - En mode **Autoriser par défaut**, le trafic est autorisé (s'il est sortant).
   - En mode **Bloquer par défaut**, le trafic est bloqué.
   - En mode **Interactif**, l'utilisateur décide de l'action à mener. Ce mode n'est pas disponible à partir de Windows 8.

Remarque
Si vous n'avez pas changé le mode de fonctionnement, le pare-feu est en mode **Bloquer par défaut**.

Détection du réseau local

Remarque
Cette fonction n'est plus disponible à partir de Windows 8.

Vous pouvez assigner le réseau local d'un ordinateur à des règles de pare-feu.

Lorsqu'il démarre, le pare-feu détermine le réseau local de l'ordinateur, puis surveille tout changement pendant son fonctionnement. Si un quelconque changement est détecté, le pare-feu met à jour toutes les règles du réseau local avec la nouvelle plage d'adresses de ce même réseau.

Attention
Nous vous conseillons d'être extrêmement vigilants lors de l'utilisation des règles du réseau local comme configurations secondaires. S'il s'agit d'un ordinateur portable utilisé en dehors du bureau, il peut se connecter à un réseau local inconnu. Dans ce cas, il est possible que les règles de pare-feu de la configuration secondaire qui utilisent le réseau local comme adresse autorisent le trafic inconnu.

Règles globales

Création d'une règle globale

Remarque
Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - pare-feu** pour configurer une stratégie de pare-feu.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Important
Nous vous conseillons de créer des règles globales uniquement si vous êtes familier avec les protocoles réseau.

Les règles globales s'appliquent à toutes les communications réseau et applications qui n'ont pas encore de règle.

Pour créer une règle globale :

1. Cliquez deux fois sur la stratégie de pare-feu que vous désirez modifier.
2. Sur la page de **Bienvenue** de l'assistant **Stratégie de pare-feu**, cliquez sur **Stratégie de pare-feu avancée**.
3. Sous **Configurations**, cliquez sur **Configurer** près de l'emplacement pour lequel vous voulez configurer le pare-feu.
4. Cliquez sur l'onglet **Règles globales**.
5. Cliquez sur **Ajouter**.
6. Sous **Nom de la règle**, saisissez un nom pour la règle.

   Le nom de la règle doit être unique dans la liste des règles. Deux règles globales ne peuvent pas avoir le même nom.
7. Pour appliquer la règle avant toute règle d'applications ou toute règle globale à priorité normale, sélectionnez la case **Règle à priorité élevée**.

   Retrouvez plus de renseignements sur l'ordre dans lequel les règles sont appliquées à la section Ordre dans lequel les règles sont appliquées (page 133).
8. Sous **Sélectionner les événements que la règle traitera**, sélectionnez les conditions auxquelles la connexion doit correspondre pour que la règle s'applique.
9. Sous **Sélectionner l'action par laquelle la règle répondra**, sélectionnez soit **Autoriser** soit **Bloquer**.
10. Procédez de l'une des manières suivantes :

    - Pour autoriser d'autres connexions vers et depuis la même adresse distante tout en conservant la connexion initiale existante, sélectionnez **Connexions simultanées**.

      Remarque
      Cette option est uniquement disponible pour les règles TCP qui sont en mode dynamique par défaut.

    - Pour autoriser les réponses depuis l'ordinateur distant qui seront basées sur la connexion initiale, sélectionnez **Inspection dynamique**.

      Remarque
      Cette option est uniquement disponible pour les règles UDP et IP.

    Remarque
    À partir de Windows 8, ces options ne s'appliquent pas car l'**Inspection dynamique** est toujours utilisée et que les **Connexions simultanées** ne sont pas prises en charge.

11. Sous **Description de la règle**, cliquez sur une valeur soulignée. Par exemple, si vous cliquez sur le lien **TCP avec état**, la boîte de dialogue **Sélection du protocole** s'ouvre.

Modification d'une règle globale

Remarque
Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - pare-feu** pour configurer une stratégie de pare-feu.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Important
Nous vous conseillons de modifier les règles globales uniquement si vous êtes familier avec les protocoles réseau.

Pour modifier une règle globale :

1. Cliquez deux fois sur la stratégie de pare-feu que vous désirez modifier.
2. Sur la page de **Bienvenue** de l'assistant **Stratégie de pare-feu**, cliquez sur **Stratégie de pare-feu avancée**.
3. Sous **Configurations**, cliquez sur **Configurer** près de l'emplacement pour lequel vous voulez configurer le pare-feu.
4. Cliquez sur l'onglet **Règles globales**.
5. Dans la liste **Règle**, sélectionnez la règle que vous souhaitez modifier.
6. Cliquez sur **Modifier**.

   Retrouvez plus de renseignements sur les paramètres des règles globales dans l'article 57757 de la base de connaissances Sophos.

Copie d'une règle globale

Remarque
Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - pare-feu** pour configurer une stratégie de pare-feu.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

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

1. Cliquez deux fois sur la stratégie de pare-feu que vous désirez modifier.
2. Sur la page de **Bienvenue** de l'assistant **Stratégie de pare-feu**, cliquez sur **Stratégie de pare-feu avancée**.
3. Sous **Configurations**, cliquez sur **Configurer** près de l'emplacement pour lequel vous voulez configurer le pare-feu.
4. Cliquez sur l'onglet **Règles globales**.
5. Dans la liste **Règle**, sélectionnez la règle que vous souhaitez copier.
6. Cliquez sur **Copier**.

Suppression d'une règle globale

Remarque
Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - pare-feu** pour configurer une stratégie de pare-feu.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

1. Cliquez deux fois sur la stratégie de pare-feu que vous désirez modifier.
2. Sur la page de **Bienvenue** de l'assistant **Stratégie de pare-feu**, cliquez sur **Stratégie de pare-feu avancée**.
3. Sous **Configurations**, cliquez sur **Configurer** près de l'emplacement pour lequel vous voulez configurer le pare-feu.
4. Cliquez sur l'onglet **Règles globales**.
5. Dans la liste **Règle**, sélectionnez la règle que vous souhaitez supprimer.
6. Cliquez sur **Supprimer**.

Modification de l'ordre dans lequel les règles sont appliquées

Remarque
Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - pare-feu** pour configurer une stratégie de pare-feu.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Les règles globales sont appliquées dans l'ordre dans lequel elles apparaissent en partant du haut de la liste.

Pour modifier l'ordre dans lequel les règles globales sont appliquées :

1. Cliquez deux fois sur la stratégie de pare-feu que vous désirez modifier.
2. Sur la page de **Bienvenue** de l'assistant **Stratégie de pare-feu**, cliquez sur **Stratégie de pare-feu avancée**.
3. Sous **Configurations**, cliquez sur **Configurer** près de l'emplacement pour lequel vous voulez configurer le pare-feu.
4. Cliquez sur l'onglet **Règles globales**.
5. Dans la liste **Règle**, cliquez sur la règle que vous souhaitez faire monter ou descendre dans la liste.
6. Cliquez sur **Monter** ou **Descendre**.

Règles d’applications

Création d’une règle d’applications

Remarque
Si vous utilisez l’administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - pare-feu** pour configurer une stratégie de pare-feu.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

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

1. Cliquez deux fois sur la stratégie de pare-feu que vous désirez modifier.
2. Sur la page de **Bienvenue** de l’assistant **Stratégie de pare-feu**, cliquez sur **Stratégie de pare-feu avancée**.
3. Sous **Configurations**, cliquez sur **Configurer** près de l’emplacement pour lequel vous voulez configurer le pare-feu.
4. Cliquez sur l’onglet **Applications**.
5. Sélectionnez l’application dans la liste et cliquez sur **Personnaliser**.
6. Dans la boîte de dialogue **Règles d’applications**, cliquez sur **Ajouter**.
7. Sous **Nom de la règle**, saisissez un nom pour la règle.

   Le nom de la règle doit être unique dans la liste des règles. Deux règles d’applications ne peuvent pas avoir le même nom, en revanche, deux applications peuvent chacune avoir une règle portant le même nom.
8. Sous **Sélectionner les événements que la règle traitera**, sélectionnez les conditions auxquelles la connexion doit correspondre pour que la règle s’applique.
9. Sous **Sélectionner l’action par laquelle la règle répondra**, sélectionnez soit **Autoriser** soit **Bloquer**.
10. Procédez de l’une des manières suivantes :

    - Pour autoriser d’autres connexions vers et depuis la même adresse distante tout en conservant la connexion initiale existante, sélectionnez **Connexions simultanées**.

      Remarque
      Cette option est uniquement disponible pour les règles TCP qui sont en mode dynamique par défaut.

    - Pour autoriser les réponses depuis l’ordinateur distant qui seront basées sur la connexion initiale, sélectionnez **Inspection dynamique**.

      Remarque
      Cette option est uniquement disponible pour les règles UDP et IP.

Remarque
À partir de Windows 8, ces options ne s’appliquent pas car l’**Inspection dynamique** est toujours utilisée et que les **Connexions simultanées** ne sont pas prises en charge.

11. Sous **Description de la règle**, cliquez sur une valeur soulignée. Par exemple, si vous cliquez sur le lien **TCP avec état**, la boîte de dialogue **Sélection du protocole** s'ouvre.

Création d'une règle d'applications depuis une stratégie de pare-feu

Remarque
Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - pare-feu** pour configurer une stratégie de pare-feu.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Vous pouvez créer une règle d'applications directement depuis une stratégie de pare-feu à l'aide des pages de configuration de la stratégie de pare-feu avancée.

Pour créer une règle d'applications depuis une stratégie de pare-feu :

1. Cliquez deux fois sur la stratégie que vous désirez modifier.
2. Sur la page de bienvenue de l'assistant **Stratégie de pare-feu**, cliquez sur le bouton **Stratégie de pare-feu avancée**.
3. Dans la boîte de dialogue **Stratégie de pare-feu** qui apparaît, cliquez sur le bouton **Configurer** situé à côté de l'emplacement pour lequel vous souhaitez configurer le pare-feu.
4. Procédez de l'une des manières suivantes :
   - Si vous souhaitez ajouter une application à la stratégie de pare-feu, dans la boîte de dialogue qui apparaît, allez dans l'onglet **Applications** et cliquez sur **Ajouter**.
   - Si vous souhaitez autoriser une application à lancer des processus cachés, allez dans l'onglet **Processus** et cliquez sur **Ajouter** dans la zone supérieure.
   - Si vous souhaitez autoriser une application à accéder au réseau à l'aide de rawsockets, allez dans l'onglet **Processus** et cliquez sur **Ajouter** dans la zone inférieure.

   La boîte de dialogue **Stratégie de pare-feu - Ajouter une application** apparaît.
5. Si vous ajoutez une application, dans la boîte **Type d'événements**, vous pouvez choisir d'ajouter une application modifiée, une nouvelle application ou une application pour laquelle aucune règle d'applications n'est définie dans la stratégie de pare-feu.
6. Sélectionnez une entrée pour l'application que vous souhaitez ajouter ou autoriser à lancer des processus cachés ou à utiliser des rawsockets et cliquez sur **OK**.
   L'application est ajoutée à la stratégie de pare-feu.

Si vous avez ajouté une application sur l'onglet **Applications**, celle-ci est ajoutée comme fiable. Si vous le souhaitez, vous pouvez la bloquer ou lui créer une règle personnalisée.

Modification d'une règle d'applications

Remarque
Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - pare-feu** pour configurer une stratégie de pare-feu.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

1. Cliquez deux fois sur la stratégie de pare-feu que vous désirez modifier.

2. Sur la page de **Bienvenue** de l'assistant **Stratégie de pare-feu**, cliquez sur **Stratégie de pare-feu avancée**.
3. Sous **Configurations**, cliquez sur **Configurer** près de l'emplacement pour lequel vous voulez configurer le pare-feu.
4. Cliquez sur l'onglet **Applications**.
5. Sélectionnez l'application dans la liste et cliquez sur **Personnaliser**.
6. Dans la boîte de dialogue **Règles d'applications**, cliquez sur **Modifier**.
7. Sous **Nom de la règle**, saisissez un nom pour la règle.

   Le nom de la règle doit être unique dans la liste des règles. Deux règles d'applications ne peuvent pas avoir le même nom, en revanche, deux applications peuvent chacune avoir une règle portant le même nom.
8. Sous **Sélectionner les événements que la règle traitera**, sélectionnez les conditions auxquelles la connexion doit correspondre pour que la règle s'applique.
9. Sous **Sélectionner l'action par laquelle la règle répondra**, sélectionnez soit **Autoriser** soit **Bloquer**.
10. Procédez de l'une des manières suivantes :

    - Pour autoriser d'autres connexions vers et depuis la même adresse distante tout en conservant la connexion initiale existante, sélectionnez **Connexions simultanées**.

      Remarque
      Cette option est uniquement disponible pour les règles TCP qui sont en mode dynamique par défaut.

    - Pour autoriser les réponses depuis l'ordinateur distant qui seront basées sur la connexion initiale, sélectionnez **Inspection dynamique**.

      Remarque
      Cette option est uniquement disponible pour les règles UDP et IP.

    Remarque
    À partir de Windows 8, ces options ne s'appliquent pas car l'**Inspection dynamique** est toujours utilisée et que les **Connexions simultanées** ne sont pas prises en charge.

11. Sous **Description de la règle**, cliquez sur une valeur soulignée. Par exemple, si vous cliquez sur le lien **TCP avec état**, la boîte de dialogue **Sélection du protocole** s'ouvre.

Application de règles d'applications prédéfinies

Remarque
Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - pare-feu** pour configurer une stratégie de pare-feu.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Les règles d'applications prédéfinies sont une série de règles d'applications créées par Sophos. Pour ajouter des règles prédéfinies à la liste des règles pour une application :

1. Cliquez deux fois sur la stratégie de pare-feu que vous désirez modifier.
2. Sur la page de **Bienvenue** de l'assistant **Stratégie de pare-feu**, cliquez sur **Stratégie de pare-feu avancée**.
3. Sous **Configurations**, cliquez sur **Configurer** près de l'emplacement pour lequel vous voulez configurer le pare-feu.
4. Cliquez sur l'onglet **Applications**.
5. Sélectionnez l'application dans la liste et cliquez sur **Personnaliser**.
6. Passez votre curseur sur **Ajouter des règles prédéfinies** et cliquez sur une règle prédéfinie.

Copie d'une règle d'applications

Remarque
Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - pare-feu** pour configurer une stratégie de pare-feu.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

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

1. Cliquez deux fois sur la stratégie de pare-feu que vous désirez modifier.
2. Sur la page de **Bienvenue** de l'assistant **Stratégie de pare-feu**, cliquez sur **Stratégie de pare-feu avancée**.
3. Sous **Configurations**, cliquez sur **Configurer** près de l'emplacement pour lequel vous voulez configurer le pare-feu.
4. Cliquez sur l'onglet **Applications**.
5. Sélectionnez l'application dans la liste et cliquez sur **Personnaliser**.
6. Dans la boîte de dialogue **Règles d'applications**, sélectionnez la règle que vous voulez copier et cliquez sur **Copier**.

Suppression d'une règle d'applications

Remarque
Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - pare-feu** pour configurer une stratégie de pare-feu.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

1. Cliquez deux fois sur la stratégie de pare-feu que vous désirez modifier.
2. Sur la page de **Bienvenue** de l'assistant **Stratégie de pare-feu**, cliquez sur **Stratégie de pare-feu avancée**.
3. Sous **Configurations**, cliquez sur **Configurer** près de l'emplacement pour lequel vous voulez configurer le pare-feu.
4. Cliquez sur l'onglet **Applications**.
5. Sélectionnez l'application dans la liste et cliquez sur **Personnaliser**.
6. Dans la boîte de dialogue **Règles d'applications**, sélectionnez la règle que vous voulez supprimer et cliquez sur **Supprimer**.

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

Remarque
Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - pare-feu** pour configurer une stratégie de pare-feu.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Les règles d'applications sont appliquées dans l'ordre dans lequel elles apparaissent en partant du haut de la liste.

Pour modifier l'ordre dans lequel les règles d'applications sont appliquées :

1. Cliquez deux fois sur la stratégie de pare-feu que vous désirez modifier.
2. Sur la page de **Bienvenue** de l'assistant **Stratégie de pare-feu**, cliquez sur **Stratégie de pare-feu avancée**.
3. Sous **Configurations**, cliquez sur **Configurer** près de l'emplacement pour lequel vous voulez configurer le pare-feu.
4. Cliquez sur l'onglet **Applications**.
5. Sélectionnez l'application dans la liste et cliquez sur **Personnaliser**.
6. Dans la boîte de dialogue **Règles d'applications**, dans la liste **Règle**, cliquez sur la règle que vous souhaitez faire monter ou descendre dans la liste.
7. Cliquez sur **Monter** ou **Descendre**.

Connexion intuitive selon l'emplacement

La connexion intuitive selon l'emplacement est une fonction de Sophos Client Firewall qui affecte une configuration de pare-feu à chaque adaptateur réseau sur un ordinateur selon l'emplacement actuel des adaptateurs réseau de l'ordinateur.

Cette fonction est généralement utilisée lorsque un employé travaille depuis son domicile sur un ordinateur portable professionnel. Il utilise deux connexions réseau en même temps :

- Pour son usage professionnel, il se connecte au réseau de l'entreprise par le biais d'un client VPN et d'un **adaptateur réseau virtuel**.
- Pour son usage privé, il se connecte à son fournisseur de services par le biais d'un câble réseau et d'un **adaptateur réseau physique**.

Dans ce cas de figure, la configuration professionnelle doit être appliquée à la connexion professionnelle virtuelle tandis que la configuration privée, généralement plus limitée, doit être appliquée à la connexion du fournisseur de services privé.

Remarque
La configuration privée nécessite l'instauration de certaines règles afin de permettre d'établir la connexion professionnelle "virtuelle".

À propos de la configuration de la connexion intuitive selon l'emplacement

1. Définissez la liste des adresses MAC de la passerelle ou les noms de domaine de vos emplacements principaux. Généralement, il s'agit de vos réseaux professionnels.

2. Créez la configuration du pare-feu à utiliser pour vos emplacements principaux. Généralement, cette configuration est moins restrictive.
3. Créez une configuration de pare-feu secondaire. Généralement, cette configuration est plus restrictive.
4. Choisissez une configuration à appliquer.

Selon la méthode de détection que vous utilisez, le pare-feu récupère l'adresse DNS ou de la passerelle des adaptateurs réseau pour chacun de vos ordinateurs et la compare à votre liste d'adresses.

- Si une adresse de votre liste correspond à l'adresse d'un adaptateur réseau, l'adaptateur est affecté à la configuration de l'**emplacement principal**.
- Si aucune des adresses de votre liste ne correspond à l'adresse d'un adaptateur réseau, l'adaptateur est affecté à la stratégie de l'**emplacement secondaire**.

Important
La configuration secondaire passe du mode **Interactif** au mode **Bloquer par défaut** sur un ordinateur lorsque les deux conditions suivantes sont rencontrées :

- Les deux emplacements sont actifs.
- La configuration principale n'est *pas* interactive.

Définition des emplacements principaux

1. Cliquez deux fois sur la stratégie de pare-feu que vous désirez modifier.
2. Sur la page de **Bienvenue** de l'assistant **Stratégie de pare-feu**, cliquez sur **Stratégie de pare-feu avancée**.
3. Sous **Configurations**, cliquez sur **Configurer** près de l'emplacement pour lequel vous voulez configurer le pare-feu.
4. Cliquez sur l'onglet **Détection de l'emplacement**.
5. Sous **Méthode de détection**, cliquez sur le bouton **Configurer** correspondant à la méthode que vous souhaitez utiliser pour définir vos emplacements principaux :

Option	Description
Identifier l'emplacement par DNS	Vous créez une liste de noms de domaine et d'adresses IP attendues qui correspondent à vos emplacements principaux.
Identifier l'emplacement par adresse MAC de la passerelle	Vous créez une liste d'adresses MAC de la passerelle qui correspondent à vos emplacements principaux.

6. Suivez les instructions à l'écran.

Création d'une configuration secondaire

1. Cliquez deux fois sur la stratégie de pare-feu que vous désirez modifier.
2. Sur la page de **Bienvenue** de l'assistant **Stratégie de pare-feu**, cliquez sur **Stratégie de pare-feu avancée**.
3. Sous **Configurations**, cliquez sur **Configurer** près de l'emplacement pour lequel vous voulez configurer le pare-feu.
4. Sélectionnez la case à cocher **Ajout d'une configuration pour un second emplacement**.

Paramétrez maintenant votre configuration secondaire. Retrouvez plus de renseignements sur la manière de procéder à la section Ouverture des pages de configuration avancée (page 122).

Attention
Nous vous conseillons d'être extrêmement vigilants lors de l'utilisation des règles du réseau local comme configurations secondaires. S'il s'agit d'un ordinateur portable utilisé en dehors du bureau, il peut se connecter à un réseau local inconnu. Dans ce cas, il est possible que les règles de pare-feu de la configuration secondaire qui utilisent le réseau local comme adresse autorisent le trafic inconnu.

Sélection de la configuration à appliquer

1. Cliquez deux fois sur la stratégie de pare-feu que vous désirez modifier.
2. Sur la page de **Bienvenue** de l'assistant **Stratégie de pare-feu**, cliquez sur **Stratégie de pare-feu avancée**.
3. Sous **Configurations**, cliquez sur **Configurer** près de l'emplacement pour lequel vous voulez configurer le pare-feu.
4. Dans l'onglet **Général**, sous **Emplacement appliqué**, cliquez sur l'une des options suivantes :

Option	Description
Appliquer la configuration pour l'emplacement détecté	Le pare-feu applique soit la configuration principale, soit la configuration secondaire à chaque connexion réseau selon les paramètres de détection de la connexion intuitive selon l'emplacement (comme indiqué à la section À propos de la configuration de la connexion intuitive selon l'emplacement (page 142)).
Appliquer la configuration pour l'emplacement principal	Le pare-feu applique la configuration principale à toutes les connexions réseau.
Appliquer la configuration pour l'emplacement secondaire	Le pare-feu applique la configuration secondaire à toutes les connexions réseau.

Rapport du pare-feu

Par défaut, le pare-feu sur un terminal signale les changements d'état, les événements et les erreurs à Enterprise Console.

Modifications d'état du pare-feu

Le pare-feu signale les modifications d'état suivantes :

- Modifications du mode de fonctionnement
- Modifications de la version du logiciel
- Modifications de la configuration du pare-feu pour autoriser tout le trafic
- Modifications du pare-feu pour qu'il soit conforme à la stratégie

Lorsque vous travaillez en mode interactif, la configuration de votre pare-feu peut volontairement différer de la stratégie appliquée par **Enterprise Console**. Dans ce cas, vous pouvez décider de

ne **pas** envoyer d'alertes « Diffère de la stratégie » à Enterprise Console lorsque vous modifiez certaines parties de la configuration de votre pare-feu.

Retrouvez plus de renseignements à la section Activation ou désactivation de rapport sur les modifications locales (page 145).

Événements du pare-feu

Un *événement* est lorsque le système d'exploitation du terminal ou une application connue sur le terminal tente de communiquer avec un autre ordinateur via une connexion réseau.

Vous pouvez empêcher le pare-feu de signaler les événements à Enterprise Console.

Retrouvez plus de renseignements à la section Désactivation du signalement du trafic réseau inconnu (page 146).

Activation ou désactivation de rapport sur les modifications locales

Remarque
Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - pare-feu** pour configurer une stratégie de pare-feu.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Si la configuration du pare-feu sur les terminaux diffère de la stratégie, vous pouvez **désactiver le signalement des modifications locales**.

Remarque
Cette option n'est plus disponible à partir de Windows 8.

La désactivation du rapport sur les modifications locales empêche le pare-feu d'envoyer des alertes « Diffère de la stratégie » à Enterprise Console concernant les modifications apportées aux règles globales, aux applications, aux processus ou aux sommes de contrôle. Vous pouvez, si vous le souhaitez, exécuter cette opération, par exemple, lorsque les terminaux sont en mode interactif, car il s'agit de paramètres qui peuvent être changés à l'aide des boîtes de dialogue d'apprentissage.

Si la configuration du pare-feu sur les terminaux est prévue pour être conforme à la stratégie, **activez le signalement des modifications locales**.

Pour désactiver le signalement des modifications locales :

1. Cliquez deux fois sur la stratégie de pare-feu que vous désirez modifier.
2. Sur la page de **Bienvenue** de l'assistant **Stratégie de pare-feu**, cliquez sur **Stratégie de pare-feu avancée**.
3. Sous **Configurations**, cliquez sur **Configurer** près de l'emplacement pour lequel vous voulez configurer le pare-feu.
4. Cliquez sur l'onglet **Général**.
5. Sous **Rapport**, procédez de l'une des manières suivantes :
    - Pour activer le signalement des modifications locales, sélectionnez la case à cocher **Afficher une alerte sur la console d'administration en cas de modifications locales de règles globales, d'applications, de processus ou de sommes de contrôle**.

- Pour désactiver le signalement des modifications locales, dessélectionnez la case à cocher **Afficher une alerte dans la console d'administration si des changements locaux sont appliqués aux règles d'applications**.

Désactivation du signalement du trafic réseau inconnu

Remarque
Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - pare-feu** pour configurer une stratégie de pare-feu.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Vous pouvez empêcher le pare-feu installé sur les terminaux de signaler le trafic réseau inconnu à Enterprise Console. Le pare-feu considère le trafic comme inconnu s'il n'a pas de règle.

Pour empêcher le pare-feu installé sur les terminaux de signaler le trafic réseau inconnu à Enterprise Console :

1. Cliquez deux fois sur la stratégie de pare-feu que vous désirez modifier.
2. Sur la page de **Bienvenue** de l'assistant **Stratégie de pare-feu**, cliquez sur **Stratégie de pare-feu avancée**.
3. Sous **Configurations**, cliquez sur **Configurer** près de l'emplacement pour lequel vous voulez configurer le pare-feu.
4. Cliquez sur l'onglet **Général**.
5. Sous **Blocage**, sélectionnez la case **Utiliser les sommes de contrôle pour authentifier les applications**.
6. Sous **Rapport**, dessélectionnez la case à cocher **Signaler les applications et le trafic inconnus à la console d'administration**.

Désactivation du rapport d'erreurs de pare-feu

Important
Nous vous déconseillons de désactiver en permanence le rapport d'erreurs de pare-feu. Désactivez le rapport uniquement lorsque nécessaire.

Pour empêcher le pare-feu sur les terminaux de signaler les erreurs à l'Enterprise Console :

1. Cliquez deux fois sur la stratégie de pare-feu que vous désirez modifier.
2. Sur la page de **Bienvenue** de l'assistant **Stratégie de pare-feu**, cliquez sur **Stratégie de pare-feu avancée**.
3. Sous **Configurations**, cliquez sur **Configurer** près de l'emplacement pour lequel vous voulez configurer le pare-feu.
4. Cliquez sur l'onglet **Général**.
5. Sous **Rapport**, dessélectionnez la case à cocher **Signaler les erreurs à la console d'administration**.

Importation ou exportation de la configuration du pare-feu

Remarque
Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - pare-feu** pour configurer une stratégie de pare-feu.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Vous pouvez importer ou exporter les paramètres généraux ainsi que les règles du pare-feu sous un fichier de configuration (*.conf). Vous pouvez utiliser cette fonction pour effectuer les opérations suivantes :

- Sauvegarder et restaurer la configuration de votre pare-feu.
- Importer les règles d'application créées sur un ordinateur et les utiliser pour créer une stratégie pour d'autres ordinateurs exécutant la même série d'applications.
- Fusionner les configurations créés sur plusieurs ordinateurs différents pour créer une stratégie valide pour un ou plusieurs groupes d'ordinateurs sur le réseau.

Pour importer ou exporter la configuration du pare-feu :

1. Vérifiez quelle stratégie de pare-feu est utilisée par le ou les groupes d'ordinateurs que vous désirez configurer.

   Retrouvez plus de renseignements à la section Vérification des stratégies utilisées par un groupe (page 27).
2. Dans le volet **Stratégies**, cliquez deux fois sur **Pare-feu** puis cliquez deux fois sur la stratégie que vous souhaitez importer ou exporter.
3. Sur la page de **Bienvenue** de l'assistant **Stratégie de pare-feu**, cliquez sur **Stratégie de pare-feu avancée**.
4. Dans la boîte de dialogue **Stratégie de pare-feu**, sur l'onglet **Général**, sous **Gestion de la configuration**, cliquez sur **Importer** ou sur **Exporter**.

7.3 Stratégie de contrôle des applications

L'Enterprise Console vous permet de détecter et de bloquer les « applications contrôlées », c'est-à-dire les applications légitimes qui ne constituent pas une menace pour la sécurité, mais dont vous considérez l'usage inadapté sur votre lieu de travail. 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 uniquement à Sophos Endpoint Security and Control pour Windows.

Les applications peuvent être bloquées ou autorisées pour différents groupes d'ordinateurs en toute facilité. Par exemple, l'utilisation d'une application de voix sur IP (VoIP) peut être interdite sur les ordinateurs utilisés dans les locaux de l'entreprise mais autorisée sur les ordinateurs distants.

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, en revanche, vous pouvez envoyer une

demande à Sophos afin d'inclure une nouvelle application légitime que vous souhaitez contrôler sur votre réseau.

Retrouvez plus de renseignements dans l'article 63656 de la base de connaissances Sophos.

Cette section vous décrit comment sélectionner les applications que vous souhaitez contrôler sur votre réseau et comment paramétrer la recherche des applications contrôlées.

Remarque
Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - contrôle des applications** pour pouvoir configurer une stratégie de contrôle des applications.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements sur l'administration déléguée à la section Gestion des rôles et des sous-parcs (page 14).

Événements de contrôle des applications

En cas d'événement de contrôle des applications, par exemple, lorsqu'une application contrôlée a été détectée sur le réseau, l'événement est consigné dans le journal des événements de contrôle des applications et peut être consulté depuis l'Enterprise Console. Retrouvez plus de renseignements à la section Affichage des événements du contrôle des applications (page 201).

Le nombre d'ordinateurs ayant des événements dépassant le seuil spécifié au cours des sept derniers jours est affiché sur le Tableau de bord.

Vous pouvez également paramétrer l'envoi des alertes à des destinataires de votre choix en cas d'événement de contrôle des applications. Retrouvez plus de renseignements à la section Configuration des alertes et des messages du contrôle des applications (page 194).

7.3.1 Sélection des applications à contrôler

Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - contrôle des applications** pour pouvoir configurer une stratégie de contrôle des applications.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

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

1. Vérifiez quelle stratégie de contrôle des applications est utilisée par le ou les groupes d'ordinateurs que vous souhaitez configurer.

   Retrouvez plus de renseignements à la section Vérification des stratégies utilisées par un groupe (page 27).
2. Dans le volet **Stratégies**, cliquez deux fois sur **Contrôle des applications**. Puis cliquez deux fois sur la stratégie que vous désirez changer.
3. Dans la boîte de dialogue **Stratégie de contrôle des applications**, cliquez sur l'onglet **Autorisation**.
4. Sélectionnez un **Type d'application**, par exemple **Partage de fichiers**.

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

- 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 “Tout ajouter”.

5. Sur l’onglet **Contrôle** de la boîte de dialogue **Stratégie de contrôle des applications**, assurez-vous que la recherche des applications contrôlées est activée. (Retrouvez plus de renseignements à la section Recherche des applications à contrôler (page 149)). Cliquez sur **OK**.

7.3.2 Recherche des applications à contrôler

Si vous utilisez l’administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - contrôle des applications** pour pouvoir configurer une stratégie de contrôle des applications.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Vous pouvez configurer Sophos Endpoint Security and Control pour rechercher les applications que vous souhaitez contrôler sur accès sur votre réseau.

1. Vérifiez quelle stratégie de contrôle des applications est utilisée par le ou les groupes d’ordinateurs que vous souhaitez configurer.

   Retrouvez plus de renseignements à la section Vérification des stratégies utilisées par un groupe (page 27).
2. Dans le volet **Stratégies**, cliquez deux fois sur **Contrôle des applications**. Puis cliquez deux fois sur la stratégie que vous désirez changer.
   La boîte de dialogue **Stratégie de contrôle des applications** apparaît.
3. 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).

Retrouvez tous les renseignements nécessaires à la suppression des applications contrôlées de vos ordinateurs en réseau à la section Désinstallation des applications contrôlées non désirées (page 150).

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. Retrouvez plus d'instructions à la section Configuration des alertes et des messages du contrôle des applications (page 194).

7.3.3 Désinstallation des applications contrôlées non désirées

Avant de désinstaller les applications contrôlées, assurez-vous que le contrôle sur accès à la recherche des applications contrôlées est désactivé. Ce type de contrôle bloque les programmes utilisés pour installer et désinstaller les applications et peut donc gêner la désinstallation.

Vous pouvez supprimer une application de l'une des deux façons suivantes :

- Sur chaque ordinateur, exécutez le programme de désinstallation du produit. Vous pouvez généralement réaliser cette opération en ouvrant le Panneau de configuration de Windows et en utilisant Ajout/Suppression de programmes.
- Sur le serveur, utilisez votre script habituel ou votre outil d'administration pour lancer la désinstallation du produit sur les ordinateurs en réseau.

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

7.4 Stratégie de contrôle des données

Remarque
Cette fonction n'est pas incluse dans toutes les licences. Pour pouvoir l'utiliser, il se peut que vous deviez changer votre contrat de licence. Retrouvez plus de renseignements à la section http://www.sophos.com/fr-fr/products/complete/comparison.aspx.

Le contrôle des données vous permet de réduire les pertes accidentelles de données depuis les stations de travail grâce à la surveillance et à la restriction du transfert de fichiers contenant des données sensibles. Pour ce faire, créez des règles de contrôle des données puis ajoutez ces règles aux stratégies de **Contrôle des données**.

Vous pouvez surveiller et contrôler le transfert de fichiers effectué vers des périphériques de stockage spécifiés (par exemple, un périphérique de stockage amovible ou un lecteur optique), ou effectué par des applications spécifiées (par exemple, un client de messagerie ou un navigateur Web).

Pour que vous puissiez rapidement définir et déployer une stratégie de contrôle des données, les SophosLabs maintiennent à jour une bibliothèque de définitions des données sensibles (Listes de contrôle du contenu). Même si cette bibliothèque regroupe principalement les définitions sur les informations personnelles identifiables, elle couvre également d'autres structures de données usuelles. Vous pouvez utiliser les Listes de contrôle du contenu dans l'Enterprise Console conformément aux instructions présentes plus bas dans cette section.

7.4.1 Comment fonctionne le contrôle des données ?

Le contrôle des données identifie la perte accidentelle de données qui est généralement due à une gestion imprudente des données sensibles par les employés. Par exemple, un utilisateur envoie un fichier contenant des données sensibles à son domicile via un service de messagerie électronique.

Le contrôle des données vous permet de surveiller et de contrôler le transfert des fichiers depuis les ordinateurs vers les périphériques de stockage et les applications connectées à Internet.

- **Périphériques de stockage :** le contrôle des données intercepte tous les fichiers copiés sur les périphériques des stockage surveillés à l'aide de l'Explorateur Windows (qui inclut le bureau Windows). En revanche, les enregistrements directs depuis les applications, telles que Microsoft Word, ou les transferts à l'aide de l'invite de commande ne sont pas interceptés.

  Il est possible de forcer tous les transferts à effectuer sur les périphériques de stockage surveillés à l'aide de l'Explorateur Windows en utilisant l'action **Autoriser le transfert après accord de l'utilisateur et journaliser l'événement** ou l'action **Bloquer le transfert et journaliser l'événement**. Dans les deux cas, toute tentative d'enregistrement direct à partir d'une application ou de transfert de fichiers à l'aide de l'invite de commande est bloquée par le contrôle des données. Une alerte de bureau apparaît et demande à l'utilisateur d'utiliser l'Explorateur Windows pour terminer le transfert.

  Lorsqu'une stratégie de contrôle des données contient des règles avec l'option **Autoriser le transfert de fichiers et journaliser l'événement**, les enregistrements directs depuis des applications et les transferts à l'aide de l'invite de commandes ne sont pas interceptés. Ce comportement permet à l'utilisateur d'utiliser des périphériques de stockage sans aucune restriction. Par contre, les événements de contrôle des données sont quand même journalisés pour les transferts effectués à l'aide de l'Explorateur Windows.

  Remarque
  Cette restriction ne s'applique pas à la surveillance des applications.

- **Applications :** Pour garantir que seuls les chargements de fichiers effectués par les utilisateurs sont surveillés, certains emplacements de fichiers système sont exclus de la surveillance par le contrôle des données. Ceci réduit considérablement le risque de création d'événements de contrôle des données par des applications ouvrant des fichiers de configuration plutôt que par des utilisateurs chargeant des fichiers.

  Important
  En cas d'événements erronés générés par une application ouvrant des fichiers de configuration, vous pouvez résoudre le problème en ajoutant des exclusions d'emplacement personnalisés ou en configurant une règle de contrôle des données moins sensible. Retrouvez plus de renseignements dans l'article 113024 de la base de connaissances Sophos.

  Remarque
  Les exclusions du contrôle sur accès ne s'appliquent pas toujours au contrôle des données.

À quel moment le contrôle des données utilise les exclusions du contrôle sur accès ?

Selon la manière dont vous copiez et l'endroit où vous déplacez les fichiers, le contrôle de données prendra ou ne prendra pas en compte les exclusions du contrôle sur accès que vous avez définies dans la stratégie antivirus et HIPS.

Le contrôle de données **utilise** les exclusions du contrôle sur accès lorsque les fichiers sont téléchargés ou joints à l'aide d'une application sous surveillance (par exemple, un client de messagerie, un navigateur Web ou un client de messagerie instantanée). Retrouvez plus de renseignements sur la configuration des exclusions du contrôle sur accès à la section Exclusion d'éléments du contrôle sur accès (page 88).

Important
Si vous avez exclus des fichiers à distance du contrôle sur accès, le contrôle des données ne contrôlera pas les fichiers que vous avez téléchargés ou joints à partir d'un emplacement réseau sur une application sous surveillance (par exemple, un email ou un navigateur Web). Retrouvez plus de renseignements à la section Le contrôle des données n'effectue pas le contrôle des fichiers téléchargés ou joints (page 233).

Le contrôle des données **n'utilise pas** les exclusions du contrôle sur accès lorsque les fichiers sont copiés ou déplacés à l'aide de l'Explorateur Windows. Par conséquent, les exclusions ne fonctionneront pas si, par exemple, vous copiez les fichiers sur un périphérique de stockage (par ex ; USB) ou si vous copiez ou déplacez les fichiers sur un emplacement réseau. Tous les fichiers seront contrôlés, même si vous avez exclus des fichiers à distance du contrôle sur accès.

Remarque
Si vous copiez ou déplacez des fichiers **archivés** sur un emplacement réseau, la procédure risque d'être longue. Par exemple, elle prendra plus d'une minute pour 100 Mo de données selon votre connexion réseau. En effet, le contrôle des fichiers archivés est beaucoup plus long que le contrôle des fichiers non archivés.

Stratégies de contrôle des données

Le contrôle des données vous permet de surveiller et de contrôler le transfert des fichiers en définissant les stratégies de contrôle des données et en les appliquant aux groupes d'ordinateurs sur votre réseau.

Important
Le contrôle des données n'est pas pris en charge sur Windows 2008 Server Core et doit être désactivé sur les ordinateurs exécutant ce système d'exploitation. Pour exclure les ordinateurs Windows 2008 Server Core du contrôle des données, placez-les dans un groupe dont la stratégie de contrôle des données avec le contrôle des données a été désactivé. Retrouvez plus de renseignements à la section Activation ou désactivation du contrôle des données (page 156).

Les stratégies de contrôle des données incluent une ou plusieurs règles qui précisent les conditions et les actions à entreprendre en cas de correspondance à la règle. Une règle de contrôle des données peut être incluse dans plusieurs stratégies.

Lorsqu'une stratégie de contrôle des données contient plusieurs règles, un fichier qui correspond à *une quelconque* des règles de la stratégie de contrôle des données enfreint la stratégie.

Conditions de la règle du contrôle des données

Les conditions de la règle de contrôle des données incluent la destination, le nom de fichier et son extension, le type du fichier ou le contenu du fichier.

La destination inclut des périphériques (par exemple, les périphériques de stockage amovibles comme les lecteurs flash USB) et les applications (par exemple, les navigateurs Internet et les clients de messagerie).

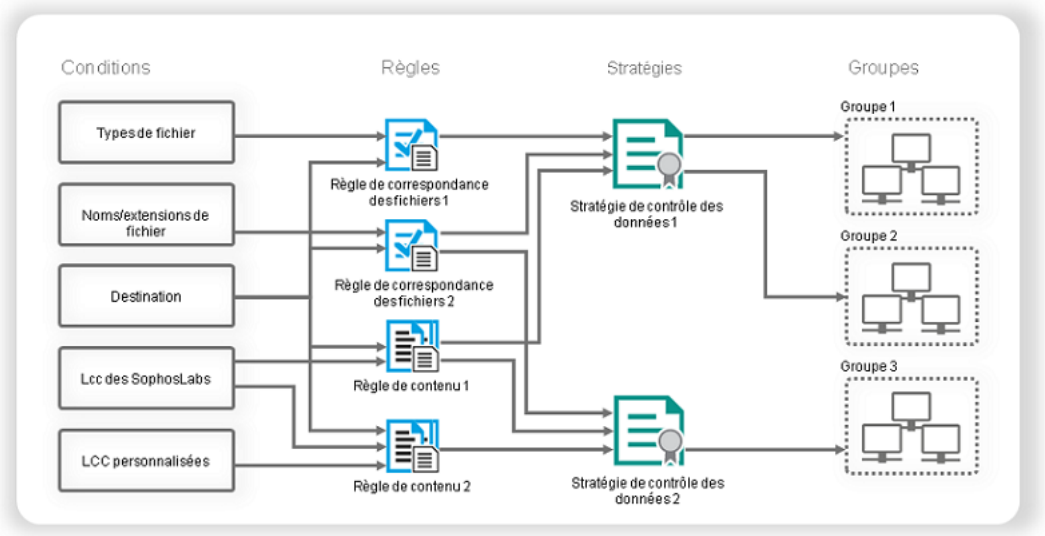
La correspondance du contenu du fichier est définie à l'aide de la Liste de contrôle du contenu. Il s'agit d'une description sous format XML de données structurées. Les SophosLabs mettent à

disposition toute une série de Listes de contrôle du contenu qui peuvent être utilisées dans vos règles de contrôle des données.

Retrouvez plus de renseignements sur les règles de contrôle des données et sur les conditions appliquées aux fichiers à la section À propos des règles de contrôle des données (page 154).

Retrouvez plus de renseignements sur les Listes de contrôle du contenu (LCC) qui définissent le contenu d'un fichier à la section À propos des Listes de contrôle du contenu (page 154).

Contrôle des données



Actions d'une règle de contrôle des données

Lorsque le contrôle des données détecte toutes les conditions spécifiées dans une règle, la correspondance de la règle est trouvée et le contrôle des données exécute l'action spécifiée dans la règle et consigne l'événement. Vous pouvez spécifier l'une des actions suivantes :

- Autoriser le transfert de fichiers et journaliser l'événement
- Autoriser le transfert après accord de l'utilisateur et journaliser l'événement
- Bloquer le transfert et journaliser l'événement

Si un fichier a pour correspondance deux règles de contrôle des données spécifiant des actions différentes, la règle spécifiant l'action la plus restrictive est appliquée. Les règles de contrôle des données qui bloquent le transfert des fichiers ont la priorité sur les règles autorisant le transfert de fichiers après acceptation par l'utilisateur. Les règles qui autorisent le transfert des fichiers après acceptation par l'utilisateur ont la priorité sur les règles qui autorisent le transfert de fichiers.

Par défaut, en cas de correspondance à une règle et de blocage du transfert des fichiers ou en cas de nécessité de confirmation par l'utilisateur du transfert des fichiers, un message apparaît sur le bureau du terminal. La règle avec correspondance est incluse dans le message. Vous pouvez ajouter vos propres messages personnalisés aux messages standard pour confirmation par l'utilisateur du transfert des fichiers et pour le transfert des fichiers bloqués. Retrouvez plus de renseignements à la section Configuration des alertes et des messages du contrôle des données (page 195).

7.4.2 À propos des règles de contrôle des données

Les règles de contrôle des données spécifient les conditions de la détection par le contrôle des données, les actions qui sont effectuées en cas de correspondance à la règle et tous les fichiers à exclure du contrôle.

Vous pouvez créer vos propres règles ou utiliser les échantillons de règles fournis. Nous fournissons un certain nombre de règles de contrôle des données préconfigurées que vous pouvez utiliser non modifiées ou personnaliser selon vos besoins. Ces règles sont fournies en guise d'exemple seulement et ne sont pas mises à jour.

Il existe deux types de règles de contrôle des données : la *règle de correspondance de fichier* et la *règle de contenu*.

Règles de correspondance de fichier

Une *règle de correspondance de fichier* précise l'action à effectuer si un utilisateur tente de transférer vers la destination spécifiée un fichier avec un nom spécifique ou d'un type donné (catégorie de type de fichier véritable comme la feuille de calcul), par exemple, le blocage du transfert des bases de données sur des périphériques de stockage amovibles.

Le contrôle des données inclut les définitions des types de fichiers véritables pour plus de 150 formats de fichiers différents. Nous pouvons de temps en temps ajouter des types de fichiers véritables supplémentaires. Les nouveaux types de fichiers ajoutés sont automatiquement ajoutés à toutes les règles de contrôle des données qui utilisent la catégorie correspondante des types de fichiers véritables.

Les types de fichiers non couverts par une définition de type de fichier véritable peuvent être identifiés à l'aide de leurs extensions de fichiers.

Règles de contenu

Une *règle de contenu* est une règle contenant une ou plusieurs Listes de contrôle du contenu et spécifiant l'action à effectuer si un utilisateur tente de transférer vers la destination spécifiée des données qui correspondent à toutes les Listes de contrôle du contenu.

7.4.3 À propos des Listes de contrôle du contenu

Une *Liste de contrôle du contenu (LCC)* est une série de conditions décrivant le contenu d'un fichier structuré. Une Liste de contrôle du contenu peut soit décrire un seul type de données (par exemple, une adresse postale ou un numéro de sécurité social), soit une combinaison de types de données (par exemple, un nom de projet qui pourrait s'apparenter au terme "confidentiel").

Vous pouvez soit utiliser les *Listes de contrôle du contenu des SophosLabs* mises à disposition par Sophos, soit créer les vôtres.

Les Listes de contrôle du contenu des SophosLabs mettent à votre disposition des définitions rédigées par des experts pour des types de données financières et personnellement identifiables les plus usuelles, par exemple, les numéros de carte de crédit, les numéros de sécurité sociale, les adresses postales ou électroniques. Des techniques de pointe telles que les sommes de contrôle sont utilisées dans les Listes de contrôle du contenu SophosLabs afin d'augmenter la précision de la détection des données sensibles.

Vous ne pouvez pas modifier les Listes de contrôle du contenu SophosLabs, en revanche, vous pouvez demander à Sophos de créer une nouvelle Liste de contrôle du contenu SophosLabs. Retrouvez plus de renseignements dans l'article 51976 de la base de connaissances de Sophos.

Remarque
Les caractères à double octets (par exemple, les caractères japonais ou chinois) ne sont pas officiellement pris en charge dans la version actuelle des Listes de contrôle du contenu. Toutefois, vous pouvez saisir des caractères à double octets dans l'éditeur de la Liste de contrôle du contenu.

Paramétrage de la quantité pour les Listes de contrôle du contenu SophosLabs

La majorité des Listes de contrôle du contenu SophosLabs ont une *quantité* attribuée.

Une *quantité* correspond au volume du type de données clé de la Liste de contrôle du contenu devant être trouvé dans un fichier avant qu'il y ait correspondance avec la Liste de contrôle du contenu. Vous pouvez modifier la quantité d'une Liste de contrôle du contenu SophosLabs dans une règle de contenu qui inclut cette Liste de contrôle du contenu.

Grâce à l'utilisation d'une quantité, vous pouvez ajuster vos règles de contrôle des données et ainsi éviter le blocage des documents qui ne contiennent pas d'informations sensibles (par exemple, un document contenant une adresse postale ou un ou deux numéros de téléphone dans l'en-tête ou dans la signature). Si vous recherchez une seule adresse postale, il se peut que des milliers de documents correspondent à la règle et qu'ils entraînent le déclenchement d'un événement de contrôle des données. Toutefois, si vous souhaitez empêcher la perte d'une liste de clients, procédez uniquement à la détection du transfert de documents contenant, par exemple, plus de 50 adresses postales. Dans d'autres cas, il est, en revanche, fortement conseillé de rechercher une seule instance du contenu, par exemple, un numéro de carte de crédit.

7.4.4 À propos des événements du contrôle des données

Lorsqu'un événement de contrôle des données se produit, par exemple, la copie d'un fichier contenant des données sensibles sur une clé USB, l'événement est envoyé à l'Enterprise Console et est visible dans le **Contrôle des données - Observateur d'événements**. L'événement est aussi journalisé localement sur le terminal et peut être visualisé, avec les droits appropriés, dans Sophos Endpoint Security and Control.

Remarque
un terminal peut envoyer à l'Enterprise Console un maximum de 50 événements de contrôle des données par heure. Tous les événements sont journalisés localement sur le terminal.

Dans la boîte de dialogue **Contrôle des données - Observateur d'événements**, vous pouvez utiliser des filtres pour n'afficher que les événements qui vous intéressent. Vous pouvez aussi exporter la liste des événements du contrôle des données dans un fichier. Retrouvez plus de renseignements aux sections À propos des événements du contrôle des données (page 155) et Exportation dans un fichier de la liste des événements (page 210).

Le nombre d'ordinateurs avec des événements de contrôle des données au-dessus d'un seuil spécifié dans les sept derniers jours apparaît sur le Tableau de bord. Retrouvez plus de renseignements sur la manière de configurer le seuil à la section Volets du tableau de bord (page 4).

Vous pouvez aussi configurer l'envoi des alertes par email aux destinataires de votre choix lorsqu'un événement de contrôle des données s'est produit. Retrouvez plus de renseignements à la section Configuration des alertes et des messages du contrôle des données (page 195).

7.4.5 Activation ou désactivation du contrôle des données

Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - contrôle des données** pour modifier une stratégie de contrôle des données.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Par défaut, le contrôle des données est désactivé et aucune règle n'est spécifiée pour surveiller ou restreindre le transfert des fichiers via le réseau.

Pour activer le contrôle des données :

1. Vérifiez quelle stratégie de contrôle des données est utilisée par le groupe ou les groupes d'ordinateurs que vous souhaitez configurer.

   Retrouvez plus de renseignements à la section Vérification des stratégies utilisées par un groupe (page 27).
2. Dans le volet **Stratégies**, cliquez deux fois sur **Contrôle des données**. Puis cliquez deux fois sur la stratégie que vous désirez changer.
   La boîte de dialogue **Stratégie de contrôle des données** apparaît.
3. Sur l'onglet **Règles de la stratégie**, sélectionnez la case à cocher **Activer le contrôle des données**.
4. Cliquez sur le bouton **Ajouter une règle**. Dans la boîte de dialogue **Gestion des règles de contrôle des données**, sélectionnez les règles que vous voulez ajouter à la stratégie et cliquez sur **OK**.

Important
Si vous n'ajoutez pas de règles de contrôle des données, ce contrôle ne surveille ou ne restreint pas le transfert des fichiers tant que vous n'avez pas exécuté cette opération.

Si vous voulez ultérieurement désactiver le contrôle des données, dessélectionnez la case à cocher **Activer le contrôle des données**.

7.4.6 Création d'une règle de correspondance des fichiers

Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Personnalisation du contrôle des données** pour créer ou modifier des règles de contrôle des données.
- Vous devez disposer du droit **Paramétrage de la stratégie - contrôle des données** pour paramétrer des stratégies de contrôle des données.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Retrouvez un aperçu des règles de correspondance des fichiers à la section À propos des règles de contrôle des données (page 154).

Pour créer une règle de correspondance des fichiers et l'ajouter à une stratégie de contrôle des données :

1. Vérifiez quelle stratégie de contrôle des données est utilisée par le groupe ou les groupes d'ordinateurs que vous souhaitez configurer.

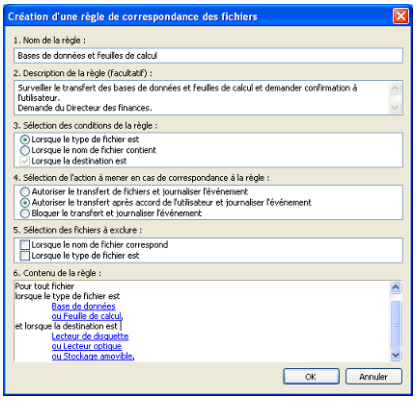
   Retrouvez plus de renseignements à la section Vérification des stratégies utilisées par un groupe (page 27).

   Sinon, vous pouvez créer une règle dans le menu **Outils** et l'ajouter ultérieurement à une ou à plusieurs stratégies. Dans le menu **Outils**, choisissez **Gérer le contrôle des données**, puis cliquez sur **Règles de contrôle des données** et exécutez les étapes 4 à 10.
2. Dans le volet **Stratégies**, cliquez deux fois sur **Contrôle des données**. Puis cliquez deux fois sur la stratégie que vous désirez changer.
3. Dans la boîte de dialogue **Stratégie de contrôle des données**, sur l'onglet **Règles de stratégie**, assurez-vous que la case à cocher **Activer le contrôle des données** est sélectionnée et cliquez sur **Gérer les règles**.
4. Dans la boîte de dialogue **Gestion des règles de contrôle des données**, cliquez sur **Ajouter une règle de correspondance au fichier**.
5. Dans la boîte de dialogue **Création d'une règle de correspondance au fichier**, sous **Nom de la règle**, saisissez un nom de règle.
6. Sous **Description de la règle (facultatif)**, saisissez la description d'une règle, si vous le souhaitez.
7. Sous **Sélectionner les conditions de la règle**, sélectionnez les conditions de la règle.

   La condition de destination est présélectionnée et doit être incluse dans la règle.

   Par défaut, tous les types de fichiers sont contrôlés. Si vous voulez contrôler seulement certains types de fichiers, sélectionnez **Lorsque le type de fichier est**. Vous pouvez alors paramétrer cette condition comme le décrit l'étape 10.
8. Sous **Sélectionner l'action en cas de correspondance**, sélectionnez l'action.
9. Si vous voulez exclure des fichiers du contrôle des données, sous **Sélectionner les fichiers à exclure**, sélectionnez la case à cocher **Lorsque le nom de fichier correspond** ou **Lorsque le type de fichier est**.
10. Sous **Règle de contenu**, cliquez sur chaque valeur soulignée et paramétrez les conditions de la règle.
    Par exemple, si vous cliquez sur **Sélectionner une destination**, la boîte de dialogue **Condition de correspondance au type de destination** s'ouvre et vous pouvez y sélectionner les périphériques et/ou les applications vers lesquels vous voulez restreindre le transfert des données.

    Sélectionnez ou saisissez les conditions pour chaque valeur soulignée.



    Cliquez sur **OK**.

    La nouvelle règle apparaît dans la boîte de dialogue **Gestion des règles de contrôle des données**.

11. Pour ajouter la règle à la stratégie, sélectionnez la case à cocher près du nom de la règle et cliquez sur **OK**.
    La règle est ajoutée à la stratégie de contrôle des données.

Vous pouvez configurer les alertes et les messages qui seront envoyés à l'utilisateur lorsqu'une correspondance à une règle est trouvée dans la stratégie de contrôle des données. Retrouvez plus de renseignements à la section Configuration des alertes et des messages du contrôle des données (page 195).

7.4.7 Création d'une règle de contenu

Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Personnalisation du contrôle des données** pour créer ou modifier des règles de contrôle des données et des Listes de contrôle du contenu.
- Vous devez disposer du droit **Paramétrage de la stratégie - contrôle des données** pour paramétrer des stratégies de contrôle des données.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Retrouvez un aperçu des règles de contenu et des listes de contrôle du contenu à la section À propos des règles de contrôle des données (page 154).

Pour créer une règle de contenu et l'ajouter à une stratégie de contrôle des données :

1. Vérifiez quelle stratégie de contrôle des données est utilisée par le groupe ou les groupes d'ordinateurs que vous souhaitez configurer.

   Retrouvez plus de renseignements à la section Vérification des stratégies utilisées par un groupe (page 27).

   Sinon, vous pouvez créer une règle dans le menu **Outils** et l'ajouter ultérieurement à une ou à plusieurs stratégies. Dans le menu **Outils**, choisissez **Gérer le contrôle des données**, puis cliquez sur **Règles de contrôle des données** et exécutez les étapes 4 à 13.
2. Dans le volet **Stratégies**, cliquez deux fois sur **Contrôle des données**. Puis cliquez deux fois sur la stratégie que vous désirez changer.
3. Dans la boîte de dialogue **Stratégie de contrôle des données**, sur l'onglet **Règles de stratégie**, assurez-vous que la case à cocher **Activer le contrôle des données** est sélectionnée et cliquez sur **Gérer les règles**.
4. Dans la boîte de dialogue **Gestion des règles de contrôle des données**, cliquez sur le bouton **Ajouter une règle de contenu**.
5. Dans la boîte de dialogue **Création d'une règle de contenu**, sous **Nom de la règle**, saisissez un nom de règle.
6. Sous **Description de la règle (facultatif)**, saisissez la description d'une règle, si vous le souhaitez.
7. Sous **Sélectionner les conditions de la règle**, le contenu du fichier et les conditions de destination sont déjà sélectionnés. Vous devez configurer les deux conditions d'une règle de contenu.
8. Sous **Sélectionner l'action en cas de correspondance**, sélectionnez l'action.
9. Si vous voulez exclure des fichiers du contrôle des données, sous **Sélectionner les fichiers à exclure**, sélectionnez la case à cocher **Lorsque le nom de fichier correspond** ou **Lorsque le type de fichier est**.
10. Sous **Règle de contenu**, cliquez sur la valeur soulignée « sélectionner le contenu du fichier ».
11. Dans la boîte de dialogue **Gestion de la Liste de contrôle du contenu**, sélectionnez les Listes de contrôle du contenu que vous voulez inclure à la règle.

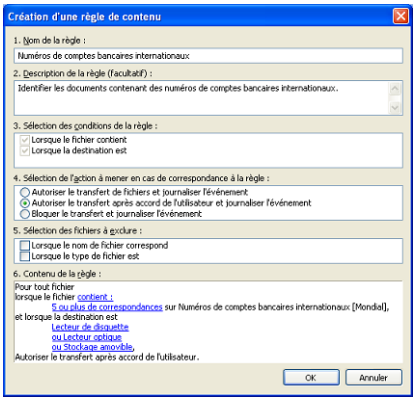
Si vous voulez ajouter les Listes de contrôle du contenu des SophosLabs, sélectionnez-en une pour chaque pays dont vous avez besoin.

Conseil
Ne sélectionnez pas une Liste de contrôle de contenu globale si vous n'avez pas besoin de prendre en charge tous les pays. Sélectionnez plutôt les Listes de contrôle de contenu des pays dont vous avez besoin. Ceci vous permettra de réduire considérablement le temps de contrôle et de réduire le risque de correspondances non désirées ou accidentelles.

Retrouvez plus de renseignements sur la création d'une nouvelle liste de contrôle du contenu à la section Création ou modification d'une Liste de contrôle du contenu simple (page 162) ou Création ou modification d'une Liste de contrôle du contenu avancée (page 163).

Cliquez sur **OK**.

12. Si vous voulez changer la quantité attribuée à une Liste de contrôle du contenu des SophosLabs, sous **Contenu de la règle**, cliquez sur la valeur soulignée « quantité » (« *n* ou plus de correspondances ») que vous voulez changer. Dans la boîte de dialogue **Éditeur de quantité**, saisissez une nouvelle quantité. Retrouvez plus de renseignements à la section À propos des Listes de contrôle du contenu (page 154).
13. Sous **Contenu de la règle**, sélectionnez ou saisissez les conditions pour le reste des valeurs soulignées.



Cliquez sur **OK**.

La nouvelle règle apparaît dans la boîte de dialogue **Gestion des règles de contrôle des données**.

14. Pour ajouter la règle à la stratégie, sélectionnez la case à cocher près du nom de la règle et cliquez sur **OK**.
La règle est ajoutée à la stratégie de contrôle des données.

Vous pouvez configurer les alertes et les messages qui seront envoyés à l'utilisateur lorsqu'une correspondance à une règle est trouvée dans la stratégie de contrôle des données. Retrouvez plus de renseignements à la section Configuration des alertes et des messages du contrôle des données (page 195).

7.4.8 Ajout d'une règle de contrôle des données à une stratégie

Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - contrôle des données** pour réaliser cette tâche.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Pour ajouter une règle de contrôle des données à une stratégie :

1. Vérifiez quelle stratégie de contrôle des données est utilisée par le groupe ou les groupes d'ordinateurs que vous souhaitez configurer.

   Retrouvez plus de renseignements à la section Vérification des stratégies utilisées par un groupe (page 27).
2. Dans le volet **Stratégies**, cliquez deux fois sur **Contrôle des données**. Puis cliquez deux fois sur la stratégie que vous désirez changer.
   La boîte de dialogue **Stratégie de contrôle des données** apparaît.
3. Sur l'onglet **Règles de la stratégie**, cliquez sur **Ajouter une règle**.
   La boîte de dialogue **Gestion des règles de contrôle des données** apparaît.
4. Sélectionnez les règles que vous voulez ajouter au profil et cliquez sur **OK**.

7.4.9 Suppression d'une règle de contrôle des données d'une stratégie

Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - contrôle des données** pour réaliser cette tâche.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Pour supprimer une règle de contrôle des données d'une stratégie :

1. Vérifiez quelle stratégie de contrôle des données est utilisée par le groupe ou les groupes d'ordinateurs que vous souhaitez configurer.

   Retrouvez plus de renseignements à la section Vérification des stratégies utilisées par un groupe (page 27).
2. Dans le volet **Stratégies**, cliquez deux fois sur **Contrôle des données**. Puis cliquez deux fois sur la stratégie que vous désirez changer.
   La boîte de dialogue **Stratégie de contrôle des données** apparaît.
3. Sur l'onglet **Règles de stratégie**, sélectionnez la règle que vous voulez supprimer et cliquez sur **Supprimer**.

7.4.10 Exclusion de fichiers ou de types de fichiers du contrôle des données

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Personnalisation du contrôle des données** pour exclure des fichiers du contrôle des données. Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Vous pouvez exclure des fichiers et des types de fichiers du contrôle des données en paramétrant les exclusions dans une règle de contrôle des données.

Pour exclure un fichier ou un type de fichier du contrôle des données, excluez-le dans une règle possédant la priorité la plus élevée (c'est-à-dire, spécifiant l'action la plus restrictive).

Pour exclure des fichiers ou des types de fichiers du contrôle des données :

1. Dans le menu **Outils**, choisissez **Gérer le contrôle des données**, puis cliquez sur **Règles de contrôle des données**.

2. Dans la boîte de dialogue **Gestion des règles de contrôle des données**, sélectionnez la règle que vous voulez modifier et cliquez sur **Modifier**, ou créez une nouvelle règle en cliquant sur le bouton **Ajouter une règle de correspondance au fichier** ou **Ajouter une règle de contenu**.
3. Pour exclure des fichiers du contrôle des données, dans la boîte de dialogue **Éditeur de règle**, sous **Sélectionner les fichiers à exclure**, sélectionnez la case à cocher **Lorsque le nom de fichier correspond**.
4. Sous **Règle de contenu**, cliquez sur la valeur soulignée pour spécifier les noms des fichiers exclus.
5. Dans la boîte de dialogue **Exclusion à la condition du nom de fichier**, cliquez sur **Ajouter** et spécifiez les noms des fichiers que vous voulez exclure.

   Vous pouvez utiliser les caractères de remplacement * et ?

   Le caractère joker ? peut seulement être utilisé dans un nom de fichier ou dans une extension. Il permet généralement de retrouver n'importe quel caractère. En revanche, lorsqu'il est utilisé à la fin d'un nom de fichier ou d'une extension, il ne retrouve que les caractères uniques ou n'en retrouve pas. Par exemple, fichier??.txt permet de retrouver fichier.txt, fichier1.txt et fichier12.txt, mais pas fichier123.txt.

   Le caractère de remplacement * peut seulement être utilisé dans un nom de fichier ou dans une extension, sous la forme [nomfichier].* ou *.[extension]. Par exemple, fichier*.txt, fichier.txt* et fichier.*txt sont incorrects.
6. Pour exclure des types de fichiers du contrôle des données, dans la boîte de dialogue **Éditeur de règle**, sous **Sélectionner les fichiers à exclure**, sélectionnez la case à cocher **Lorsque le nom de fichier correspond**.
7. Sous **Règle de contenu**, cliquez sur la valeur soulignée pour spécifier des types de fichiers exclus.
8. Dans la boîte de dialogue **Exclusion de la condition de type de fichiers**, sélectionnez les types de fichiers que vous voulez exclure et cliquez sur **OK**.

7.4.11 Importation ou exportation d'une règle de contrôle des données

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Personnalisation du contrôle des données** pour importer ou exporter une règle de contrôle des données. Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Les règles de contrôle des données peuvent être importées dans ou exportées depuis l'Enterprise Console sous la forme de fichiers XML.

Pour importer ou exporter une règle de contrôle des données :

1. Dans le menu **Outils**, choisissez **Gérer le contrôle des données**, puis cliquez sur **Règles de contrôle des données**.
2. Dans la boîte de dialogue **Gestion des règles de contrôle des données**, cliquez sur le bouton **Importer** ou **Exporter**.
   - Si vous voulez importer une règle, dans la boîte de dialogue **Importer**, naviguez jusqu'à la règle que vous voulez importer, sélectionnez-la et cliquez sur **Ouvrir**.
   - Si vous voulez exporter une règle, dans la boîte de dialogue **Exporter**, naviguez pour sélectionner une destination pour le fichier, saisissez le nom du fichier et cliquez sur **Enregistrer**.

7.4.12 Création ou modification d'une Liste de contrôle du contenu simple

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Personnalisation du contrôle des données** pour créer une Liste de contrôle du contenu. Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Retrouvez un aperçu des listes de contrôle du contenu à la section À propos des Listes de contrôle du contenu (page 154).

Pour créer ou modifier une Liste de contrôle du contenu :

1. Dans le menu **Outils**, choisissez **Gérer le contrôle des données**, puis cliquez sur **Listes de contrôle du contenu du contrôle des données**.
2. Dans la boîte de dialogue **Gestion des Listes de contrôle du contenu**, cliquez sur **Ajouter** pour créer une nouvelle Liste de contrôle du contenu ou sélectionnez-en une existante et cliquez sur **Modifier**.
3. Dans la boîte de dialogue **Ajout d'une Liste de contrôle du contenu**, dans le champ **Nom**, saisissez un nom de Liste de contrôle du contenu.
4. Dans le champ **Description**, saisissez une description de Liste de contrôle du contenu, si vous le souhaitez.
5. Si vous voulez ajouter des balises ou modifier les balises affectées à la Liste de contrôle du contenu, cliquez sur **Changer** près du champ **Balises**.

   Vous pouvez attribuer des balises pour identifier le type de Liste de contrôle du contenu et la zone où il s'applique.
6. Dans la boîte de dialogue **Modification des balises de la Liste de contrôle du contenu**, dans la liste **Balises disponibles**, sélectionnez les balises que vous voulez attribuer et déplacez-les dans la liste **Balises sélectionnées**. Cliquez sur **OK**.
7. Dans la section **Recherche de correspondances du contenu**, sélectionnez une condition de recherche ("Un de ces termes", "Tous ces termes" ou "Cette phrase exactement") et saisissez les termes que vous voulez rechercher dans les documents, séparés par un espace. Cliquez sur **OK**.

   Remarque
   La recherche n'est pas sensible aux majuscules.

   Les guillemets ne sont pas reconnus dans les Listes de contrôle du contenu simples. Utilisez la condition « Cette phrase exactement » pour rechercher une phrase exacte via un contrôle.

   Pour créer des expressions plus complexes, utilisez l'éditeur avancé de Liste de contrôle du contenu comme indiqué à la section Création ou modification d'une Liste de contrôle du contenu avancée (page 163).

La nouvelle Liste de contrôle du contenu apparaît dans la boîte de dialogue **Gestion des Listes de contrôle du contenu**.

Exemples

Condition de recherche	Exemple	Description
Tout terme correspondant	confidentiel secret	Retrouve les documents contenant « confidentiel » ou « secret ».
Tous les termes correspondants	projet confidentiel	Retrouve les documents contenant à la fois « projet » et « confidentiel ».
Correspondance exacte	pour une utilisation interne seulement	Retrouve les documents contenant la phrase « pour une utilisation interne seulement ».

Maintenant, vous pouvez ajouter la nouvelle Liste de contrôle du contenu.

7.4.13 Création ou modification d'une Liste de contrôle du contenu avancée

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Personnalisation du contrôle des données** pour créer une Liste de contrôle du contenu. Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Retrouvez un aperçu des listes de contrôle du contenu à la section À propos des Listes de contrôle du contenu (page 154).

Vous pouvez créer une Liste de contrôle du contenu contenant une ou plusieurs expressions régulières et un score de déclenchement. Pour cela, utilisez l'éditeur avancé.

Pour créer ou modifier une Liste de contrôle du contenu à l'aide de l'éditeur avancé :

1. Dans le menu **Outils**, choisissez **Gérer le contrôle des données**, puis cliquez sur **Listes de contrôle du contenu du contrôle des données**.
2. Dans la boîte de dialogue **Gestion des Listes de contrôle du contenu**, cliquez sur **Ajouter** pour créer une nouvelle Liste de contrôle du contenu ou sélectionnez-en une existante et cliquez sur **Modifier**.
3. Dans la boîte de dialogue **Ajout d'une Liste de contrôle du contenu**, dans le champ **Nom**, saisissez un nom de Liste de contrôle du contenu.
4. Dans le champ **Description**, saisissez une description de Liste de contrôle du contenu, si vous le souhaitez.
5. Si vous voulez ajouter des balises ou modifier les balises affectées à la Liste de contrôle du contenu, cliquez sur **Changer** près du champ **Balises**.

   Vous pouvez attribuer des balises pour identifier le type de Liste de contrôle du contenu et la zone où il s'applique.
6. Dans la boîte de dialogue **Modification des balises de la Liste de contrôle du contenu**, dans la liste **Balises disponibles**, sélectionnez les balises que vous voulez attribuer et déplacez-les dans la liste **Balises sélectionnées**. Cliquez sur **OK**.
7. Cliquez sur l'onglet **Avancé**.

8. Dans le volet **Avancés**, cliquez sur **Créer** pour créer une nouvelle expression ou sélectionner une expression existante et cliquez sur **Modifier**.
9. Dans la boîte de dialogue **Liste de contrôle du contenu - Avancée**, saisissez une expression régulière Perl 5.

   Retrouvez une description des expressions régulières Perl 5 dans la documentation Perl ou sur http://www.boost.org/doc/libs/1_34_1/libs/regex/doc/syntax_perl.html.
10. Dans le champ **Score de l'expression**, saisissez le nombre qui sera ajouté au score total d'une Liste de contrôle du contenu lorsque l'expression régulière sera trouvée.
11. Dans le champ **Décompte maximum**, saisissez le nombre maximum de correspondances d'une expression régulière pouvant être comptabilisées jusqu'au résultat total.
    Par exemple, une expression avec un score de 5 et un compte maximum de 2 peut ajouter un maximum de 10 au score total de la Liste de contrôle du contenu. Si l'expression est trouvée 3 fois, cela ajoute tout de même 10 au score total.

    Cliquez sur **OK**.
12. Répétez les étapes 5 à 11 si vous voulez ajouter des expressions plus régulières à la Liste de contrôle du contenu.
13. Dans le champ **Seuil de déclenchement**, saisissez le nombre de fois qu'une expression régulière doit être trouvée avant qu'il y ait correspondance avec une Liste de contrôle du contenu.

    Par exemple, considérez une Liste de contrôle du contenu avec un seuil de déclenchement de 8 et comprenant 3 expressions (A, B et C) avec les scores et les décomptes maximums suivants :

Expression	Score	Décompte maximum
Expression A	5	2
Expression B	3	1
Expression C	1	5

    La correspondance à cette Liste de contrôle du contenu est trouvée si le contrôle des données trouve 2 correspondances à l'expression 1 ou 1 à l'expression 1 et 1 à l'expression 2, ou 1 à l'expression 2 et 5 à l'expression 3.

    Cliquez sur **OK**.

La nouvelle Liste de contrôle du contenu apparaît dans la boîte de dialogue **Gestion des Listes de contrôle du contenu**.

Exemple d'expression régulière

```
(?i)\b[a-ceghj-npr-tw-z][a-ceghj-npr-tw-z]\s?\d{2}\s?\d{2}\s?\d{2}\s?
[abcd]?\b
```

Cette expression régulière correspond aux numéros de sécurité nationaux RU, par exemple, AA 11 11 11 A.

(?i)	Rend la correspondance trouvée insensible à la casse.
\b	Correspond à une limite entre un caractère lettre et un caractère autre que lettre.

[a-ceghj-npr-tw-z]	Correspond à tout caractère dans une série de caractères (A à C E G H J à N P R à T W à Z).
?	Correspond à l'élément précédent zéro ou une fois.
\s?	Correspond à zéro ou un espace blanc.
\d{2}	Correspond à deux chiffres.
[abcd]	Correspond à tout caractère de la liste (A, B, C ou D).

Maintenant, vous pouvez ajouter la nouvelle Liste de contrôle du contenu.

7.4.14 Importation ou exportation d'une Liste de contrôle du contenu

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Personnalisation du contrôle des données** pour importer ou exporter une Liste de contrôle du contenu. Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Les Listes de contrôle du contenu peuvent être importées dans ou exportées depuis l'Enterprise Console sous la forme de fichiers XML. Vous pouvez partager les Listes de contrôle du contenu entre les produits Sophos qui les prennent en charge.

Remarque
les Listes de contrôle du contenu des SophosLabs ne peuvent pas être exportées.

Pour importer ou exporter une Liste de contrôle du contenu :

1. Dans le menu **Outils**, choisissez **Gérer le contrôle des données**, puis cliquez sur **Listes de contrôle du contenu du contrôle des données**.
2. Dans la boîte de dialogue **Gestion des Listes de contrôle du contenu**, cliquez sur le bouton **Importer** ou **Exporter**.
   - Si vous voulez importer une Liste de contrôle du contenu, dans la boîte de dialogue **Importer**, naviguez jusqu'à la liste que vous voulez importer, sélectionnez-la et cliquez sur **Ouvrir**.
   - Si vous voulez exporter une Liste de contrôle du contenu, dans la boîte de dialogue **Exporter**, naviguez pour sélectionner une destination pour le fichier, saisissez le nom du fichier et cliquez sur **Enregistrer**.

7.5 Stratégie de contrôle des périphériques

Remarque
Cette fonction n'est pas incluse dans toutes les licences. Si vous voulez l'utiliser, il se peut que vous deviez changer votre contrat de licence. Retrouvez plus de renseignements à la section http://www.sophos.com/fr-fr/products/complete/comparison.aspx.

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 vos utilisateurs d'utiliser sur leurs ordinateurs des périphériques de stockage externes, des supports de stockage amovibles et des technologies de connexion sans fil non autorisés. Ceci réduit considérablement votre exposition aux pertes accidentelles de données et limite les possibilités pour les utilisateurs d'introduire des logiciels n'appartenant pas à votre environnement réseau.

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

Grâce au contrôle des périphériques, vous réduisez aussi considérablement les risques de création de ponts entre un réseau professionnel et un réseau non professionnel. Le mode **Bloquer le pont** est disponible pour les types de périphériques à la fois sans fil et modem. Ce mode fonctionne en désactivant les adaptateurs réseau sans fil ou modem lorsqu'un terminal est connecté à un réseau physique (généralement, via une connexion Ethernet). Une fois l'ordinateur déconnecté du réseau physique, les adaptateurs réseau sans fil ou modem sont réactivés de manière transparente.

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

Si vous voulez activer le contrôle des périphériques pour la première fois, nous vous conseillons de :

- Sélectionner les types de périphériques à contrôler.
- Détecter les périphériques sans les bloquer.
- Utiliser les événements de contrôle des périphériques pour décider quels types de périphériques bloquer et, le cas échéant, lesquels doivent être exemptés.
- Détecter et bloquer ou autoriser l'accès en lecture seule aux périphériques de stockage.

Retrouvez plus de renseignements sur les paramètres conseillés pour le contrôle des périphériques dans le *Guide de configuration des stratégies de Sophos Enterprise Console*.

Remarque
Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - contrôle des périphériques** pour configurer une stratégie de contrôle des périphériques.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

7.5.1 À propos des événements du contrôle des périphériques

Lorsqu'un événement de contrôle des périphériques se produit, par exemple, un périphérique de stockage amovible a été bloqué, l'événement est envoyé à l'Enterprise Console et est visible dans la boîte de dialogue **Contrôle des périphériques - Observateur d'événements**.

Remarque
Si vous définissez les lecteurs de disques optiques sur « Lecture seule », les événements liés à ces lecteurs de disque ne sont pas envoyés à l'Enterprise Console ni journalisés localement. Ces mesures évitent la création de rapports d'événements non désirés.

Dans la boîte de dialogue **Contrôle des périphériques - Observateur d'événements**, vous pouvez utiliser des filtres pour n'afficher que les événements qui vous intéressent. Vous pouvez aussi exporter la liste des événements du contrôle des périphériques dans un fichier. Retrouvez plus de renseignements aux sections À propos des événements du contrôle des périphériques (page 166) et Exportation dans un fichier de la liste des événements (page 210).

Vous pouvez utiliser les événements de contrôle des périphériques pour ajouter des exemptions pour des périphériques spécifiques ou des modèles de périphériques aux stratégies de contrôle des périphériques. Retrouvez plus de renseignements sur l'exemption de périphériques à la section Exemption d'un périphérique d'une seule stratégie (page 171) ou Exemption d'un périphérique de toutes les stratégies (page 170).

Le nombre d'ordinateurs avec des événements de contrôle des périphériques au-dessus d'un seuil spécifié dans les sept derniers jours apparaît sur le Tableau de bord. Retrouvez plus de renseignements sur la manière de configurer le seuil à la section Configuration du tableau de bord (page 49).

Vous pouvez aussi configurer l'envoi des alertes par email aux destinataires de votre choix lorsqu'un événement de contrôle des périphériques s'est produit. Retrouvez plus de renseignements à la section Configuration des alertes et des messages du contrôle des périphériques (page 196).

7.5.2 Quels types de périphériques peuvent être contrôlés ?

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

Stockage

- Périphériques de stockage amovible (par exemple, les clés USB à mémoire flash, les lecteurs de cartes PC et les lecteurs de disques durs externes)
- Lecteurs de supports optiques (lecteurs de CD-ROM/DVD/Blu-ray)
- Lecteurs de disquette
- Périphériques de stockage amovibles sécurisés (par exemple, les clés USB chiffrées)

Retrouvez une liste des périphériques de stockage amovibles sécurisés pris en charge dans l'article 63102 de la base de connaissances Sophos.

Conseil
À l'aide de la catégorie de stockage amovible sécurisé, vous pouvez facilement autoriser l'utilisation de périphériques de stockage amovibles sécurisés pris en charge tout en en bloquant d'autres.

Réseau

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

Pour les interfaces réseau, vous pouvez aussi sélectionner le mode **Bloquer le pont** qui aide à réduire considérablement tout risque de création de ponts réseaux, par exemple entre un réseau professionnel et un réseau non professionnel. Ce mode fonctionne en désactivant les adaptateurs réseau sans fil ou modem lorsqu'un terminal est connecté à un réseau physique (généralement,

via une connexion Ethernet). Une fois l'ordinateur déconnecté du réseau physique, les adaptateurs réseau sans fil ou modem sont réactivés de manière transparente.

Courte portée

- Interfaces Bluetooth
- Infrarouge (interfaces infrarouge IrDA)

Le contrôle des périphériques bloque à la fois les périphériques et les interfaces internes et externes. Par exemple, une stratégie bloquant les interfaces Bluetooth bloquera :

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

Supports

- MTP/PTP

  Ceci inclut les téléphones mobiles, les tablettes, les appareils photos numériques, les lecteurs multimédia et autres appareils se connectant à un ordinateur à l'aide des protocoles MTP (Media Transfer Protocol) ou PTP (Picture Transfer Protocol).

7.5.3 Sélection des types de périphériques à contrôler

Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - contrôle des périphériques** pour modifier une stratégie de contrôle des périphériques.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Important
Ne bloquez pas les connexions Wi-Fi sur les ordinateurs qui sont administrés par l'Enterprise Console via Wi-Fi.

1. Vérifiez quelle stratégie de contrôle des applications est utilisée par le ou les groupes d'ordinateurs que vous souhaitez configurer.

   Retrouvez plus de renseignements à la section Vérification des stratégies utilisées par un groupe (page 27).
2. Dans le volet **Stratégies**, cliquez deux fois sur **Contrôle des données**. Puis cliquez deux fois sur la stratégie que vous désirez changer.
3. Dans la boîte de dialogue **Stratégie de contrôle des périphériques**, sur l'onglet **Configuration**, sous **Stockage**, sélectionnez le type de périphérique de stockage que vous voulez contrôler.
4. Cliquez dans la colonne **État** près du type de périphérique, puis cliquez sur la flèche du menu déroulant qui apparaît. Sélectionnez le type d'accès que vous voulez autoriser.

   Par défaut, les périphériques ont un accès complet. Pour les périphériques de stockage amovibles, les unités de disque optiques et les lecteurs de disquettes, vous pouvez changer en « Bloquées » ou en « Lecture seule ». Pour les périphériques de stockage amovibles sécurisés, vous pouvez changer en « Bloqué ».
5. Sous **Réseau**, sélectionnez le type de périphérique réseau que vous voulez bloquer.

6. Cliquez dans la colonne **État** près du type de périphérique réseau, puis cliquez sur la flèche du menu déroulant qui apparaît.
   - Sélectionnez « Bloqué » si vous voulez bloquer le type de périphérique.
   - Sélectionnez « Bloquer le pont » si vous voulez empêcher la création d'un pont entre un réseau professionnel et un réseau non professionnel. Le type de périphérique sera bloqué lorsqu'un terminal sera connecté à un réseau physique (généralement via une connexion Ethernet). Une fois que le terminal est déconnecté du réseau physique, le type de périphérique sera réactivé.
7. Sous **Courte portée**, sélectionnez le type de périphérique de courte portée que vous voulez bloquer. Dans la colonne **État** près du type de périphérique, sélectionnez « Bloqué ».

   Cliquez sur **OK**.
8. Pour bloquer les appareils multimédia qui se connectent à un ordinateur par MTP (Media Transfer Protocol) ou PTP (Picture Transfer Protocol), tels que les téléphones mobiles, les tablettes, les appareils photos numériques ou les lecteurs multimédia, sous **Supports**, sélectionnez **MTP/PTP**. Dans la colonne **État**, sélectionnez « Bloqué ».

7.5.4 Détection des périphériques sans les bloquer

Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - contrôle des périphériques** pour modifier une stratégie de contrôle des périphériques.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Vous pouvez détecter des périphériques sans les bloquer. Ceci est utile si vous avez l'intention de bloquer des périphériques à l'avenir, mais voulez d'abord détecter et exempter les périphériques dont vous avez besoin.

Pour détecter les périphériques sans les bloquer, activez le contrôle des périphériques dans une stratégie de contrôle des périphériques et activez le mode *détection seulement*. Changez l'état des périphériques que vous souhaitez détecter sur « Bloqué ». Ceci générera des événements pour les périphériques utilisés sur les terminaux si la stratégie est enfreinte, mais les périphériques ne seront pas bloqués.

Retrouvez plus de renseignements sur la consultation des événements de contrôle des périphériques à la section À propos des événements du contrôle des périphériques (page 166).

Pour détecter des périphériques sans les bloquer :

1. Vérifiez quelle stratégie de contrôle des applications est utilisée par le ou les groupes d'ordinateurs que vous souhaitez configurer.

   Retrouvez plus de renseignements à la section Vérification des stratégies utilisées par un groupe (page 27).
2. Dans le volet **Stratégies**, cliquez deux fois sur **Contrôle des données**. Puis cliquez deux fois sur la stratégie que vous désirez changer.
3. Dans la boîte de dialogue **Stratégie de contrôle des périphériques**, sur l'onglet **Configuration**, sélectionnez **Activer le contrôle des périphériques**.
4. Sélectionnez **Détecter mais ne pas bloquer les périphériques**.
5. Si vous ne l'avez pas encore fait, changez l'état des périphériques que vous voulez détecter sur « Bloqué ». Retrouvez plus de renseignements à la section Sélection des types de périphériques à contrôler (page 168).

   Cliquez sur **OK**.

7.5.5 Détection et blocage des périphériques

Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - contrôle des périphériques** pour modifier une stratégie de contrôle des périphériques.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

1. Vérifiez quelle stratégie de contrôle des applications est utilisée par le ou les groupes d'ordinateurs que vous souhaitez configurer.

   Retrouvez plus de renseignements à la section Vérification des stratégies utilisées par un groupe (page 27).
2. Dans le volet **Stratégies**, cliquez deux fois sur **Contrôle des données**. Puis cliquez deux fois sur la stratégie que vous désirez changer.
3. Dans la boîte de dialogue **Stratégie de contrôle des périphériques**, sur l'onglet **Configuration**, sélectionnez la case à cocher **Activer le contrôle des périphériques**.
4. Dessélectionnez la case à cocher **Détecter mais ne pas bloquer les périphériques**.
5. Si vous ne l'avez pas encore fait, changez l'état des périphériques que vous voulez bloquer sur « Bloqué ». Retrouvez plus de renseignements à la section Sélection des applications à contrôler (page 148).

   Cliquez sur **OK**.

7.5.6 Exemption d'un périphérique de toutes les stratégies

Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - contrôle des périphériques** pour modifier une stratégie de contrôle des périphériques.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Vous pouvez exempter un périphérique de toutes les stratégies, y compris de celle par défaut. Cette exception sera alors ajoutée à toutes les stratégies que vous créez.

Vous pouvez exempter l'instance d'un périphérique (« ce périphérique uniquement ») ou un modèle particulier de périphérique (« Tous les périphériques avec cet ID du modèle ») de périphérique. Ne définissez pas plusieurs exemptions pour le même périphérique sous les champs ID du modèle et ID du périphérique. Si les deux sont définis, le niveau de l'instance du périphérique aura priorité.

Pour exempter un périphérique de toutes les stratégies de contrôle des périphériques :

1. Dans le menu **Événements**, 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.

   Retrouvez plus de renseignements à la section À propos des événements du contrôle des périphériques (page 166).
3. Sélectionnez l'entrée du périphérique que vous voulez exempter des stratégies, puis cliquez sur **Exempter un périphérique**.

La boîte de dialogue **Exemption d'un périphérique** apparaît. Sous **Détails du périphérique**, le type, le modèle, l'ID du modèle et l'ID du périphérique apparaissent. Sous **Détails de l'exemption**, **Étendue**, les mots « Toutes les stratégies » apparaissent.

Remarque
S'il n'y a aucun événement pour le périphérique que vous voulez exempter, par exemple, un lecteur de CD-ROM ou de DVD sur un terminal, allez sur l'ordinateur contenant le périphérique et activez ce dernier dans le Gestionnaire de périphériques (pour accéder au Gestionnaire des périphériques, cliquez avec le bouton droit de la souris **Poste de travail**, cliquez sur **Gérer**, puis cliquez sur **Gestionnaire de périphériques**). Ceci générera un nouvel événement de « blocage » qui apparaîtra dans la boîte de dialogue **Contrôle des périphériques - Observateur d'événements**. Vous pouvez ensuite exempter le périphérique comme le décrit plus haut cette étape.

4. Indiquez si vous voulez exempter ce périphérique uniquement ou tous les périphériques avec cet ID du modèle.
5. Indiquez si vous voulez autoriser un accès complet ou un accès en lecture seule au périphérique.
6. Dans le champ **Commentaire**, saisissez si vous le souhaitez un commentaire. Par exemple, vous pouvez indiquer qui a fait la demande d'exemption du périphérique.
7. Cliquez sur **OK**.

7.5.7 Exemption d'un périphérique d'une seule stratégie

Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - contrôle des périphériques** pour modifier une stratégie de contrôle des périphériques.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Vous pouvez exempter un périphérique donné d'une stratégie de contrôle des périphériques.

Vous pouvez exempter l'instance d'un périphérique (« ce périphérique uniquement ») ou un modèle particulier de périphérique (« Tous les périphériques avec cet ID du modèle ») de périphérique. Ne définissez pas plusieurs exemptions pour le même périphérique sous les champs ID du modèle et ID du périphérique. Si les deux sont définis, le niveau de l'instance du périphérique aura priorité.

Pour exempter un périphérique d'une stratégie :

1. Vérifiez quelle stratégie de contrôle des applications est utilisée par le ou les groupes d'ordinateurs que vous souhaitez configurer.

   Retrouvez plus de renseignements à la section Vérification des stratégies utilisées par un groupe (page 27).
2. Dans le volet **Stratégies**, cliquez deux fois sur **Contrôle des données**. Puis cliquez deux fois sur la stratégie que vous désirez changer.
3. Dans la boîte de dialogue **Stratégie de contrôle des périphériques**, sur l'onglet **Configuration**, sélectionnez **Ajouter exemption**.
   La boîte de dialogue **Contrôle des périphériques - Observateur d'événements** apparaît.
4. Si vous voulez afficher certains événements seulement, dans le volet **Critères de recherche**, définissez les filtres de façon appropriée et cliquez sur **Rechercher** pour afficher les événements.

   Retrouvez plus de renseignements à la section À propos des événements du contrôle des périphériques (page 166).

5. Sélectionnez l'entrée du périphérique que vous voulez exempter de la stratégie, puis cliquez sur **Exempter un périphérique**.

   La boîte de dialogue **Exemption d'un périphérique** apparaît. Sous **Détails du périphérique**, le type, le modèle, l'ID du modèle et l'ID du périphérique apparaissent. Sous **Détails de l'exemption**, **Étendue**, vous voyez apparaître « Cette stratégie uniquement ».

   Remarque
   S'il n'y a aucun événement pour le périphérique que vous voulez exempter, par exemple, un lecteur de CD-ROM ou de DVD sur un terminal, allez sur l'ordinateur contenant le périphérique et activez ce dernier dans le Gestionnaire de périphériques (pour accéder au Gestionnaire des périphériques, cliquez avec le bouton droit de la souris **Poste de travail**, cliquez sur **Gérer**, puis cliquez sur **Gestionnaire de périphériques**). Ceci générera un nouvel événement de « blocage » qui apparaîtra dans la boîte de dialogue **Contrôle des périphériques - Observateur d'événements**. Vous pouvez ensuite exempter le périphérique comme le décrit plus haut cette étape.

6. Indiquez si vous voulez exempter ce périphérique uniquement ou tous les périphériques avec cet ID du modèle.
7. Indiquez si vous voulez autoriser un accès complet ou un accès en lecture seule au périphérique.
8. Dans le champ **Commentaire**, saisissez si vous le souhaitez un commentaire. Par exemple, vous pouvez indiquer qui a fait la demande d'exemption du périphérique.
9. Cliquez sur **OK**.

7.5.8 Affichage ou modification de la liste de périphériques exemptés

Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - contrôle des périphériques** pour modifier une stratégie de contrôle des périphériques.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Pour voir ou modifier la liste de périphériques exemptés :

1. Vérifiez quelle stratégie de contrôle des applications est utilisée par le ou les groupes d'ordinateurs que vous souhaitez configurer.

   Retrouvez plus de renseignements à la section Vérification des stratégies utilisées par un groupe (page 27).
2. Dans le volet **Stratégies**, cliquez deux fois sur **Contrôle des données**. Puis cliquez deux fois sur la stratégie que vous désirez changer.
3. Dans la boîte de dialogue **Stratégie de contrôle des périphériques**, sur l'onglet **Configuration**, sélectionnez le type de périphérique pour lequel vous voulez visualiser les exemptions, par exemple, le lecteur optique. Cliquez sur **Voir les exemptions**.
   La boîte de dialogue **Exemptions de <Type de périphérique>** apparaît. Si une exemption concerne tous les périphériques avec cet ID du modèle, le champ **ID du périphérique** est vide.
4. Si vous voulez modifier la liste des périphériques exemptés, effectuez l'une des opérations suivantes :
   - Si vous voulez ajouter une exemption, cliquez sur **Ajouter**. Retrouvez plus de renseignements à la section Exemption d'un périphérique d'une seule stratégie (page 171).

- Si vous voulez modifier une exemption, sélectionnez-la et cliquez sur **Modifier**. Modifiez les paramètres dans la boîte de dialogue **Exemption d'un périphérique** comme vous le souhaitez.
- Si vous voulez supprimer une exemption, sélectionnez le périphérique exempté et cliquez sur **Supprimer**.

  Ceci le supprime de la stratégie que vous modifiez. Si vous voulez supprimer le périphérique d'autres stratégies, répétez les étapes de cette tâche pour chaque stratégie.

7.6 Stratégie de protection antialtération

La protection antialtération vous permet d'interdire aux utilisateurs non autorisés (administrateurs locaux et utilisateurs ayant peu d'expérience technique) et aux programmes malveillants connus de désinstaller les logiciels de sécurité de Sophos ou de les désactiver par le biais de l'interface Sophos Endpoint Security and Control.

Remarque
La protection antialtération n'est pas conçue pour assurer une protection contre les utilisateurs expérimentés techniquement. Elle n'assure pas non plus la protection contre les programmes malveillants spécifiquement conçus pour corrompre le système d'exploitation afin d'éviter d'être détecté. Ce type de programmes malveillants est uniquement détecté en effectuant un contrôle à la recherche de menaces et de comportements suspects. Retrouvez plus de renseignements à la section Stratégie antivirus et HIPS (page 81).

Après avoir activé la protection antialtération et créé un mot de passe, un membre du groupe SophosAdministrator sur le terminal qui ne connaît pas le mot de passe ne pourra pas :

- Reconfigurer les paramètres du contrôle sur accès ou de la détection des comportements suspects dans Sophos Endpoint Security and Control.
- Désactiver la protection antialtération.
- Désinstaller les composants de Sophos Endpoint Security and Control (Sophos Anti-Virus, Sophos Client Firewall, Sophos AutoUpdate ou Sophos Remote Management System).

Si vous voulez permettre aux SophosAdministrators d'exécuter ces tâches, vous devez leur fournir le mot de passe de la protection antialtération afin qu'ils puissent s'authentifier.

La protection antialtération n'affecte pas les membres des groupes SophosUser et SophosPowerUser. Lorsque la protection antialtération est activée, ils peuvent effectuer toutes les tâches qu'ils sont habituellement autorisés à effectuer sans avoir à saisir de mot de passe pour la protection antialtération.

Remarque
Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - protection antialtération** pour modifier une stratégie de protection antialtération.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Événements de protection antialtération

En cas d'événement de protection antialtération, (lorsque, par exemple, une tentative non autorisée de désinstaller Sophos Anti-Virus depuis un terminal a été bloquée), l'événement est consigné dans le journal des événements et peut être consulté depuis l'Enterprise Console. Retrouvez plus de renseignements à la section Affichage des événements de protection antialtération (page 204).

Il y a deux types d'événements de protection antialtération :

- Les événements réussis d'authentification de la protection antialtération affichant le nom de l'utilisateur authentifié et l'heure d'authentification.
- Les tentatives ratées de modifications affichant le nom du produit ou du composant Sophos pris pour cible, l'heure de la tentative et des informations détaillées sur l'utilisateur responsable de cette tentative.

7.6.1 Activation ou désactivation de la protection antialtération

Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - protection antialtération** pour modifier une stratégie de protection antialtération.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Pour démarrer ou arrêter la protection antialtération :

1. Vérifiez quelle stratégie de protection antialtération est utilisée par le ou les groupes d'ordinateurs que vous souhaitez configurer.

   Retrouvez plus de renseignements à la section Vérification des stratégies utilisées par un groupe (page 27).
2. Dans le volet **Stratégies**, cliquez deux fois sur **Protection antialtération**. Puis cliquez deux fois sur la stratégie que vous désirez changer.
3. Dans la boîte de dialogue **Stratégie de protection antialtération**, sélectionnez ou dessélectionnez la case **Activer la protection antialtération**.

   Si vous souhaitez activer la protection antialtération pour la première fois, cliquez sur **Définir** sous le champ **Mot de passe**. Dans la boîte de dialogue **Mot de passe de la protection antialtération**, saisissez et confirmez un mot de passe.

   Conseil
   Nous vous conseillons d'utiliser un mot de passe contenant au minimum 8 caractères incluant une combinaison de minuscules, de majuscules et de chiffres.

7.6.2 Changement du mot de passe de la protection antialtération

Pour changer le mot de passe de la protection antialtération :

1. Vérifiez quelle stratégie de protection antialtération est utilisée par le ou les groupes d'ordinateurs que vous souhaitez configurer.

Retrouvez plus de renseignements à la section Vérification des stratégies utilisées par un groupe (page 27).

2. Dans le volet **Stratégies**, cliquez deux fois sur **Protection antialtération**. Puis cliquez deux fois sur la stratégie que vous désirez changer.
3. Dans la boîte de dialogue **Stratégie de protection antialtération**, cliquez sur **Changer** sous le champ **Mot de passe**. Dans la boîte de dialogue **Mot de passe de la protection antialtération**, saisissez et confirmez le nouveau mot de passe.

Conseil
Le mot de passe doit contenir au minimum 8 caractères incluant une combinaison de minuscules, de majuscules et de chiffres.

7.6.3 À propos de la protection antialtération renforcée

La protection antialtération renforcée est basée sur la fonctionnalité de protection antialtération. Si la protection antialtération renforcée est activée, les actions suivantes sont bloquées pour Sophos Anti-Virus, Sophos AutoUpdate, Sophos Management Communication System, Sophos Remote Management System et Sophos Endpoint Defense :

- Arrêt des services à partir de l'interface d'utilisation Services
- Arrêt des services à partir de l'interface d'utilisation Gestionnaire des tâches
- Modification de la configuration d'un service à partir de l'interface d'utilisation Services
- Arrêt des services et modification de la configuration des services à partir de la ligne de commande
- Désinstallation
- Réinstallation
- Arrêt des processus à partir de l'interface d'utilisation Gestionnaire des tâches
- Suppression ou modification des fichiers ou des dossiers protégés
- Suppression ou modification des clés de registre protégées

Important
Pour activer la protection antialtération renforcée, la protection antialtération doit être activée. Si la protection antialtération est désactivée, la protection antialtération renforcée sera automatiquement désactivée.

7.6.4 Paramètres de la protection antialtération améliorée

1. Dans le volet **Stratégies**, cliquez deux fois sur **Protection antialtération**. Puis cliquez deux fois sur la stratégie que vous désirez changer.
2. Dans la boîte de dialogue **Stratégie de protection antialtération**, sélectionnez la case **Activer la protection antialtération** puis sélectionnez la case **Activer la protection antialtération renforcée**.
3. S'il s'agit d'une nouvelle installation ou d'une mise à niveau, dans la boîte de dialogue **Stratégie de protection antialtération**, cliquez sur **Définir** dans le champ **Mot de passe**.

Si la protection antialtération est déjà activée, cliquez sur **Changer** dans le champ **Mot de passe**. Dans la boîte de dialogue **Mot de passe de la protection antialtération**, saisissez et confirmez un mot de passe.

Remarque
Le même mot de passe est utilisé pour la protection antialtération et la protection antialtération renforcée. Lorsque la protection antialtération renforcée est activée, elle remplace la protection antialtération. C'est pourquoi le mot de passe doit être changé lorsque le mot de passe de la protection antialtération a déjà été défini.

Nous vous conseillons d'utiliser un mot de passe différent pour chaque stratégie.

7.7 Stratégie de correctif

Remarque
Cette fonction n'est pas incluse dans toutes les licences. Si vous voulez l'utiliser, il se peut que vous deviez changer votre contrat de licence. Retrouvez plus de renseignements à la section http://www.sophos.com/fr-fr/products/complete/comparison.aspx.

L'Enterprise Console vous permet de vérifier que les correctifs de sécurité les plus récents sont installés sur vos ordinateurs.

Les SophosLabs mettent à votre disposition des niveaux qui vous aident à déterminer quels sont les problèmes de correctifs de sécurité les plus sérieux afin que vous puissiez les résoudre rapidement. Les niveaux des SophosLabs prennent en compte les vulnérabilités les plus récentes et peuvent donc être différents du niveau de sévérité indiqué par un autre éditeur.

Avant d'utiliser un correctif, installez l'agent de correctif sur vos ordinateurs en réseau afin qu'ils puissent procéder à l'évaluation des correctifs et communiquer leur état à l'Enterprise Console. Vous pouvez l'installer à l'aide de l'**Assistant de protection des ordinateurs**. Retrouvez plus de renseignements à la section Protection automatique des ordinateurs (page 46).

Cette section suppose que vous avez installé l'agent de correctif.

Remarque
Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - correctif** pour configurer une stratégie de correctif.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements sur l'administration déléguée à la section Gestion des rôles et des sous-parcs (page 14).

7.7.1 Comment fonctionne l'évaluation des correctifs ?

L'évaluation des correctifs est désactivée dans la stratégie par défaut. Dès que l'évaluation des correctifs est activée, celle-ci commence sur les ordinateurs. L'opération peut prendre quelques minutes. Les évaluations suivantes ont lieu aux intervalles définis dans la stratégie (par défaut, elles ont lieu tous les jours).

Remarque
Si les ordinateurs commencent une évaluation avant que l'Enterprise Console ait téléchargé les données des correctifs depuis Sophos pour la première fois, l'observateur des événements des correctifs n'affichera aucun résultat. Le téléchargement peut durer quelques heures. Pour vérifier s'il est terminé, consultez le champ **Mises à jour des correctifs** dans la boîte de dialogue **Événements > Événements d'évaluation des correctifs**.

Si, pour quelque raison que ce soit, l'agent de correctif ne peut pas se mettre à jour depuis l'Enterprise Console, il continuera à évaluer les ordinateurs par rapport aux détections des correctifs précédemment téléchargées.

Les ordinateurs sont uniquement évalués pour s'assurer que les correctifs de sécurité sont bien installés sur l'ordinateur. Si un nouveau correctif est publié pour remplacer un correctif plus ancien, l'évaluation des correctifs ne vérifiera plus la présence de l'ancien correctif. Seul le nouveau correctif sera évalué.

Définition des correctifs remplacés

Si un éditeur publie un correctif qui remplace un ancien correctif, le nouveau correctif est appelé le correctif remplaçant. Le correctif qu'il remplace est appelé le correctif remplacé.

Sophos vous conseille d'installer le correctif remplaçant afin de maintenir vos ordinateurs à jour.

Exemple : si vous recherchez le virusX et réalisez que la protection contre ce virus est disponible dans le correctif P01, qui a été remplacé par le correctif P02, Sophos vous conseille d'installer P02.

7.7.2 À propos des événements d'évaluation des correctifs

Lorsqu'un événement d'évaluation des correctifs se produit, par exemple, si un correctif est manquant sur un ordinateur, l'événement est envoyé à l'Enterprise Console et est visible dans la boîte de dialogue **Évaluation des correctifs - Observateur d'événements**.

Dans la boîte de dialogue **Évaluation des correctifs - Observateur d'événements**, vous pouvez utiliser des filtres pour n'afficher que les événements qui vous intéressent. Vous pouvez aussi exporter la liste des événements d'évaluation des correctifs dans un fichier. Retrouvez plus de renseignements aux sections Événements d'évaluation des correctifs (page 204) et Exportation dans un fichier de la liste des événements (page 210).

7.7.3 Activation ou désactivation de l'évaluation des correctifs

Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - correctif** pour configurer une stratégie de correctif.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Pour activer ou désactiver l'évaluation des correctifs :

1. Vérifiez quelle stratégie de correctif est utilisée par le(s) groupe(s) d'ordinateurs que vous désirez configurer.

   Retrouvez plus de renseignements à la section Vérification des stratégies utilisées par un groupe (page 27).

2. Dans le volet **Stratégies**, cliquez deux fois sur **Correctif**. Puis cliquez deux fois sur la stratégie que vous désirez changer.
3. Dans la boîte de dialogue **Stratégie de correctif**, dessélectionnez la case **Activer les évaluations des correctifs** et cliquez sur **OK**.

7.7.4 Sélection de l'intervalle d'évaluation des correctifs

Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - correctif** pour configurer une stratégie de correctif.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Pour paramétrer l'intervalle d'évaluation des correctifs

1. Vérifiez quelle stratégie de correctif est utilisée par le ou les groupes d'ordinateurs que vous désirez configurer.

   Retrouvez plus de renseignements à la section Vérification des stratégies utilisées par un groupe (page 27).
2. Dans le volet **Stratégies**, cliquez deux fois sur **Correctif**. Puis cliquez deux fois sur la stratégie que vous désirez changer.
3. Dans la boîte de dialogue **Stratégie de correctif**, cliquez sur la flèche du menu déroulant du champ **Évaluer les correctifs manquants** et sélectionnez l'intervalle de votre choix. Cliquez sur **OK**.

   Pour que l'évaluation ait lieu à cet intervalle, l'évaluation des correctifs doit être activée dans la stratégie.

7.8 Stratégie de contrôle du Web

Remarque
Cette fonction n'est pas incluse dans toutes les licences. Si vous voulez l'utiliser, il se peut que vous deviez changer votre contrat de licence. Retrouvez plus de renseignements à la section http://www.sophos.com/fr-fr/products/complete/comparison.aspx.

Par défaut, la stratégie de contrôle du Web est désactivée dans Enterprise Console. La sélection de l'option **Activer le contrôle du Web** vous permet de choisir l'une des options de stratégie suivantes :

- **Contrôle des sites Web inappropriés** : cette option de base du contrôle du Web inclut 14 catégories de sites essentielles. Elle a été conçue pour empêcher l'accès des utilisateurs à certains sites Web à propos desquels votre entreprise pourrait être tenue légalement responsable. Retrouvez plus de renseignements à la section Contrôle des sites Web inappropriés (page 179).
- **Contrôle du Web intégral** : cette option applique une stratégie entièrement fonctionnelle englobant plus de 50 catégories de sites Internet. Elle nécessite l'utilisation d'une Sophos Web Appliance, d'une Sophos Management Appliance ou d'une Sophos UTM appliance (à partir de la version 9.2) pour pouvoir effectuer la synchronisation avec les terminaux, de distribuer les mises à jour des stratégies et de collecter les données d'activité sur Internet. Retrouvez plus de renseignements à la section Contrôle intégral du Web (page 184).

Lors de l'utilisation de l'option Contrôle des sites Web inappropriés, vous pouvez soit modifier une stratégie de contrôle du Web existante, soit créer une nouvelle stratégie. Retrouvez plus

de renseignements à la section Création d'une stratégie (page 31). Vous pouvez paramétrer les diverses catégories de sites sur « Bloquer, »« Avertir » ou « Autoriser. » L'état du contrôle du Web et les événements Web apparaissent dans Enterprise Console. Retrouvez plus de renseignements sur les événements Web à la section Affichage des événements Web (page 208).

Si, à la place, vous utilisez la stratégie Contrôle intégral du Web, Enterprise Console requiert l'emplacement de l'appliance Web, UTM ou de l'appliance d'administration (Management Appliance) à partir de laquelle toute la stratégie de filtrage Web est configurée, avec une clé partagée pour sécuriser la communication entre l'appliance et Enterprise Console. Lorsque la stratégie de contrôle intégral du Web est sélectionnée, la plupart des opérations de rapport et de surveillance sont transférées dans l'appliance. Par contre, les sites Web contrôlés et évalués par le filtrage instantané des URL (Protection Web (page 104)) de Sophos Endpoint Security and Control apparaissent dans Enterprise Console sous la forme d'événements Web.

Retrouvez plus de renseignements sur le contrôle du Web dans le *Guide général de contrôle du Web des terminaux*.

Remarque
Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - Contrôle du Web** pour modifier une stratégie de contrôle du Web.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements sur l'administration déléguée à la section Gestion des rôles et des sous-parcs (page 14).

7.8.1 Contrôle des sites Web inappropriés

Remarque
Cette fonction n'est pas incluse dans toutes les licences. Si vous voulez l'utiliser, il se peut que vous deviez personnaliser votre licence. Retrouvez plus de renseignements à la section http://www.sophos.com/fr-fr/products/complete/comparison.aspx.

Avec cette forme basique de contrôle des sites Web, vous pouvez filtrer l'activité Web des utilisateurs en vous basant sur 14 catégories de sites Web. Il existe une action par défaut pour chaque catégorie (décrite dans la section À propos des catégories de sites Web (page 180)), mais, si nécessaire, vous pouvez sélectionner une action différente, comme indiqué à la section Sélection d'une action de catégorie de site Web (page 183).

La visite de sites Web restreints peut être bloquée pour les utilisateurs. Un événement qui est déclenché est montré à l'utilisateur et envoyé à Enterprise Console.

Autrement, les utilisateurs peuvent être avertis via une notification lorsqu'ils se rendent sur les sites Web contrôlés. Un événement d'avertissement est déclenché même s'ils ne poursuivent pas la visite du site Web. Si l'utilisateur poursuit et consulte un site malgré l'avertissement, un second événement est déclenché et envoyé à Enterprise Console.

Remarque
Bien que les sites HTTP et HTTPS soient tous les deux filtrés dans tous les navigateurs Web pris en charge, les notifications à l'utilisateur sont différentes si l'URL est HTTP ou HTTPS. Avec les sites HTTP, les utilisateurs voient des pages de notification pour des sites dont les catégories sont définies sur « Bloquer » ou « Avertir ». Pour HTTPS, les utilisateurs voient seulement des notifications « Bloquer » apparaître sous la forme d'une infobulle dans la barre d'état système Windows. Les actions « Avertir » de HTTPS n'apparaissent pas pour l'utilisateur et ne sont pas journalisées. À la place, les utilisateurs sont autorisés à continuer vers la page requise et l'événement est consigné dans le journal sous la forme d'une action « Continuer » dans Enterprise Console.

Si vous sélectionnez l'action « Autoriser » pour une catégorie de site Web, les utilisateurs peuvent accéder à tous les sites Web de cette catégorie, sauf si des exceptions de sites Web sont spécifiées. Les événements « Autoriser » ne sont pas journalisés lorsque l'option **Contrôle des sites Web inappropriés** est sélectionnée.

Remarque
Les sites autorisés sont tout de même contrôlés et évalués par la fonction de filtrage instantané des URL (protection Web) de Sophos Endpoint Security and Control.

Activation du contrôle des sites Web inappropriés

Effectuez les étapes suivantes pour activer le contrôle du Web dans Enterprise Console et utilisez le contrôle des sites Web inappropriés.

Remarque
Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - Contrôle du Web** pour modifier une stratégie de contrôle du Web.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements sur l'administration déléguée à la section Gestion des rôles et des sous-parcs (page 14).

Pour activer le contrôle des sites Web inappropriés :

1. Vérifiez quelle stratégie de contrôle du Web est utilisée par le ou les groupes d'ordinateurs que vous souhaitez configurer. Retrouvez plus de renseignements à la section Vérification des stratégies utilisées par un groupe (page 27).
2. Dans le volet **Stratégies**, cliquez deux fois sur **Contrôle du Web**. Puis cliquez deux fois sur la stratégie que vous désirez changer.
   La boîte de dialogue **Stratégie de contrôle du Web** apparaît.
3. Sur l'onglet **Général**, sélectionnez **Activer le contrôle du Web**.
   La stratégie **Contrôle des sites Web inappropriés** apparaît. Bien qu'il y ait une action par défaut pour chacune des 14 catégories de sites, vous pouvez définir une action différente. Retrouvez plus de renseignements à la section Sélection d'une action de catégorie de site Web (page 183).

À propos des catégories de sites Web

En sélectionnant **Contrôle des sites Web inappropriés**, vous pouvez configurer 14 catégories de sites Web, contrôlant ainsi le contenu Internet auquel les utilisateurs peuvent accéder via un

navigateur web. Retrouvez plus de renseignements à la section Contrôle des sites Web inappropriés (page 179).

Les catégories de sites Web décrites ci-dessous sont filtrées. L'action par défaut de chaque catégorie est indiquée entre parenthèses. Chaque catégorie peut être configurée ainsi : **Bloquer**, **Avertir** ou **Autoriser**. La sélection de **Autoriser** permet à l'utilisateur d'accéder à tous les sites de cette catégorie. Retrouvez plus de renseignements sur la modification de l'action à la section Sélection d'une action de catégorie de site Web (page 183).

- **Adulte sexuellement explicite (Bloquer)** : cette catégorie inclut les sites de produits pour adultes, notamment les sex toys, CD-ROM et vidéos ; pornographie juvénile et pédophilie (y compris la liste de l'Internet Watch Foundation) ; services pour adultes comprenant vidéo-conférences, services d'escorte et clubs de strip-tease ; histoires érotiques et descriptions textuelles d'actes sexuels ; dessins animés et films d'animation à caractère explicite ; groupes en ligne, y compris groupes de discussion et forums sexuellement explicites par nature ; sites orientés sexuellement ou érotiques avec nudité partielle ou intégrale ; représentations ou images d'actes sexuels, y compris avec des animaux ou des objets inanimés utilisés d'une manière sexuelle ; textes ou graphiques sur l'exploitation sexuelle ou sexuellement violent ; asservissement, fétichisme, piercings génitaux ; sites naturistes contenant de la nudité ; et photographique érotique ou fétichiste contenant de la nudité.

  Remarque
  Nous n'incluons pas les sites concernant la santé sexuelle, le cancer du sein ou les maladies sexuellement transmissibles (sauf ceux comportant des exemples graphiques).

- **Alcool et tabac (Avertir)** : cette catégorie inclut les sites qui font gratuitement ou non la promotion de l'alcool du tabac ou qui distribuent des produits relatifs.
- **Proxies anonymiseurs (Bloquer)** : cette catégorie inclut les sites pour proxies à distance ou surf anonyme, les mémoires cache de moteurs de recherche qui passent au travers du filtrage ainsi que les sites de traduction de type web qui ignorent également le filtrage.
- **Activité criminelle (Bloquer)** : cette catégorie inclut les sites préconisant, enseignant la réalisation d'actes illégaux ou donnant des conseils sur ce type d'actes ; astuces pour esquiver l'application de la loi ; et techniques de crochetage et de cambriolage.
- **Jeu (Avertir)** : cette catégorie inclut les sites de jeu en ligne ou de loterie invitant à utiliser de l'argent réel ou virtuel ; informations ou conseils pour placer des paris, participer à des loteries ou jouer ; casinos virtuels et sociétés de jeu offshore ; paris sportifs ; sports virtuels et « fantasy leagues » offrant des récompenses significatives ou demandant des paris importants.
- **Piratage (Bloquer)** : cette catégorie inclut des sites pour la promotion, l'instruction ou des conseils concernant l'utilisation douteuse ou illégale d'équipements et de logiciels afin de pirater des mots de passe, créer des virus, accéder à d'autres ordinateurs et systèmes informatiques de communication ; des sites contenant des instructions ou des solutions de filtrage des logiciels ; logiciels et sites d'informations piratés ; sites pirates ; sites de téléchargements de logiciels et de fichiers multimédia piratés ; et sites de crimes informatiques.
- **Drogues illégales (Bloquer)** : cette catégorie inclut les sites de recettes, d'instructions ou de kits pour la fabrication ou la plantation de substances illicites autres que celles pour une utilisation industrielle ; rendre attractif, encourager ou instruire l'utilisation d'alcool, de tabac, de drogues illégales ou de toute autre substance illégale pour les mineurs (ou d'en masquer l'utilisation) ; informations sur les drogues légales, y compris inhalation de colle, mauvais emploi de drogues prescrites ou abus d'autres substances légales ; distribution de drogues illégales gratuitement ou non ; affichage, vente ou détails sur l'utilisation de l'attirail de drogue.
- **Haine et intolérance (Bloquer)** : cette catégorie inclut les sites qui préconisent ou incitent à la dégradation ou l'attaque de populations ou d'institutions spécifiques basés sur la religion, la race, la nationalité, le genre, l'âge, le handicap ou l'orientation sexuelle ; sites qui font la promotion d'un

agenda politique ou social prônant la suprématie par nature et l'exclusion en fonction de la race, de la religion, de la nationalité, du genre, du handicap ou de l'orientation sexuelle ; sites révisionnistes de l'holocauste ou sites négationnistes encourageant la haine ; coercition ou recrutement pour devenir membre d'une bande organisée[1] ou d'un culte [2] ; sites militants ou extrémistes ; matériaux manifestement insensibles ou offensants, y compris ceux avec un manque de reconnaissance ou de respect pour les opinions et les croyances adverses.

Remarque
Nous n'incluons pas les informations, les incidents historiques ou de presse pouvant inclure les critères ci-dessus (sauf dans les exemples graphiques).

[1]Une bande organisée se définit comme un groupe dont les activités principales consistent à commettre des actes criminels. Ils ont un nom, un signe ou un symbole d'identification en commun et les membres prennent part, individuellement ou collectivement, à des activités criminelles au nom du groupe.

[2]Un culte est défini comme un groupe dont les disciples ont été trompés et manipulés afin d'être recrutés et retenus par un excès d'influence dans le but de modifier leurs personnalités et leurs comportements ; un groupe dans lequel le commandement est tout-puissant, l'idéologie totalitaire et où la volonté de l'individu est subordonnée à celle du groupe ; et un groupe qui se démarque de la société.

- **Phishing et fraude (Bloquer)** : cette catégorie inclut les sites impliqués dans les escroquerie par phishing et téléphone, les sites de conseils sur le vol de services et les sites de plagiat et de tricherie, notamment la vente de documents de recherche.
- **URL de spam (Bloquer)** : cette catégorie inclut les URL rencontrées dans le spam, en particulier concernant les sujets suivants : informatique, finance et actions boursières, divertissement, jeux, santé et médecine, humour et gadgets, rencontres, produits et services, shopping et voyages.
- **Spywares (Bloquer)** : cette catégorie inclut des sites qui fournissent ou font la promotion du rassemblement ou du suivi d'informations inconnues de l'utilisateur final ou de l'entreprise, ou réalisés sans le consentement explicite de ceux-là. Cela comprend des sites qui véhiculent des exécutables malveillants ou des virus, de la surveillance par des tiers ainsi que d'autres logiciels commerciaux non sollicités, spywares et autres malwares « phone home ».
- **Mauvais goût et offensant (Avertir)** : cette catégorie inclut des sites qui contiennent du langage violent et offensant, notamment via des blagues, des bandes dessinées ou de la satire, ainsi qu'une utilisation excessive de gestes profanateurs et obscènes.
- **Violence (Avertir)** : cette catégorie inclut des sites représentant, décrivant ou préconisant les assauts physiques contre des êtres humains, des animaux ou des institutions ; représentation de la torture, de la mutilation, du sang ou d'une mort horrible ; préconisant, encourageant ou représentant la mise en danger d'un individu, ou le suicide, y compris via les troubles alimentaires ou les addictions ; instructions, recettes ou kits pour la confection de bombes ou de toute autre engin nuisible ou destructeur ; sites faisant la promotion du terrorisme ; et les sports et jeux violents, y compris les vidéos et les jeux en ligne.

  Remarque
  Nous ne bloquons pas les informations, les incidents historiques ou de presse pouvant inclure les critères ci-dessus, sauf ceux qui comportent des exemples graphiques.

- **Armes (Avertir)** : cette catégorie inclut des sites avec informations d'achat et de commande en ligne, contenant les tarifs et les emplacements des marchands d'armes ; toute page ou site avec principalement du contenu relatif à la vente d'armes, de munitions ou de substances toxiques ou contenant des liens vers ce type de contenu ; la présentation ou le détail sur l'utilisation d'armes,

de munitions ou de substances toxiques ; et les clubs qui proposent des entraînements sur les mitrailleuses, les automatiques, les autres armes d'assaut et l'entraînement des tireurs.

Remarque
Les armes sont définies comme des objets (tels un couteau ou un pistolet) utilisés pour blesser, battre ou détruire.

Sélection d'une action de catégorie de site Web

Avec le contrôle du Web activé et la stratégie **Contrôle des sites Web inappropriés** sélectionnée, vous pouvez configurer l'action pour chaque catégorie de site Web. Vous pouvez aussi créer une nouvelle stratégie basée sur la stratégie par défaut. Retrouvez plus de renseignements à la section Création d'une stratégie (page 31).

Pour sélectionner une action de catégorie de site :

1. Dans l'onglet **Général**, dans la liste déroulante près de la ou des catégories de site que vous voulez configurer, sélectionnez l'un des éléments suivants :
   - **Bloquer** : empêche les utilisateurs de consulter les sites de cette catégorie. S'il s'agit d'une page Web HTTP, une notification de blocage apparaît pour l'utilisateur, expliquant pourquoi le site a été bloqué. S'il s'agit d'une page HTTPS, une infobulle apparaît pour l'utilisateur dans la barre d'état système Windows.
   - **Avertir** : avertit l'utilisateur s'il court le risque de violer la stratégie d'utilisation de Web de son entreprise tout en lui permettant de poursuivre. S'il s'agit d'une page HTTP, une notification d'avertissement apparaît pour l'utilisateur, le mettant en garde à propos de la poursuite de sa visite sur le site Web. S'il s'agit d'une page HTTPS, l'utilisateur ne reçoit pas de notification et est autorisé à continuer à naviguer sur le site Web. L'événement est journalisé comme une action « Continuer » dans Enterprise Console.
   - **Autoriser** : laisse l'utilisateur consulter les sites de cette catégorie. L'événement n'est pas journalisé.
2. Cliquez sur **OK**.

Gestion des exceptions de site Web

Si vous avez sélectionné la stratégie **Contrôle des sites Web inappropriés**, vous pouvez créer des exceptions aux actions « Bloquer » et « Avertir ». Vous pouvez exempter des sites Web du filtrage en ajoutant à la liste « Sites Web à autoriser » ou « Sites Web à bloquer ». Les entrées peuvent être des adresses IP et des noms de domaine. Vous pouvez aussi modifier des entrées existantes de sites Web et supprimer des sites Web d'une liste.

Remarque
En cas de conflits entre les entrées ou si elles apparaissent à la fois dans les listes « Bloquer » et « Autoriser », ce sont les entrées de la liste Bloquer qui sont prises en compte. Par exemple, si la même adresse IP apparaît dans la liste Bloquer et dans la liste Autoriser, le site Web est bloqué. De plus, si un domaine est inclus à la liste Bloquer et qu'un sous-domaine de ce domaine est inclus à la liste Autoriser, l'entrée Autoriser est ignorée et le domaine et tous ses sous-domaines sont bloqués.

Pour ajouter une exception de site Web :

1. Sur l'onglet **Exceptions de site Web**, cliquez sur le bouton **Ajouter** près de la zone de texte **Sites Web à autoriser** ou **Sites Web à bloquer**.

2. Dans la boîte de dialogue **Ajouter le site Web à autoriser**, cliquez sur **Nom de domaine**, **Adresse IP avec sous-masque de réseau** ou **Adresse IP**. Des exemples apparaissent pour chaque format au-dessus de la zone de texte associée.
3. Dans la zone de texte, entrez le nom de domaine ou l'adresse IP du site Web que vous voulez autoriser ou bloquer.
4. Cliquez sur **OK**.

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

7.8.2 Contrôle intégral du Web

Remarque
Cette fonction n'est pas incluse dans toutes les licences. Si vous voulez l'utiliser, il se peut que vous deviez personnaliser votre contrat de licence. Retrouvez plus de renseignements à la section http://www.sophos.com/fr-fr/products/complete/comparison.aspx.

Si vous utilisez Sophos Web Appliance, Sophos Management Appliance ou une appliance Sophos UTM (à partir de la version 9.2), vous pouvez distribuer une stratégie d'appliance à vos utilisateurs avec Enterprise Console.

Les terminaux communiquent avec Enterprise Console de la même façon que lorsque la stratégie Contrôle des sites Web inappropriés est sélectionnée. En revanche, les règles de filtrage Web et les journaux d'activité Web sont synchronisés avec l'appliance que vous indiquez. La stratégie est stockée sur les terminaux et appliquée en fonction des données Sophos les plus récentes.

Les utilisateurs sont bloqués, avertis ou autorisés en fonction de la stratégie de contrôle du Web. Pour voir les données sur l'activité des utilisateurs, vous pouvez utiliser les fonctions **Rapports** et **Recherche** de Appliance Web ou de Management Appliance ou l'option **Journaux et rapports > Web Protection** de l'applicance UTM. Les événements de contrôle du Web sont tous enregistrés sur l'appliance. Toutefois, les sites contrôlés et évalués par le filtrage instantané des URL (Protection Web) de Sophos Endpoint Security and Control sont enregistrés en tant qu'événements Web dans Enterprise Console.

Remarque
Bien que les sites HTTP et HTTPS soient tous les deux filtrés dans tous les navigateurs Web pris en charge, les notifications à l'utilisateur de Web Appliance ou de Management Appliance sont différentes selon que l'URL soit HTTP ou HTTPS. Avec les sites HTTP, les utilisateurs voient des pages de notification pour des sites dont les catégories sont définies sur « Bloquer » ou « Avertir ». Pour HTTPS, les utilisateurs voient seulement des notifications « Bloquer » apparaître sous la forme d'une infobulle dans la barre d'état système Windows. Les actions « Avertir » de HTTPS n'apparaissent pas pour l'utilisateur et ne sont pas journalisées. À la place, les utilisateurs sont autorisés à continuer vers la page requise et l'événement est journalisé sous la forme d'une action « Continuer » dans la Appliance Web ou la Management Appliance.

L'appliance UTM utilise un service Cloud central appelé Sophos LiveConnect pour assurer la protection et la surveillance des terminaux. LiveConnect vous permet de gérer tous les terminaux utilisés sur votre réseau local, sur des sites distants ou par vos employés en déplacement. Les mises à jour des stratégies sont distribuées aux utilisateurs et les données de rapport émises par les terminaux sont téléchargés même lorsque les utilisateurs ne sont pas connectés à partir d'un réseau.

Lors de l'utilisation de la Management Appliance ou de la Appliance Web, les terminaux communiquent avec l'appliance soit directement soit par le biais de Sophos LiveConnect.

Lorsque **Contrôle intégral du Web** est sélectionné, une stratégie dotée d'un maximum de fonctions prend effet. Par rapport au contrôle du Web de base, le contrôle intégral du Web offre les avantages suivants selon l'appliance que vous utilisez :

- En fonction de plus de 50 catégories d'URL, les utilisateurs sont avertis ou bloqués.
- Des stratégies « Heures spéciales » peuvent être appliquées.
- De nombreuses stratégies supplémentaires peuvent être utilisées comme exceptions par utilisateur ou par groupe sur les stratégies par défaut et d'Heures spéciales.
- Les journaux et rapports détaillées sont disponibles sur Appliance Web, Management Appliance ou l'appliance UTM.
- LiveConnect permet la distribution de mises à jour de stratégies et le téléchargement en amont des données des rapports, même quand les utilisateurs se connectent à distance.
- Les utilisateurs peuvent envoyer des commentaires concernant la gestion des URL bloquées.
- Des pages de notification personnalisées incluant votre logo et un message exclusif à votre entreprise peuvent être affichées aux utilisateurs. Retrouvez plus de renseignements dans la documentation de Sophos Web Appliance.
- Lorsque SafeSearch est activé, la navigation sur des sites inappropriés est automatiquement limitée à partir de moteurs de recherche fréquemment utilisés.

Retrouvez plus de renseignements sur la configuration d'une stratégie Appliance Web complète dans la documentation Sophos Web Appliance disponible en anglais sur http://wsa.sophos.com/docs/wsa/.

Retrouvez toute la documentation de l'appliance UTM sur http://www.sophos.com/fr-fr/support/documentation/sophos-utm.aspx.

Activation du contrôle intégral du Web

Remarque
La procédure suivante suppose que vous avez configuré une Sophos Web Appliance, une Sophos Management Appliance ou une appliance Sophos UTM (à partir de la version 9.2) pour qu'elle fonctionne parfaitement et utilisant le contrôle du Web sur les terminaux.

Par défaut, la stratégie de contrôle du Web est désactivée. Exécutez les étapes suivantes pour activer le contrôle du Web et utiliser la stratégie de contrôle intégral du Web.

Remarque
Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - Contrôle du Web** pour modifier une stratégie de contrôle du Web.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements sur l'administration déléguée à la section Gestion des rôles et des sous-parcs (page 14).

Pour activer le contrôle intégral du Web

1. Vérifiez quelle stratégie de contrôle du Web est utilisée par le ou les groupes d'ordinateurs que vous souhaitez configurer. Retrouvez plus de renseignements à la section Vérification des stratégies utilisées par un groupe (page 27).

2. Dans le volet **Stratégies**, cliquez deux fois sur **Contrôle du Web**. Puis cliquez deux fois sur la stratégie que vous désirez changer.
   La boîte de dialogue **Stratégie de contrôle du Web** apparaît.
3. Sur l'onglet **Général**, cliquez sur **Activer le contrôle du Web**.
4. Sélectionnez **Contrôle intégral du Web**.
5. Dans le volet **Paramètres**, saisissez le **Nom d'hôte de l'appliance** et la **Clé de sécurité pour l'échange de stratégies**.
   - Pour une Appliance Web ou une Management Appliance, vous devez fournir un nom d'hôte pleinement qualifié. La clé de sécurité doit correspondre à celle affichée sur la page **Endpoint Web Control** de l'appliance.
   - Pour UTM, saisissez le nom d'hôte et la Clé partagée du service Broker de Sophos LiveConnect utilisé par UTM. Vous pouvez les retrouver dans l'interface administrative WebAdmin d'UTM dans l'onglet **Endpoint Protection** > **Gestion de l'ordinateur** > **Avancé** à la section **Sophos LiveConnect - Enregistrement** sous **Informations SEC**.

   Retrouvez plus de renseignements dans la documentation de Sophos Web Appliance disponible sur http://wsa.sophos.com/docs/wsa/ ou dans la documentation de l'appliance UTM disponible sur http://www.sophos.com/fr-fr/support/documentation/sophos-utm.aspx.
6. Vous pouvez également choisir de sélectionner **Bloquer la navigation s'il est impossible de déterminer la catégorie du site Web**. Si un terminal ne parvient pas à récupérer les données sur la catégorisation des sites Web, les URL qui ne peuvent pas rentrer dans des catégories sont bloquées jusqu'à la restauration du service.

   Cette case à cocher n'est pas sélectionnée par défaut, ce qui permet aux utilisateurs de continuer de naviguer si le service de catégorisation échoue.
7. Cliquez sur **OK**.
   Enterprise Console reconfigure les terminaux des utilisateurs pour communiquer avec Appliance Web, Management Appliance ou avec le service Broker de Sophos LiveConnect utilisé par UTM.

7.9 Stratégie de prévention des Exploits

Remarque
Cette fonction n'est pas incluse dans toutes les licences. Pour pouvoir l'utiliser, il se peut que vous deviez changer votre contrat de licence. Retrouvez plus de renseignements à la section http://www.sophos.com/fr-fr/products/complete/comparison.aspx.

La prévention des Exploits vous permet de :

- Protéger les fichiers document contre les ransomwares (CryptoGuard).
- Protéger contre les attaques sur le secteur de démarrage (WipeGuard).

Important
Cette fonctionnalité n'est pas actuellement disponible sur les serveurs.

- Protéger les fonctions critiques des navigateurs Web (Safe Browsing).
- Limiter les Exploits. Cette option permet de protéger les applications les plus vulnérables aux attaques de malwares (par exemple, les applications Java).
- Protéger contre les attaques contre les processus creux.
- Protéger contre le chargement de fichiers .DLL à partir de dossiers non fiables.

- Protéger contre la surveillance d'exécution du processeur.

Par défaut, la prévention des Exploits et toutes les options de prévention des Exploits sont activées.

Important
Si vous procédez à la mise à niveau de votre licence pour y inclure la prévention des Exploits, celle-ci ne sera pas automatiquement installée sur les ordinateurs que vous administrez déjà. Vous devez protéger de nouveau les ordinateurs pour l'installer. Retrouvez plus de renseignements à la section Protection automatique des ordinateurs (page 46).

Vous pouvez exclure les applications de la prévention des Exploits. Veuillez noter qu'elles demeureront protégées par CryptoGuard et Safe Browsing si ces options sont sélectionnées dans le cadre d'une stratégie de prévention des Exploits.

Vous pouvez également exclure les événements d'Exploits de la prévention des Exploits.

Retrouvez plus de renseignements sur les paramètres conseillés pour la prévention des Exploits dans le *Guide de configuration des stratégies de Sophos Enterprise Console*.

Remarque
Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - Prévention des Exploits** pour pouvoir configurer une stratégie de prévention des Exploits.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

HitmanPro.Alert et mises à jour de la stratégie

HitmanPro.Alert détecte les applications qui ont besoin d'être protégées sur les terminaux. Il signale l'application détectée au serveur Sophos Enterprise Console. Le serveur récupère les applications à protéger et fusionne, toutes les 120 minutes, les nouvelles données d'application dans la stratégie. Le serveur distribue la stratégie mise à jour aux terminaux et fournit une liste des applications à protéger.

7.9.1 Activation ou désactivation de la prévention des Exploits

Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - Prévention des Exploits** pour pouvoir configurer une stratégie de prévention des Exploits.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Remarque
Par défaut, la prévention des Exploits est activée et toutes les options de prévention des Exploits sont activées.

Pour activer ou désactiver la prévention des Exploits :

1. Vérifiez quelle stratégie de prévention des Exploits est utilisée par le(s) groupe(s) d'ordinateurs que vous souhaitez configurer.

Retrouvez plus de renseignements à la section Vérification des stratégies utilisées par un groupe (page 27).

2. Dans le volet **Stratégies**, cliquez deux fois sur **Prévention des Exploits**. Puis cliquez deux fois sur la stratégie que vous désirez changer.
3. Dans l'onglet **Paramètres de protection** de la boîte de dialogue **Stratégie de prévention des Exploits**, sélectionnez ou dessélectionnez la case **Activer la prévention des Exploits**.
4. Sélectionnez ou dessélectionnez la case **Protéger les fichiers document contre les ransomwares (CryptoGuard)**.

   Vous pouvez également choisir de vous protéger contre les ransomwares exécutés à distance (uniquement possible sur les terminaux 64 bits).
5. Sélectionnez ou dessélectionnez la case **Protéger l'enregistrement de disque et de démarrage (WipeGuard)**.
6. Sélectionnez ou dessélectionnez la case **Protéger les fonctions critiques des navigateurs Web (Safe Browsing)**.
7. Sélectionnez ou dessélectionnez la case **Limiter les Exploits dans les applications vulnérables**.

   Vous pouvez choisir les types d'applications que vous souhaitez protéger contre les attaques, comme par exemple les applications Microsoft Office.
8. Sélectionnez ou dessélectionnez la case **Bloquer les attaques contre les processus creux**.
9. Sélectionnez ou dessélectionnez la case **Bloquer le chargement de DLL à partir de dossiers non fiables**.
10. Sélectionnez ou dessélectionnez la case **Activer la surveillance d'exécution du CPU**.
11. Cliquez sur **OK**.

Vous pouvez exclure les applications de la prévention des Exploits. Veuillez noter qu'elles demeureront protégées par CryptoGuard et Safe Browsing si ces options sont sélectionnées. Retrouvez plus de renseignements à la section Exclusion des applications de la prévention des Exploits (page 188).

Vous pouvez également exclure les événements d'Exploits de la prévention des Exploits. Retrouvez plus de renseignements à la section Exclusion des événements d'Exploits de la prévention des Exploits (page 189).

7.9.2 Exclusion des applications de la prévention des Exploits

Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - Prévention des Exploits** pour pouvoir configurer une stratégie de prévention des Exploits.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Important
Les applications vulnérables sont protégées par défaut. Veuillez procéder à l'exclusion d'applications de la prévention des Exploits avec le plus grand soin. Veuillez noter qu'elles demeureront protégées par CryptoGuard et Safe Browsing comme indiqué à la section Activation ou désactivation de la prévention des Exploits (page 187).

Vous pouvez exclure les applications de la prévention des Exploits. Vous pouvez également protéger les applications qui avaient déjà été exclues auparavant.

Pour exclure les applications :

1. Vérifiez quelle stratégie de prévention des Exploits est utilisée par le(s) groupe(s) d'ordinateurs que vous souhaitez configurer.

   Retrouvez plus de renseignements à la section Vérification des stratégies utilisées par un groupe (page 27).
2. Dans le volet **Stratégies**, cliquez deux fois sur **Prévention des Exploits**. Puis cliquez deux fois sur la stratégie que vous désirez changer.
3. Dans l'onglet **Exclusions d'application** de la boîte de dialogue **Stratégie de prévention des Exploits**, sélectionnez les applications que voulez exclure dans la liste **Applications protégées** et cliquez sur **Exclure**.
   Les applications sélectionnées vont être déplacées dans la liste **Applications exclues**
4. Vous pouvez protéger les événements d'Exploits actuellement exclus de la vérification depuis la liste **Applications exclues** en sélectionnant les événements et en cliquant sur **Inclure**.
5. Cliquez sur **OK**.

7.9.3 Exclusion des événements d'Exploits de la prévention des Exploits

Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - Prévention des Exploits** pour pouvoir configurer une stratégie de prévention des Exploits.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Important

- Lorsque vous excluez un événement d'Exploits, seul l'Exploit spécifique sera exclu et pas toute l'application.
- Si un événement d'Exploit fait partie d'une application qui a déjà été exclue, vous n'avez pas besoin d'exclure l'événement d'Exploit.

Vous pouvez exclure les événements d'Exploits de la prévention des Exploits. Vous pouvez également protéger les événements d'Exploits qui avaient déjà été exclus auparavant.

Pour exclure les événements d'Exploits :

1. Vérifiez quelle stratégie de prévention des Exploits est utilisée par le(s) groupe(s) d'ordinateurs que vous souhaitez configurer.

   Retrouvez plus de renseignements à la section Vérification des stratégies utilisées par un groupe (page 27).
2. Dans le volet **Stratégies**, cliquez deux fois sur **Prévention des Exploits**. Puis cliquez deux fois sur la stratégie que vous désirez changer.
3. Dans l'onglet **Exclusions d'Exploit** de la boîte de dialogue **Stratégie de prévention des Exploits**, sélectionnez les événements d'Exploits que voulez exclure dans la liste **Événements d'Exploits détectés** et cliquez sur **Exclure**.
   Les événements d'Exploits sélectionnés vont être déplacés dans la liste **Événements d'Exploits exclus**
4. Vous pouvez protéger les événements d'Exploits actuellement exclus de la vérification depuis la liste **Événements d'Exploits exclus** en sélectionnant les événements et en cliquant sur **Inclure**.
5. Cliquez sur **OK**.

8 Paramétrage des alertes et des messages

Plusieurs méthodes d'alerte sont utilisées dans Enterprise Console.

- **Alertes affichées dans la console**

  Si un élément demandant votre attention est trouvé sur un ordinateur ou si une erreur s'est produite, Sophos Endpoint Security and Control envoie une alerte à l'Enterprise Console. L'alerte apparaît dans la liste des ordinateurs. Retrouvez plus de renseignements sur la manière de traiter les alertes à la section Traitement des alertes sur les éléments détectés (page 52).

  Ces alertes sont toujours affichées. Il n'est pas nécessaire de les paramétrer.

- **Événements affichés dans la console**

  Lorsqu'un événement de contrôle d'applications, de pare-feu, d'évaluation des correctifs, de contrôle du Web, de contrôle des données, de contrôle des périphériques ou de protection antialtération se produit sur un terminal, par exemple, si une application a été bloquée par le pare-feu, l'événement est envoyé à l'Enterprise Console et peut être visualisé dans l'observateur d'événements respectif.

- **Alertes et messages envoyés par la console aux destinataires de votre choix**

  Par défaut, lorsqu'un élément est trouvé sur un ordinateur, un message apparaît sur le bureau de l'ordinateur et une entrée est ajoutée dans le journal des événements Windows. Lorsqu'un événement de contrôle des applications, de contrôle des données ou de contrôle des périphériques se produit, un message apparaît sur le bureau de l'ordinateur.

  Remarque
  Les messages de bureau optionnels définis par l'utilisateur ne s'affichent pas sur les ordinateurs à partir de Windows 8.

  Vous pouvez aussi configurer les alertes par email ou les messages SNMP pour les administrateurs.

  Remarque
  Si vous voulez utiliser le SMTP authentifié pour les alertes par email, consultez l'article 113780 de la base de connaissances Sophos.

Cette section décrit comment paramétrer les alertes à envoyer aux destinataires de votre choix.

8.1 Configuration des alertes d’abonnement logiciels

Si vous utilisez l’administration déléguée, vous devez disposer du droit **Configuration système** pour réaliser cette tâche. Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

L'Enterprise Console affiche les alertes soulevées par le gestionnaire de mise à jour dans la colonne **Alertes** de la vue **Gestionnaires de mise à jour**. Si vous vous êtes abonné à une version fixe des logiciels, une alerte apparaîtra lorsque cette version sera en instance de retrait ou retirée. Une alerte apparaîtra également si la licence de votre produit a changé.

Si vous êtes inscrit à une version fixe du logiciel et avez choisi de **Mettre automatiquement à niveau la version fixe du logiciel lorsqu'elle n'est plus prise en charge par Sophos**, votre abonnement sera mis à niveau automatiquement.

Si vous avez choisi de ne pas faire l'objet d'une mise à niveau automatiquement, vous serez invité à changer votre abonnement.

Important
L'exécution de logiciels non pris en charge vous laisse non protégé contre les nouvelles menaces de sécurité. Nous vous conseillons par conséquent de vous mettre le plus vite possible à niveau vers une version prise en charge.

Vous pouvez aussi paramétrer l'envoi des alertes par email à vos destinataires choisis lorsque la version du produit auquel vous vous êtes abonné est en instance de retrait ou retiré.

1. Dans le menu **Outils**, sélectionnez **Configurer les alertes par email**.
   La boîte de dialogue **Configuration des alertes par email** apparaît.
2. Si les paramètres SMTP n'ont pas été configurés ou si vous voulez afficher 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 email** 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 email.
6. Dans le volet **Abonnements**, sélectionnez les « Abonnements logiciels » que vous souhaitez envoyer à ce destinataire. Il y a trois alertes auxquelles vous pouvez vous abonner :
   - Un abonnement logiciels inclut la version d'un produit en instance de retrait à Sophos.
   - Un abonnement logiciels inclut la version d'un produit qui n'est plus disponible.
     Cette alerte est envoyée si le produit auquel vous vous êtes abonné a été retiré ou si votre licence a changé et la nouvelle n'inclut pas ce produit.
   - Les informations de licence Sophos ont été mises à jour. Des fonctions du produit ont pu changer.

8.2 Configuration des alertes antivirus et HIPS par email

Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - antivirus et HIPS** pour réaliser cette tâche.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

En cas de découverte d'un virus, d'un comportement suspect, d'une application indésirable ou d'une erreur sur un des ordinateurs du groupe, vous pouvez automatiser l'envoi d'alertes par email à des utilisateurs donnés.

Important
les ordinateurs Mac OS X peuvent envoyer ces alertes à une seule adresse seulement.

1. Dans le volet **Stratégies**, cliquez deux fois sur la stratégie antivirus et HIPS que vous désirez modifier.
2. Dans la boîte de dialogue **Stratégie antivirus et HIPS**, cliquez sur **Messagerie**.
3. Dans la boîte de dialogue **Messagerie**, allez dans l'onglet **Alertes par email** et sélectionnez **Activer les alertes par email**.
4. Dans le volet **Messages à envoyer**, sélectionnez les événements pour lesquels vous voulez envoyer des alertes par email.

   Remarque
   Les paramètres **Détection des comportements suspects**, **Détection des fichiers suspects**, **Détection et nettoyage des adwares et des PUA** et **Autres erreurs** s'appliquent seulement aux ordinateurs Windows.

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

   Important
   Les ordinateurs Mac OS X envoient uniquement des messages au premier destinataire de la liste.

6. Cliquez sur **Configurer SMTP** pour changer les paramètres du serveur SMTP et la langue des alertes par email.
7. Dans la boîte de dialogue **Configuration des paramètres SMTP**, saisissez les détails comme décrit ci-dessous :
   - Dans la zone de texte **Serveur SMTP**, saisissez le nom d'hôte ou l'adresse IP du serveur SMTP. Cliquez sur **Tester** pour vérifier si l'envoi de l'alerte par email fonctionne.
   - Dans la zone de texte **Adresse expéditeur SMTP**, saisissez une adresse électronique à laquelle les messages renvoyés et les rapports de non-distribution peuvent être envoyés.
   - Dans la zone de texte **Adresse réponse SMTP**, vous pouvez saisir une adresse électronique à laquelle les réponses aux alertes par email peuvent être envoyées. Les alertes par email sont envoyées depuis une boîte aux lettres sans surveillance.
   - Dans le volet **Langue**, cliquez sur la flèche du menu déroulant et sélectionnez la langue dans laquelle les alertes par email doivent être envoyées.

8.3 Configuration de la messagerie SNMP antivirus et HIPS

Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - antivirus et HIPS** pour réaliser cette tâche.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Il est possible de faire envoyer les messages SNMP à des utilisateurs particuliers lorsqu'un virus ou une erreur est rencontré sur un des ordinateurs du groupe.

Remarque
Ces paramètres s'appliquent uniquement aux ordinateurs Windows.

1. Dans le volet **Stratégies**, cliquez deux fois sur la stratégie antivirus et HIPS que vous désirez modifier.
2. Dans la boîte de dialogue **Stratégie antivirus et HIPS**, cliquez sur **Messagerie**.
3. Dans la boîte de dialogue **Messagerie**, allez dans l'onglet **Messagerie SNMP** et sélectionnez **Activer la messagerie SNMP**.
4. Dans le volet **Messages à envoyer**, sélectionnez les types d'événements pour lesquels vous voulez que Sophos Endpoint Security and Control envoie des messages SNMP.
5. Dans la zone de texte **Destination de déroutement SNMP**, saisissez l'adresse IP du destinataire.
6. Dans la zone de texte **Nom de la communauté SNMP**, saisissez le nom de la communauté SNMP.

8.4 Configuration de la messagerie de bureau antivirus et HIPS

Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - antivirus et HIPS** pour réaliser cette tâche.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Par défaut, les messages du bureau sont affichés sur l'ordinateur sur lequel un virus, un élément suspect ou une application potentiellement indésirable est trouvé. Vous pouvez configurer ces messages.

1. Dans le volet **Stratégies**, cliquez deux fois sur la stratégie antivirus et HIPS que vous désirez modifier.
2. Dans la boîte de dialogue **Stratégie antivirus et HIPS**, cliquez sur **Messagerie**.
3. Dans la boîte de dialogue **Messagerie**, cliquez sur l'onglet **Messagerie de bureau**.

   Par défaut, **Activer la messagerie de bureau** et toutes les options du volet **Messages à envoyer** sont sélectionnées. Modifiez ces paramètres, si nécessaire.

Remarque
Les paramètres **Détection des comportements suspects**, **Détection des fichiers suspects** et **Détection des adwares et des PUA** s'appliquent seulement aux ordinateurs Windows.

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

Remarque
Les messages de bureau définis par l'utilisateur ne s'affichent pas sur les ordinateurs à partir de Windows 8.

8.5 Configuration des alertes et des messages du contrôle des applications

Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - contrôle des applications** pour pouvoir configurer une stratégie de contrôle des applications.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

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

1. Dans le volet **Stratégies**, cliquez deux fois sur la stratégie de contrôle des applications que vous désirez modifier.
2. Dans la boîte de dialogue **Stratégie de contrôle des applications**, choisissez l'onglet **Messagerie**.

   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.
3. Dans la zone **Corps du message**, saisissez un message qui sera ajouté à la fin du message standard du bureau.

Remarque
Les messages de bureau définis par l'utilisateur ne s'affichent pas sur les ordinateurs à partir de Windows 8.

4. Si vous voulez envoyer des alertes par email sur les applications contrôlées détectées, sélectionnez la case à cocher **Activer les alertes par email**.
5. Sélectionnez la case **Activer la messagerie SNMP** si vous voulez envoyer des messages SNMP.

Remarque
Vos paramètres de stratégie antivirus et HIPS déterminent la configuration et les destinataires de la messagerie électronique et SNMP. Retrouvez plus de renseignements à la section Configuration de la messagerie SNMP antivirus et HIPS (page 193).

8.6 Configuration des alertes et des messages du contrôle des données

Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - contrôle des données** pour modifier une stratégie de contrôle des données.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

L'Enterprise Console utilise des événements et des messages pour signaler quand le transfert des données sensibles est détecté ou bloqué.

Retrouvez plus de renseignements sur les stratégies et les événements de contrôle des données à la section Stratégie de contrôle des données (page 150).

Lorsque le contrôle des données est activé, les événements et messages suivants sont consignés ou affichés par défaut :

- Les événements de contrôle des données sont consignés sur la station de travail.
- Les événements de contrôle des données sont envoyés à l'Enterprise Console et sont visibles dans le **Contrôle des données - Observateur d'événements** (pour ouvrir l'observateur d'événements, dans le menu **Événements**, cliquez sur **Événements du contrôle des données**).

  Remarque
  chaque ordinateur peut envoyer à l'Enterprise Console un maximum de 50 événements de contrôle des données par heure.

- Le nombre d'ordinateurs avec des événements de contrôle des données au-dessus d'un seuil spécifié dans les sept derniers jours apparaît sur le Tableau de bord.
- Des messages apparaissent sur le bureau de la station de travail.

Vous pouvez aussi configurer l'Enterprise Console pour qu'elle envoie les messages suivants :

Alertes par email	Un message électronique est envoyé aux destinataires que vous spécifiez.
Messages SNMP	Un message SNMP est envoyé aux destinataires spécifiés dans vos paramètres de stratégie antivirus et HIPS.

Pour configurer la messagerie du contrôle des données :

1. Vérifiez quelle stratégie de contrôle des données est utilisée par le groupe ou les groupes d'ordinateurs que vous souhaitez configurer.

   Retrouvez plus de renseignements à la section Vérification des stratégies utilisées par un groupe (page 27).
2. Dans le volet **Stratégies**, cliquez deux fois sur **Contrôle des données**. Puis cliquez deux fois sur la stratégie que vous désirez changer.
   La boîte de dialogue **Stratégie de contrôle des données** apparaît.

3. Dans la boîte de dialogue **Stratégie de contrôle des données**, choisissez l'onglet **Messagerie**. La messagerie de bureau est activée par défaut et **Inclure les règles correspondantes dans les messages** est sélectionné.
4. Saisissez les messages qui seront ajoutés aux messages standard pour confirmation par l'utilisateur du transfert des fichiers et pour le transfert des fichiers bloqués, si vous le souhaitez.

   Vous pouvez saisir un maximum de 100 caractères. Vous pouvez également ajouter un lien HTML au message, par exemple, À propos de Sophos.

   Remarque
   Les messages de bureau définis par l'utilisateur ne s'affichent pas sur les ordinateurs à partir de Windows 8.

5. Pour activer les alertes par email, sélectionnez la case à cocher **Activer les alertes par email**. Dans le champ **Destinataires des emails**, saisissez les adresses électroniques des destinataires. Séparez chaque adresse par un point-virgule (;).
6. Pour activer la messagerie SNMP, sélectionnez la case à cocher **Activer la messagerie SNMP**.

   Les paramètres du serveur de messagerie et de déroutement SNMP sont configurés via la stratégie antivirus et HIPS.

8.7 Configuration des alertes et des messages du contrôle des périphériques

Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - contrôle des périphériques** pour modifier une stratégie de contrôle des périphériques.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

L'Enterprise Console utilise des événements et des messages pour signaler quand un périphérique contrôlé est détecté ou bloqué.

Retrouvez plus de renseignements sur les stratégies et les événements de contrôle des périphériques à la section Stratégie de contrôle des périphériques (page 165).

Lorsque le contrôle des périphériques est activé, les événements et messages suivants sont consignés ou affichés par défaut :

- Les événements de contrôle des périphériques sont consignés sur la station de travail.
- Les événements de contrôle des périphériques sont envoyés à l'Enterprise Console et sont visibles dans le **Contrôle des périphériques - Observateur d'événements** (pour ouvrir l'observateur d'événements, dans le menu **Événements**, cliquez sur **Événements du contrôle des données**).
- Le nombre d'ordinateurs avec des événements de contrôle des périphériques au-dessus d'un seuil spécifié dans les sept derniers jours apparaît sur le Tableau de bord.
- Des messages apparaissent sur le bureau de la station de travail.

Vous pouvez aussi configurer l'Enterprise Console pour qu'elle envoie les messages suivants :

Alertes par email	Un message électronique est envoyé aux destinataires que vous indiquez.

Messages SNMP	Un message SNMP est envoyé aux destinataires spécifiés dans vos paramètres de stratégie antivirus et HIPS.

Pour configurer la messagerie du contrôle des périphériques :

1. Vérifiez quelle stratégie de contrôle des applications est utilisée par le ou les groupes d'ordinateurs que vous souhaitez configurer.

   Retrouvez plus de renseignements à la section Vérification des stratégies utilisées par un groupe (page 27).
2. Dans le volet **Stratégies**, cliquez deux fois sur **Contrôle des données**. Puis cliquez deux fois sur la stratégie que vous désirez changer.
3. Dans la boîte de dialogue **Stratégie de contrôle des périphériques**, sur l'onglet **Messagerie**, la messagerie de bureau est activée par défaut. Pour une configuration avancée de la messagerie, procédez ainsi :

   - *Pour saisir un texte de message pour la messagerie de bureau*, dans la zone **Corps du message**, saisissez un message qui sera ajouté à la fin du message standard.

     Vous pouvez saisir un maximum de 100 caractères. Vous pouvez également ajouter un lien HTML au message, par exemple, À propos de Sophos.

     Remarque
     Les messages de bureau définis par l'utilisateur ne s'affichent pas sur les ordinateurs à partir de Windows 8.

   - *Pour activer les alertes par email*, sélectionnez la case à cocher **Activer les alertes par email**. Dans le champ **Destinataires des emails**, saisissez les adresses électroniques des destinataires. Séparez chaque adresse par un point-virgule (;).
   - *Pour activer la messagerie SNMP*, sélectionnez la case à cocher **Activer la messagerie SNMP**.

   Les paramètres du serveur de messagerie et de déroutement SNMP sont configurés via la stratégie antivirus et HIPS.

8.8 Configuration des alertes par email sur l'état du réseau

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Configuration système** pour configurer les alertes par email sur l'état du réseau. Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Vous pouvez configurer l'envoi des alertes par email aux destinataires de votre choix lorsqu'un niveau d'alerte ou critique a été dépassé pour une section du tableau de bord.

1. Dans le menu **Outils**, sélectionnez **Configurer les alertes par email**.
   La boîte de dialogue **Configuration des alertes par email** apparaît.
2. Si les paramètres SMTP n'ont pas été configurés ou si vous voulez afficher 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 email** 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 email.
6. Dans le volet **Abonnements**, sélectionnez les alertes par email « niveau d'alerte dépassé » et « niveau critique dépassé » que vous souhaitez envoyer au destinataire.

8.9 Configuration des alertes par email pour la synchronisation avec Active Directory

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Configuration système** pour configurer les alertes par email de synchronisation Active Directory. Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Vous pouvez configurer l'envoi d'alertes par email aux destinataires de votre choix pour les informer de la découverte de nouveaux ordinateurs et groupes au cours des synchronisations avec Active Directory. Si vous choisissez de protéger automatiquement les ordinateurs dans les groupes synchronisés, vous pouvez aussi configurer les alertes concernant les échecs de la protection automatique.

1. Dans le menu **Outils**, sélectionnez **Configurer les alertes par email**.
   La boîte de dialogue **Configuration des alertes par email** apparaît.
2. Si les paramètres SMTP n'ont pas été configurés ou si vous voulez afficher 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 email** 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 email.
6. Dans le volet **Abonnements**, sélectionnez les alertes par email « Synchronisation avec Active Directory » que vous souhaitez envoyer au destinataire.

   Alertes par email « Synchronisation avec Active Directory » :

   - Nouveaux groupes découverts
   - Nouveaux ordinateurs découverts
   - Échec de la protection automatique des ordinateurs

8.10 Configuration de la journalisation des événements Windows

Si vous utilisez l'administration déléguée :

- Vous devez disposer du droit **Paramétrage de la stratégie - antivirus et HIPS** pour réaliser cette tâche.
- Vous ne pouvez pas modifier une stratégie si elle est appliquée hors de votre sous-parc actif.

Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Par défaut, Sophos Endpoint Security and Control ajoute des alertes au journal des événements Windows lorsqu'un virus ou spyware est détecté ou nettoyé, un comportement ou un fichier suspect est détecté ou un adware ou PUA est détecté ou nettoyé.

Pour modifier ces paramètres :

1. Dans le volet **Stratégies**, cliquez deux fois sur la stratégie antivirus et HIPS que vous désirez modifier.
2. Dans la boîte de dialogue **Stratégie antivirus et HIPS**, cliquez sur **Messagerie**.
3. Dans la boîte de dialogue **Messagerie**, allez sur l'onglet **Journalisation des événements**.

   Par défaut, la journalisation des événements est activée. Modifiez, le cas échéant, les paramètres.

   Erreurs de contrôle inclut des instances où l'accès à un élément que Sophos Endpoint Security and Control tente de contrôler lui est refusé.

8.11 Activation ou désactivation de l'envoi de commentaires à Sophos

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Configuration système** pour activer ou désactiver l'envoi de commentaires à Sophos. Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Enterprise Console va régulièrement envoyer un rapport à Sophos. Ces rapports permettront à Sophos de mieux comprendre comment sont utilisés nos produits et nous aideront à améliorer nos produits et services. Retrouvez plus de renseignements sur les informations collectées et sur leur traitement dans le Contrat de licence de l'utilisateur final (CLUF) de Sophos et dans la Politique de confidentialité de Sophos ci-dessous : http://www.sophos.fr/legal.

Certaines informations mentionnées dans le rapport sont facultatives alors que d'autres sont obligatoires comme expliqué dans le Contrat de licence de l'utilisateur final (CLUF) de Sophos et dans la Politique de confidentialité. Vous pouvez choisir à tout moment de ne pas envoyer de rapports en modifiant le paramètre **Commentaires à Sophos**.

Par défaut, l'envoi de commentaires à Sophos est activé. Vous avez la possibilité de désactiver cette option dans l'assistant d'installation de la Sophos Enterprise Console lors de l'installation ou de la mise à niveau de la console.

Si vous voulez activer ou désactiver l'envoi de commentaires à Sophos après l'installation, procédez comme suit :

1. Dans le menu **Outils**, cliquez sur **Envoyer des commentaires à Sophos**.
2. Dans la boîte de dialogue **Envoi de commentaires à Sophos**, vous pouvez activer ou désactiver l'envoi de commentaires.

- *Si vous souhaitez activer l'envoi de commentaires à Sophos,* veuillez lire l'accord et sélectionnez la case **J'accepte** si vous acceptez les conditions de l'accord.
- *Si vous souhaitez désactiver l'envoi de commentaires à Sophos,* dessélectionnez la case **J'accepte**.

9 Affichage des événements

Lorsqu'un événement de contrôle des applications, de contrôle des données, de contrôle des périphériques, de pare-feu, d'évaluation des correctifs, de protection antialtération, de contrôle du Web ou de prévention des Exploits se produit sur un terminal, par exemple, si une application a été bloquée par le pare-feu, l'événement est envoyé à l'Enterprise Console et peut être visualisé dans l'observateur d'événements correspondant.

Grâce aux observateurs d'événements, vous pouvez examiner 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 données ces sept derniers jours générés par un utilisateur donné.

Le nombre d'ordinateurs avec des événements au-dessus d'un seuil spécifié dans les sept derniers jours apparaît sur le Tableau de bord (sauf pour les événements de protection antialtération). Retrouvez plus de renseignements sur la manière de configurer le seuil à la section Configuration du tableau de bord (page 49).

Vous pouvez aussi configurer l'envoi des alertes par email aux destinataires de votre choix lorsqu'un événement s'est produit. Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

9.1 Affichage des événements du contrôle des applications

Pour afficher les événements du contrôle des applications :

1. Dans le menu **Événements**, cliquez sur **Événements du contrôle des applications**.
   La boîte de dialogue **Contrôle des applications - 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 afficher les événements pour un utilisateur ou un ordinateur donné, saisissez son nom dans le champ prévu.

   Si vous laissez les champs vides, les événements de tous les utilisateurs et ordinateurs apparaîtront.

   Vous pouvez utiliser des caractères de remplacement dans ces champs. Utilisez ? pour remplacer un seul caractère du nom et * pour remplacer une chaîne de caractères quelconque.
4. Si vous voulez afficher les événements d'un type d'application donné, dans le champ **Type d'application**, cliquez sur la flèche du menu déroulant et sélectionnez le type d'application.

   Par défaut, l'observateur d'événements affiche les événements de tous les types d'applications.
5. Cliquez sur **Rechercher** pour afficher une liste d'événements.

Vous pouvez exporter dans un fichier la liste des événements du contrôle des applications. Retrouvez plus de renseignements à la section Exportation dans un fichier de la liste des événements (page 210).

9.2 Affichage des événements du contrôle des données

Remarque
Cette fonction ne sera pas disponible si le contrôle des données n'est pas inclus dans votre licence.

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Événements du contrôle des données** pour voir les événements du contrôle des données dans Enterprise Console. Retrouvez plus de renseignements sur l'administration déléguée à la section Gestion des rôles et des sous-parcs (page 14).

Pour afficher les événements du contrôle des données :

1. Dans le menu **Événements**, cliquez sur **Événements du contrôle des données**.
   La boîte de dialogue **Contrôle des données - 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 afficher les événements pour un utilisateur, un ordinateur ou un fichier donné, saisissez son nom dans le champ prévu.

   Si vous laissez les champs vides, les événements de tous les utilisateurs, ordinateurs et fichiers apparaîtront.

   Vous pouvez utiliser des caractères de remplacement dans ces champs. Utilisez ? pour remplacer un seul caractère du nom et * pour remplacer une chaîne de caractères quelconque.
4. Si vous voulez afficher les événements pour une règle donnée, dans le champ **Nom de la règle**, cliquez sur la flèche du menu déroulant et sélectionnez le nom de la règle.

   Par défaut, l'observateur d'événements affiche les événements de toutes les règles.
5. Si vous voulez afficher les événements pour un type de fichier donné, dans le champ **Type de fichier**, cliquez sur la flèche du menu déroulant et sélectionnez le type de fichier.

   Par défaut, l'observateur d'événements affiche les événements de tous les types de fichiers.
6. Cliquez sur **Rechercher** pour afficher une liste d'événements.

Vous pouvez exporter dans un fichier la liste des événements du contrôle des données. Retrouvez plus de renseignements à la section Exportation dans un fichier de la liste des événements (page 210).

9.3 Affichage des événements du contrôle des périphériques

Pour afficher les événements du contrôle des périphériques :

1. Dans le menu **Événements**, cliquez sur **Événements du contrôle des périphériques**.
   La boîte de dialogue **Contrôle des périphériques - Observateur d'événements** apparaît.
2. Dans le champ **Période de recherche**, cliquez sur la flèche du menu déroulant et sélectionnez la période pour laquelle vous souhaitez afficher les événements.

Vous pouvez sélectionner soit une période fixe, par exemple, **Depuis 24 heures**, soit **Personnalisée** et spécifiez votre propre période en sélectionnant les dates de début et de fin.

3. Si vous voulez afficher les événements pour un certain type de périphérique donné, dans le champ **Type de périphérique**, cliquez sur la flèche du menu déroulant et sélectionnez le type de périphérique.

   Par défaut, l'observateur d'événements affiche les événements de tous les types de périphériques.

   Remarque
   Si vous définissez les lecteurs de disques optiques sur « Lecture seule », les événements liés à ces périphériques ne sont pas affichés dans l'observateur des événements.

4. Si vous voulez afficher les événements pour un utilisateur ou un ordinateur donné, saisissez son nom dans le champ prévu.

   Si vous laissez les champs vides, les événements de tous les utilisateurs et ordinateurs apparaîtront.

   Vous pouvez utiliser des caractères de remplacement dans ces champs. Utilisez ? pour remplacer un seul caractère du nom et * pour remplacer une chaîne de caractères quelconque.
5. Cliquez sur **Rechercher** pour afficher une liste d'événements.

Dans la boîte de dialogue **Contrôle des périphériques - Observateur d'événements**, vous pouvez exempter un périphérique des stratégies de contrôle des périphériques. Retrouvez plus de renseignements à la section Exemption d'un périphérique de toutes les stratégies (page 170).

Vous pouvez exporter dans un fichier la liste des événements du contrôle des périphériques. Retrouvez plus de renseignements à la section Exportation dans un fichier de la liste des événements (page 210).

9.4 Affichage des événements du pare-feu

Les événements de pare-feu sont seulement envoyés une seule fois depuis un terminal vers la console. Les événements identiques provenant de différents terminaux sont regroupés dans **Pare-feu - Observateur d'événements**. Dans la colonne **Décompte**, vous pouvez voir le nombre total de fois qu'un événement a été envoyé depuis différents terminaux.

Pour consulter les événements du pare-feu :

1. Dans le menu **Événements**, cliquez sur **Événements du pare-feu**.
   La boîte de dialogue **Pare-feu - Observateur d'événements** apparaît.
2. Dans le champ **Période de recherche**, cliquez sur la flèche du menu déroulant et sélectionnez la période pour laquelle vous souhaitez afficher les événements.

   Vous pouvez sélectionner soit une période fixe, par exemple, **Depuis 24 heures**, soit **Personnalisée** et spécifiez votre propre période en sélectionnant les dates de début et de fin.
3. Si vous voulez consulter les événements d'un certain type, dans le champ **Type d'événement**, cliquez sur la flèche du menu déroulant et sélectionnez le type d'événement.

   Par défaut, l'observateur d'événements affiche tous les types d'événements.
4. Si vous voulez consulter les événements pour un certain fichier, saisissez le nom du fichier dans le champ **Nom du fichier**.

   Si vous laissez ce champ vide, les événements de tous les fichiers apparaîtront.

   Vous pouvez utiliser des caractères joker dans ce champ. Utilisez ? pour remplacer un seul caractère du nom et * pour remplacer une chaîne de caractères quelconque.
5. Cliquez sur **Rechercher** pour afficher une liste d'événements.

Dans la boîte de dialogue **Pare-feu - Observateur d'événements**, vous pouvez créer une règle de pare-feu comme le décrit la section Création d'une règle d'événement de pare-feu (page 121).

Vous pouvez exporter dans un fichier la liste des événements du pare-feu. Retrouvez plus de renseignements à la section Exportation dans un fichier de la liste des événements (page 210).

9.5 Affichage des événements de protection antialtération

Il y a deux types d'événements de protection antialtération :

- Les événements réussis d'authentification de la protection antialtération affichant le nom de l'utilisateur authentifié et l'heure d'authentification.
- Les tentatives ratées de modifications affichant le nom du produit ou du composant Sophos pris pour cible, l'heure de la tentative et des informations détaillées sur l'utilisateur responsable de cette tentative.

Pour afficher les événements de protection antialtération :

1. Dans le menu **Événements**, cliquez sur **Événements de protection antialtération**.
   La boîte de dialogue **Protection antialtération - Observateur d'événements** apparaît.
2. Dans le champ **Période de recherche**, cliquez sur la flèche du menu déroulant et sélectionnez la période pour laquelle vous souhaitez afficher les événements.

   Vous pouvez sélectionner soit une période fixe, par exemple, **Depuis 24 heures**, soit **Personnalisée** et spécifiez votre propre période en sélectionnant les dates de début et de fin.
3. Si vous souhaitez voir certains types d'événements, dans le champ **Type d'événements**, cliquez sur la flèche du menu déroulant et sélectionnez le type d'événements.

   Par défaut, l'observateur d'événements affiche les événements de tous les types.
4. Si vous voulez afficher les événements pour un utilisateur ou un ordinateur donné, saisissez son nom dans le champ prévu.

   Si vous laissez les champs vides, les événements de tous les utilisateurs et ordinateurs apparaîtront.

   Vous pouvez utiliser des caractères de remplacement dans ces champs. Utilisez ? pour remplacer un seul caractère du nom et * pour remplacer une chaîne de caractères quelconque.
5. Cliquez sur **Rechercher** pour afficher une liste d'événements.

Vous pouvez exporter la liste des événements dans un fichier. Retrouvez plus de renseignements à la section Exportation dans un fichier de la liste des événements (page 210).

9.6 Événements d'évaluation des correctifs

Remarque
Cette fonction ne sera pas disponible si l'évaluation des correctifs n'est pas incluse dans votre licence.

La boîte de dialogue **Évaluation des correctifs - Observateur d'événements** contient des informations sur tous les correctifs de sécurité et sur tous les résultats des évaluations des correctifs.

Le champ **Mises à jour des correctifs** affiche l'état de téléchargement des informations relatives aux correctifs. Il affiche un des messages d'état suivants :

- **Non téléchargées** indique que les informations relatives au correctif ne sont pas téléchargées ou que vous n'avez pas la licence d'utilisation de la fonctionnalité Correctif.
- **Téléchargement** indique que le premier téléchargement, après l'installation, est en cours.
- **OK** indique que les informations relatives au correctif sont à jour.
- **Expirées** indique que la mise à jour des données de correctif n'a pas complètement réussie dans les dernières 72 heures. En général, cet état apparaît si SEC n'est pas à jour à cause de problèmes de connectivité réseau. Il peut également apparaître si vous passez d'une licence SEC avec la fonction Correctif vers une licence sans cette fonction. Une mise à jour partielle peut s'être produite lorsque ce message d'état apparaît.

La boîte de dialogue **Évaluation des correctifs - Observateur d'événements** comporte les onglets suivants :

Correctifs par niveau

Cet onglet affiche par défaut les correctifs manquants. Chaque correctif apparaît accompagné de la comptabilisation des ordinateurs sur lesquels le correctif n'est pas présent, ainsi que des menaces et des vulnérabilités associées au correctif. Vous pouvez utiliser des filtres pour afficher une liste complète de tous les correctifs pris en charge avec une comptabilisation du nombre d'ordinateurs sur lesquels ils ne sont pas installés.

Ordinateurs avec correctifs manquants

Cet onglet affiche l'état de l'évaluation des correctifs par ordinateur. Chaque ordinateur est affiché en même temps que tous ses correctifs manquants. Les ordinateurs sont répertoriés plusieurs fois si plus d'un correctif est manquant.

9.6.1 Affichage des événements d'évaluation des correctifs

Pour voir les événements d'évaluation des correctifs :

1. Dans le menu **Événements**, cliquez sur **Événements d'évaluation des correctifs**.
   La boîte de dialogue **Évaluation des correctifs - Observateur d'événements** apparaît.
2. Cliquez sur l'un des onglets **Correctifs par niveau** ou **Ordinateurs avec correctifs manquants**. Retrouvez plus de renseignements sur les onglets à la section Événements d'évaluation des correctifs (page 204).
3. Dans le panneau de recherche, si vous voulez afficher les événements concernant un certain correctif par son nom, un ordinateur, une menace ou une vulnérabilité, saisissez les informations dans le champ respectif. Les critères disponibles sont basés sur les informations affichées dans l'onglet.

   Si vous laissez les champs vides, les événements de tous les noms de correctif, de tous les identifiants de correctif et de tous les noms d'ordinateurs apparaîtront.

   Vous pouvez utiliser des caractères de remplacement dans ces champs. Utilisez ? pour remplacer un seul caractère du nom et * pour remplacer une chaîne de caractères quelconque.
4. Si vous désirez voir les événements concernant un certain correctif par état, classification, éditeur, groupe ou date de publication, cliquez sur la flèche du menu déroulant du champ respectif et sélectionnez l'option qui convient. Les critères disponibles sont basés sur les informations affichées dans l'onglet.

   Par défaut, l'observateur d'événements affiche les événements pour les taux de menace, les éditeurs, les groupes, les menaces et les noms des correctifs manquants.

5. Cliquez sur **Rechercher** pour afficher une liste d'événements de correctifs.
   Retrouvez plus de renseignements sur les résultats affichés à la section Catégories de résultats de recherche (page 206).

Vous pouvez cliquer avec le bouton droit de la souris sur un lien individuel pour copier son nom ou utiliser les touches Ctrl+C pour copier une rangée d'événements d'évaluation des correctifs dans le Presse-papier.

Vous pouvez exporter la liste des événements de l'évaluation des correctifs. Retrouvez plus de renseignements à la section Exportation dans un fichier de la liste des événements (page 210).

Vous pouvez voir plus de détails à propos d'un correctif spécifique en cliquant sur le lien mis à disposition. Retrouvez plus de renseignements à la section Affichage des détails sur les correctifs, menaces ou vulnérabilités (page 206).

9.6.2 Affichage des détails sur les correctifs, menaces ou vulnérabilités

Pour voir les détails sur les correctifs, menaces ou vulnérabilités :

1. Dans le menu **Événements**, cliquez sur **Événements d'évaluation des correctifs**.
   La boîte de dialogue **Évaluation des correctifs - Observateur d'événements** apparaît.
2. Cliquez sur l'un des onglets **Correctifs par notation** ou **Ordinateurs avec correctifs manquants**, sélectionnez les options requises et cliquez sur **Rechercher** pour afficher une liste d'événements.
   Retrouvez plus de renseignements sur les résultats affichés à la section Catégories de résultats de recherche (page 206).
3. Cliquez sur le nom du correctif à propos duquel vous souhaitez voir plus d'informations.
4. Dans la boîte de dialogue **Détails du correctif**, vous pouvez voir la description du correctif et des informations à propos des menaces et vulnérabilités contre lesquelles il assure la protection. Si disponible :
   - Cliquez sur le nom du correctif pour ouvrir un navigateur Web et voir les informations de l'éditeur du correctif.
   - Cliquez sur la menace pour ouvrir un navigateur Web et voir l'analyse des menaces et les conseils de Sophos pour assurer votre protection.
   - Cliquez sur la vulnérabilité pour ouvrir un navigateur Web et voir des informations sur les CVE (common vulnerabilities and exposures).
   - Cliquez sur le nom du correctif dans la colonne **Déjà corrigées par** pour ouvrir un navigateur Web et consulter les informations de l'éditeur à propos du correctif ayant été remplacé.

La liste est classée en ordre alphabétique par menace et par vulnérabilité.

9.6.3 Catégories de résultats de recherche

Les résultats de la recherche apparaissent dans différentes catégories en fonction de l'onglet :

- Correctifs par niveau (page 207)
- Ordinateurs avec correctifs manquants (page 207)

Correctifs par niveau

Les résultats de la recherche apparaissent en fonction des catégories suivantes :

- **Menaces** : une menace peut être un virus, un cheval de Troie, un ver, un spyware, un site Web malveillant, mais aussi un adware ou tout autre application potentiellement indésirable. Vous pouvez cliquer sur le nom de la menace pour voir l'analyse de la menace par Sophos et ses conseils dans un navigateur web.
- **Vulnérabilités** : une vulnérabilité est une faiblesse du logiciel pouvant être exploité par un attaquant. Les dommages potentiels pouvant être causés par l'exploitation dépendent de la nature de la vulnérabilité et des logiciels affectés. Les correctifs sont fournis pour réparer les vulnérabilités afin que l'exploitation ne soit plus possible. Vous pouvez cliquer sur le nom de la vulnérabilité pour voir les informations relatives aux vulnérabilités et expositions fréquentes (CVE, common vulnerabilities and exposures) dans un navigateur Web.
- **Niveau** : les correctifs sont classés par les SophosLabs.

  Remarque
  Nous conseillons l'application de tous les correctifs manquants, quel que soit leur niveau.

  - **Critique** : il est presque certain qu'une ou plusieurs vulnérabilités traitées par ce correctif seront exploitées.
  - **Élevé** : il est fortement probable qu'une ou plusieurs vulnérabilités traitées par ce correctif seront exploitées.
  - **Moyen** : il est possible qu'une ou plusieurs vulnérabilités traitées par ce correctif seront exploitées.
  - **Faible** : il est improbable qu'une ou plusieurs vulnérabilités traitées par ce correctif seront exploitées.
- **Nom du correctif** : affiche le nom du correctif. Vous pouvez cliquer sur le nom du correctif pour ouvrir un navigateur Web et voir les informations de l'éditeur du correctif.
- **Éditeur** : affiche le nom de l'éditeur qui a publié le correctif.
- **Ordinateurs** : affiche le nombre d'ordinateurs affectés. Si un ou plusieurs ordinateurs sont affectés, vous pouvez cliquer sur le nombre pour voir les détails dans l'onglet **Ordinateurs avec correctifs manquants**. Si vous voyez apparaître un "-", ceci signifie que le correctif n'a pas été évalué.
- **Remplacé par** : affiche le(s) nom(s) de tous les correctifs remplaçant le correctif précédent. Vous pouvez cliquer sur le nom du correctif pour ouvrir la boîte de dialogue **Détails du correctif** pour voir les informations à propos du correctif remplaçant.
- **Date de publication** : affiche la date de publication du correctif.

Ordinateurs avec correctifs manquants

Les résultats de la recherche apparaissent en fonction des catégories suivantes :

- **Ordinateur** : affiche le nom de l'ordinateur qui est affecté.
- **Niveau** : les correctifs sont classés par les SophosLabs.

Remarque
Nous conseillons l'application de tous les correctifs manquants, quel que soit leur niveau.

- **Critique** : il est presque certain qu'une ou plusieurs vulnérabilités traitées par ce correctif seront exploitées.
- **Élevé** : il est fortement probable qu'une ou plusieurs vulnérabilités traitées par ce correctif seront exploitées.
- **Moyen** : il est possible qu'une ou plusieurs vulnérabilités traitées par ce correctif seront exploitées.
- **Faible** : il est improbable qu'une ou plusieurs vulnérabilités traitées par ce correctif seront exploitées.

- **Nom du correctif** : affiche le nom du correctif. Vous pouvez cliquer sur le nom du correctif pour ouvrir un navigateur Web et voir les informations de l'éditeur du correctif.
- **Remplacé par** : affiche le(s) nom(s) de tous les correctifs remplaçant le correctif précédent. Vous pouvez cliquer sur le nom du correctif pour ouvrir la boîte de dialogue **Détails du correctif** pour voir les informations à propos du correctif remplaçant.
- **Dernière évaluation** : affiche la date à laquelle un ordinateur a été évalué pour la dernière fois à la recherche des correctifs manquants.
- **Éditeur** : affiche le nom de l'éditeur qui a publié le correctif.
- **Date de publication** : affiche la date de publication du correctif.
- **Groupe** : affiche le nom du groupe auquel appartient l'ordinateur.

9.7 Affichage des événements Web

Remarque
Cette fonction ne sera pas disponible si le contrôle du Web n'est pas inclut dans votre licence.

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Événements Web** pour voir les événements Web dans Enterprise Console. Retrouvez plus de renseignements sur l'administration déléguée à la section Gestion des rôles et des sous-parcs (page 14).

Vous pouvez voir les événements Web suivants dans l'Observateur d'événements Web :

- Les sites Web malveillants bloqués par la fonctionnalité de protection Web dans la stratégie **Antivirus et HIPS**.
- Les événements de contrôle du Web, si vous utilisez la fonctionnalité de contrôle du Web.

Les événements de contrôle du Web apparaissent différemment, en fonction de la stratégie de contrôle du Web sélectionnée. Bien que l'Observateur d'événements Web puisse être utilisé dans les deux modes de stratégie, le contenu est différent.

Lorsque l'option de stratégie **Contrôle des sites Web inappropriés** est sélectionnée, vous pouvez voir toutes les actions « Bloquer » et « Avertir ». Les sites HTTPS visités classés dans « Avertir » sont journalisés en tant qu'événements « Continuer » car Sophos Endpoint Security and Control répond différemment à HTTPS (voir la remarque à la section Contrôle des sites Web inappropriés (page 179)).

Lorsque **Contrôle intégral du Web** est sélectionné, les événements apparaissent sur l'appliance.

- Pour Sophos Web Appliance ou Sophos Management Appliance, vous pouvez afficher l'activité de navigation à l'aide des fonctions **Rapports** et **Rechercher**. Les actions « Bloquer »« Avertir, » et « Autoriser » apparaissent. Les sites HTTPS visités classés dans « Avertir » sont affichés en tant qu'événements « Continuer » car Sophos Endpoint Security and Control répond différemment à HTTPS (voir la remarque à la section Contrôle intégral du Web (page 184)).
- Pour UTM, veuillez utiliser la page **Journaux et rapports** > **Web Protection** > **Rapport d'utilisation du Web**. Vous pouvez voir les actions vous indiquant si le site Web a été livré au client (autorisé), s'il a été bloqué par une règle de contrôle des applications ou si l'utilisateur est parvenu à accéder à une page à l'aide de la fonction de blocage (remplacement), ainsi que d'autres informations.

Remarque
Quelle que soit la stratégie que vous sélectionnez, les sites Web contrôlés et évalués par le filtrage instantané des URL (Protection Web (page 104)) de Sophos Endpoint Security and Control apparaissent comme des événements Web dans Enterprise Console.

Pour voir les événements Web :

1. Dans le menu **Événements**, cliquez sur **Événements Web**.
   La boîte de dialogue **Web - Observateur d'événements** apparaît.
2. Dans la boîte **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 afficher les événements pour un **Utilisateur** ou un **Ordinateur** donné, saisissez son nom dans le champ prévu.

   Si vous laissez les champs vides, les événements de tous les utilisateurs et ordinateurs apparaîtront.

   Vous pouvez utiliser des caractères joker dans ces champs. Utilisez ? pour remplacer un seul caractère du nom et * pour remplacer une chaîne de caractères quelconque.
4. Si vous voulez afficher les événements associés à une certaine action, dans le champ **Action**, cliquez sur la flèche du menu déroulant et sélectionnez l'action.
5. Si vous voulez afficher les événements associés à un domaine spécifique, saisissez-le dans le champ **Domaine**.
6. Si vous voulez afficher les événements qui ont été déclenchés pour une **Raison** donnée, cliquez sur la flèche du menu déroulant et sélectionnez la raison.
7. Cliquez sur **Rechercher** pour afficher une liste d'événements.

Vous pouvez exporter dans un fichier la liste des événements Web. Retrouvez plus de renseignements à la section Exportation dans un fichier de la liste des événements (page 210).

9.7.1 Affichage des derniers événements Web sur un ordinateur

Vous pouvez voir les 10 derniers événements pour lesquels une mesure a été prise sur un terminal, par exemple, les sites Web récemment bloqués.

Pour voir les événements Web les plus récents :

1. Dans la vue **Terminaux**, dans la liste des ordinateurs, cliquez deux fois sur l'ordinateur pour lequel vous souhaitez voir l'activité.
2. Dans la boîte de dialogue **Détails de l'ordinateur**, défilez vers le bas jusqu'à **Événements Web les plus récents**.

Vous pouvez aussi afficher le nombre d'événements pour un utilisateur en générant un rapport. Retrouvez plus de renseignements à la section Configuration du rapport Événements par utilisateur (page 218).

9.8 Affichage des événements de prévention des Exploits

Remarque
Cette fonction ne sera pas disponible si la prévention des Exploits n'est pas incluse dans votre licence.

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Prévention des Exploits** pour voir les événements de prévention des Exploits dans Enterprise Console. Retrouvez plus de renseignements sur l'administration déléguée à la section Gestion des rôles et des sous-parcs (page 14).

Pour voir les alertes de prévention des Exploits :

1. Dans le menu **Événements**, cliquez sur **Prévention des Exploits**.
   La boîte de dialogue **Prévention des Exploits - Observateur d'événements** apparaît.
2. Dans la boîte **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 afficher les événements pour un **Utilisateur** ou un **Ordinateur** donné, saisissez son nom dans le champ prévu.

   Si vous laissez les champs vides, les événements de tous les utilisateurs et ordinateurs apparaîtront.

   Vous pouvez utiliser des caractères de remplacement dans ces champs. Utilisez ? pour remplacer un seul caractère du nom et * pour remplacer une chaîne de caractères quelconque.
4. Si vous voulez afficher les événements associés à une certaine action, dans le champ **Type**, cliquez sur la flèche du menu déroulant et sélectionnez l'action.
5. Cliquez sur **Rechercher** pour afficher une liste d'événements.

- Vous pouvez exporter dans un fichier la liste des événements de prévention des Exploits. Retrouvez plus de renseignements à la section Exportation dans un fichier de la liste des événements (page 210).
- Vous pouvez exclure les événements de prévention des Exploits de la prévention des Exploits. Retrouvez plus de renseignements à la section Exclusion des événements de la prévention des Exploits (page 211).

9.9 Exportation dans un fichier de la liste des événements

Vous pouvez exporter dans un fichier CSV la liste des événements du contrôle des applications, du contrôle des données, du contrôle des périphériques, de pare-feu, d'évaluation des correctifs, de protection antialtération, Web ou de prévention des Exploits. Vous pouvez aussi exporter dans un fichier PDF la liste des événements de l'évaluation des correctifs.

1. Dans le menu **Événements**, 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.

   Retrouvez plus de renseignements aux sections :

   - Affichage des événements du contrôle des applications (page 201)
   - À propos des événements du contrôle des données (page 155)
   - À propos des événements du contrôle des périphériques (page 166)
   - Affichage des événements du pare-feu (page 203)
   - Événements d'évaluation des correctifs (page 204)
   - Affichage des événements de protection antialtération (page 204)
   - Affichage des événements Web (page 208)
   - Affichage des événements de prévention des Exploits (page 210)
3. Cliquez sur **Exporter**.
4. Dans la fenêtre **Enregistrer sous**, naviguez jusqu'à la destination de votre choix pour le fichier, saisissez un nom de fichier dans la boîte de dialogue **Nom de fichier** et sélectionnez un type de fichier dans la boîte de dialogue **Type de fichier**.
5. Cliquez sur **Enregistrer**.

9.10 Exclusion des événements de la prévention des Exploits

Vous pouvez exclure les événements d'applications et de prévention des Exploits en sélectionnant les événements spécifiques à partir de l'observateur d'événements.

1. Dans le menu **Événements**, cliquez sur **Événements de prévention des Exploits**.
   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.

   Retrouvez plus de renseignements à la section Affichage des événements de prévention des Exploits (page 210).
3. Cliquez sur un événement puis sur **Exclure**.
   La boîte de dialogue **Exclusions de la prévention des Exploits** apparaît.
4. Cliquez sur la stratégie que vous désirez modifier. Pour modifier les paramètres de toutes les stratégies, cliquez sur **Tout sélectionner**.
5. Sous **Événement d'Exploits** ou **Application**, cliquez sur **Exclure**.
6. Cliquez sur **OK**.

L'événement de prévention des Exploits ou l'application sera exclu de la prévention des Exploits pour les stratégies sélectionnées.

10 Création de rapports

Les rapports fournissent des informations textuelles et graphiques sur de nombreux aspects de l'état de sécurité de votre réseau.

Les rapports sont disponibles via le **Gestionnaire des rapports**. À l'aide du **Gestionnaire des rapports**, vous pouvez rapidement créer un rapport basé sur un modèle existant, changer la configuration d'un rapport existant et planifier un rapport pour qu'il s'exécute à intervalles réguliers, et avoir les résultats envoyés aux destinataires de votre choix sous la forme d'une pièce jointe à un email. Vous pouvez aussi imprimer des rapports et les exporter dans un certain nombre de formats.

Sophos fournit un certain nombre de rapports prêts à l'emploi ou que vous pouvez configurer selon vos besoins. Ces rapports sont les suivants :

- Historique des alertes et des événements
- Récapitulatif des alertes
- Alertes et événements par nom d'élément
- Alertes et événements par heure
- Alertes et événements par emplacement
- Non conformité à la stratégie des terminaux
- Événements par utilisateur
- Protection des terminaux administrés
- Hiérarchie de mise à jour

Rapports et administration déléguée

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Configuration du rapport** pour créer, modifier ou supprimer un rapport. Si vous ne disposez pas de ce droit, vous pouvez seulement exécuter un rapport. Retrouvez plus de renseignements sur l'administration déléguée à la section Gestion des rôles et des sous-parcs (page 14).

Un rapport peut seulement inclure des données d'un sous-parc actif. Vous ne pouvez pas partager des rapports entre sous-parcs. Les rapports par défaut ne sont pas copiés depuis le sous-parc **par défaut** dans les nouveaux sous-parcs que vous créez.

Lorsque vous supprimez un sous-parc, tous les rapports dans ce sous-parc sont également supprimés.

10.1 Création d'un nouveau rapport

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Configuration du rapport** pour réaliser cette tâche. Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Pour créer un rapport :

1. Cliquez sur l'icône **Rapports** dans la barre d'outils.
2. Dans la boîte de dialogue **Gestionnaire des rapports**, cliquez sur **Créer**.

3. Dans la boîte de dialogue **Création d'un nouveau rapport**, sélectionnez un modèle de rapport et cliquez sur **OK**.

   Un assistant vous guide tout au long de la création du rapport d'après votre modèle choisi.

   Si vous ne voulez pas utiliser l'assistant, dans la boîte de dialogue **Création d'un nouveau rapport**, dessélectionnez la case à cocher **Utiliser l'assistant pour créer le rapport**. Vous pouvez alors configurer votre nouveau rapport dans la boîte de dialogue des propriétés du rapport. Retrouvez plus de renseignements à la section sur la configuration du rapport approprié.

10.2 Configuration du rapport d'historique des alertes et des événements

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Configuration du rapport** pour réaliser cette tâche. Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Le rapport **Historique des alertes et des événements** affiche les alertes et les événements par période de signalement spécifiée.

1. Cliquez sur l'icône **Rapports** dans la barre d'outils.
2. Dans la boîte de dialogue **Gestionnaire des rapports**, sélectionnez **Historique des alertes et des événements** et cliquez sur **Propriétés**.
3. Dans la boîte de dialogue **Propriétés - Historique des alertes et des événements**, sur l'onglet **Configuration**, configurez les options désirées.

   a) Dans le volet **Détails du rapport**, modifiez le nom et la description du rapport, si vous le souhaitez.

   b) Dans la zone de texte **Période du rapport**, dans la zone de texte **Période**, cliquez sur la flèche de déroulement et sélectionnez une période de temps.

      Vous pouvez soit sélectionner une période de temps définie comme par exemple, **Le mois dernier**, soit sélectionner l'option **Personnalisée** et définir votre propre période de temps dans les cases **Début** et **Fin**.

   c) Dans le volet **Emplacement du rapport**, cliquez sur **Groupe d'ordinateurs** ou **Ordinateur individuel**. Puis cliquez sur la flèche de déroulement pour spécifier un nom de groupe ou d'ordinateur.

   d) Dans le volet **Types d'alertes et d'événements à inclure**, sélectionnez des types d'alertes que vous voulez inclure dans le rapport.

      Par défaut, le rapport affiche tous les types d'alertes et d'événements.

      Autrement, vous pouvez configurer le rapport pour qu'il affiche uniquement les emplacements ayant signalé une alerte ou un événement particulier. Pour spécifier une alerte ou un événement particulier, cliquez sur **Avancés** et cliquez sur un nom d'alerte ou d'événement dans la liste. Pour définir plusieurs alertes ou événements, saisissez un nom dans la zone de texte en utilisant des caractères génériques. Utilisez ? pour remplacer un seul caractère du nom et * pour remplacer une chaîne de caractères quelconque. Par exemple, W32/* définit tous les virus dont le nom commence par W32/.
4. Sur l'onglet **Options d'affichage**, sélectionnez la manière dont vous souhaitez trier les alertes et les événements.

   Par défaut, les détails des alertes et des événements sont triés en fonction du **Nom de l'alerte et de l'événement**. Toutefois, les rapports peuvent aussi être triés en fonction du **Nom d'ordinateur**, du **Nom de groupe** de l'ordinateur, ou de la **Date et heure**.
5. Sur l'onglet **Planification**, sélectionnez **Planifier ce rapport** si vous voulez exécuter le rapport à intervalles réguliers, avec les résultats envoyés aux destinataires choisis sous la forme de

pièces jointes à un email. Saisissez les dates de début et de fin ainsi que la fréquence avec laquelle le rapport sera généré, spécifiez le format et la langue de sortie et saisissez les adresses électroniques des destinataires du rapport.

10.3 Configuration du rapport Récapitulatif des alertes

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Configuration du rapport** pour réaliser cette tâche. Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Le rapport **Récapitulatif des alertes** contient des statistiques sur l'état de santé général de votre réseau.

1. Cliquez sur l'icône **Rapports** dans la barre d'outils.
2. Dans la boîte de dialogue **Gestionnaire des rapports**, sélectionnez **Récapitulatif des alertes** et cliquez sur **Propriétés**.
3. Dans la boîte de dialogue **Propriétés - Récapitulatif des alertes**, sur l'onglet **Configuration**, configurez les options désirées.
   a) Dans le volet **Détails du rapport**, modifiez le nom et la description du rapport, si vous le souhaitez.
   b) Dans la zone de texte **Période du rapport**, dans la zone de texte **Période**, cliquez sur la flèche de déroulement et sélectionnez une période de temps.
      Vous pouvez soit sélectionner une période de temps définie comme par exemple, **Le mois dernier**, soit sélectionner l'option **Personnalisée** et définir votre propre période de temps dans les cases **Début** et **Fin**.
4. Sur l'onglet **Options d'affichage**, sous **Afficher les résultats par**, indiquez les intervalles de temps auxquels la non conformité est mesurée, par exemple toutes les heures ou tous les jours, cliquez sur la flèche du menu déroulant et sélectionnez un intervalle.
5. Sur l'onglet **Planification**, sélectionnez **Planifier ce rapport** si vous voulez exécuter le rapport à intervalles réguliers, avec les résultats envoyés aux destinataires choisis sous la forme de pièces jointes à un email. Saisissez les dates de début et de fin ainsi que la fréquence avec laquelle le rapport sera généré, spécifiez le format et la langue de sortie et saisissez les adresses électroniques des destinataires du rapport.

10.4 Configuration du rapport Alertes et événements par nom d'élément

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Configuration du rapport** pour réaliser cette tâche. Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Le rapport **Alertes et événements par nom d'élément** contient des statistiques sur toutes les alertes et tous les événements issus de tous les ordinateurs sur une période sélectionnée, regroupées par nom d'élément.

Pour configurer le rapport :

1. Cliquez sur l'icône **Rapports** dans la barre d'outils.
2. Dans la boîte de dialogue **Gestionnaire des rapports**, sélectionnez **Alertes et événements par nom d'élément** et cliquez sur **Propriétés**.

3. Dans la boîte de dialogue **Propriétés - Alertes et événements par nom d'élément**, sur l'onglet **Configuration**, configurez les options désirées.

   a) Dans le volet **Détails du rapport**, modifiez le nom et la description du rapport, si vous le souhaitez.

   b) Dans la zone de texte **Période du rapport**, dans la zone de texte **Période**, cliquez sur la flèche de déroulement et sélectionnez une période de temps.

   Vous pouvez soit sélectionner une période de temps définie comme par exemple, **Le mois dernier**, soit sélectionner l'option **Personnalisée** et définir votre propre période de temps dans les cases **Début** et **Fin**.

   c) Dans le volet **Emplacement du rapport**, cliquez sur **Groupe d'ordinateurs** ou **Ordinateur individuel**. Puis cliquez sur la flèche de déroulement pour spécifier un nom de groupe ou d'ordinateur.

   d) Dans le volet **Types d'alertes et d'événements à inclure**, sélectionnez des types d'alertes que vous voulez inclure dans le rapport.

   Par défaut, le rapport affiche tous les types d'alertes et d'événements.

4. Sur l'onglet **Options d'affichage**, sous **Affichage**, choisissez quels alertes et événements vous souhaitez voir apparaître dans le rapport.

   Par défaut, le rapport affiche toutes les alertes et tous les événements ainsi que le nombre d'occurrences pour chacun d'entre eux.

   Vous pouvez aussi configurer le rapport pour qu'il indique uniquement :

   - les *n* premières alertes et événements (où *n* est un nombre que vous définissez), ou
   - les alertes et les événements avec *m* occurrences ou plus (où *m* est un nombre que vous définissez).

5. Sous **Trier par**, sélectionnez si vous voulez trier les alertes et les événements par leur numéro ou par leur nom.

   Par défaut, le rapport répertorie les alertes et les événements dans l'ordre décroissant du nombre d'occurrences.

6. Sur l'onglet **Planification**, sélectionnez **Planifier ce rapport** si vous voulez exécuter le rapport à intervalles réguliers, avec les résultats envoyés aux destinataires choisis sous la forme de pièces jointes à un email. Saisissez les dates de début et de fin ainsi que la fréquence avec laquelle le rapport sera généré, spécifiez le format et la langue de sortie et saisissez les adresses électroniques des destinataires du rapport.

10.5 Configuration du rapport Alertes et événements par heure

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Configuration du rapport** pour réaliser cette tâche. Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Le rapport **Alertes et événements par heure** affiche les alertes et les événements récapitulés à des intervalles donnés.

1. Cliquez sur l'icône **Rapports** dans la barre d'outils.
2. Dans la boîte de dialogue **Gestionnaire des rapports**, sélectionnez **Alertes et événements par heure** et cliquez sur **Propriétés**.
3. Dans la boîte de dialogue **Propriétés - Alertes et événements par heure**, sur l'onglet **Configuration**, configurez les options désirées.

a) Dans le volet **Détails du rapport**, modifiez le nom et la description du rapport, si vous le souhaitez.

b) Dans la zone de texte **Période du rapport**, dans la zone de texte **Période**, cliquez sur la flèche de déroulement et sélectionnez une période de temps.

Vous pouvez soit sélectionner une période de temps définie comme par exemple, **Le mois dernier**, soit sélectionner l'option **Personnalisée** et définir votre propre période de temps dans les cases **Début** et **Fin**.

c) Dans le volet **Emplacement du rapport**, cliquez sur **Groupe d'ordinateurs** ou **Ordinateur individuel**. Puis cliquez sur la flèche de déroulement pour spécifier un nom de groupe ou d'ordinateur.

d) Dans le volet **Types d'alertes et d'événements à inclure**, sélectionnez des types d'alertes que vous voulez inclure dans le rapport.

Par défaut, le rapport affiche tous les types d'alertes et d'événements.

Autrement, vous pouvez configurer le rapport pour qu'il affiche uniquement les emplacements ayant signalé une alerte ou un événement particulier. Pour spécifier une alerte ou un événement particulier, cliquez sur **Avancés** et cliquez sur un nom d'alerte ou d'événement dans la liste. Pour définir plusieurs alertes ou événements, saisissez un nom dans la zone de texte en utilisant des caractères génériques. Utilisez ? pour remplacer un seul caractère du nom et * pour remplacer une chaîne de caractères quelconque. Par exemple, W32/* définit tous les virus dont le nom commence par W32/.

4. Sur l'onglet **Options d'affichage**, spécifiez les intervalles de temps auxquels la fréquence des alertes et des événements doit être calculée, par exemple toutes les heures ou tous les jours, cliquez sur la flèche du menu déroulant et sélectionnez un intervalle.
5. Sur l'onglet **Planification**, sélectionnez **Planifier ce rapport** si vous voulez exécuter le rapport à intervalles réguliers, avec les résultats envoyés aux destinataires choisis sous la forme de pièces jointes à un email. Saisissez les dates de début et de fin ainsi que la fréquence avec laquelle le rapport sera généré, spécifiez le format et la langue de sortie et saisissez les adresses électroniques des destinataires du rapport.

10.6 Configuration du rapport Alertes et événements par emplacement

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Configuration du rapport** pour réaliser cette tâche. Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Le rapport **Alertes et événements par emplacement** contient des statistiques sur toutes les alertes issues de tous les ordinateurs sur une période sélectionnée, regroupées par emplacement.

1. Cliquez sur l'icône **Rapports** dans la barre d'outils.
2. Dans la boîte de dialogue **Gestionnaire des rapports**, sélectionnez **Alertes et événements par emplacement** et cliquez sur **Propriétés**.
3. Dans la boîte de dialogue **Propriétés - Alertes et événements par emplacement**, sur l'onglet **Configuration**, configurez les options désirées.

a) Dans le volet **Détails du rapport**, modifiez le nom et la description du rapport, si vous le souhaitez.

b) Dans la zone de texte **Période du rapport**, dans la zone de texte **Période**, cliquez sur la flèche de déroulement et sélectionnez une période de temps.

Vous pouvez soit sélectionner une période de temps définie comme par exemple, **Le mois dernier**, soit sélectionner l'option **Personnalisée** et définir votre propre période de temps dans les cases **Début** et **Fin**.

c) Dans le volet **Emplacement du rapport**, cliquez sur **Ordinateurs** pour afficher les alertes par ordinateur ou sur **Groupe** pour afficher les alertes pour chaque groupe d'ordinateurs.

d) Dans le volet **Types d'alertes et d'événements à inclure**, sélectionnez des types d'alertes que vous voulez inclure dans le rapport.

Par défaut, le rapport affiche tous les types d'alertes et d'événements.

Autrement, vous pouvez configurer le rapport pour qu'il affiche uniquement les emplacements ayant signalé une alerte ou un événement particulier. Pour spécifier une alerte ou un événement particulier, cliquez sur **Avancés** et cliquez sur un nom d'alerte ou d'événement dans la liste. Pour définir plusieurs alertes ou événements, saisissez un nom dans la zone de texte en utilisant des caractères génériques. Utilisez ? pour remplacer un seul caractère du nom et * pour remplacer une chaîne de caractères quelconque. Par exemple, W32/* définit tous les virus dont le nom commence par W32/.

4. Sur l'onglet **Options d'affichage**, sous **Affichage**, choisissez quels emplacements vous voulez que le rapport affiche.

   Par défaut, le rapport affiche tous les ordinateurs et groupes ainsi que le nombre d'occurrences pour chacun d'entre eux. Vous pouvez le configurer pour qu'il affiche uniquement :

   - les *n* premiers emplacements qui ont enregistré le plus d'alertes et d'événements (ou *n* est un nombre que vous définissez), ou
   - les emplacements avec *m* alertes et événements ou plus (où *m* est un nombre que vous définissez).

5. Sous **Trier par**, sélectionnez si vous voulez trier les emplacements par le nombre d'éléments détectés ou par leur nom.

   Par défaut, le rapport répertorie les emplacements dans l'ordre décroissant du nombre d'alertes et d'événements par emplacement. Sélectionnez **Emplacement** si vous souhaitez qu'ils soient classés par nom dans l'ordre alphabétique.

6. Sur l'onglet **Planification**, sélectionnez **Planifier ce rapport** si vous voulez exécuter le rapport à intervalles réguliers, avec les résultats envoyés aux destinataires choisis sous la forme de pièces jointes à un email. Saisissez les dates de début et de fin ainsi que la fréquence avec laquelle le rapport sera généré, spécifiez le format et la langue de sortie et saisissez les adresses électroniques des destinataires du rapport.

10.7 Configuration du rapport de non conformité des terminaux à la stratégie

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Configuration du rapport** pour réaliser cette tâche. Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Le rapport **Non conformité des terminaux à la stratégie** affiche le pourcentage ou le nombre d'ordinateurs qui ne sont pas en conformité avec la stratégie de leur groupe, récapitulé à des intervalles donnés.

1. Cliquez sur l'icône **Rapports** dans la barre d'outils.
2. Dans la boîte de dialogue **Gestionnaire des rapports**, sélectionnez **Non conformité des terminaux à la stratégie** et cliquez sur **Propriétés**.
3. Dans la boîte de dialogue **Propriétés - Non conformité des terminaux à la stratégie**, sur l'onglet **Configuration**, configurez les options désirées.

a) Dans le volet **Détails du rapport**, modifiez le nom et la description du rapport, si vous le souhaitez.

b) Dans la zone de texte **Période du rapport**, dans la zone de texte **Période**, cliquez sur la flèche de déroulement et sélectionnez une période de temps.

Vous pouvez soit sélectionner une période de temps définie comme par exemple, **Le mois dernier**, soit sélectionner l'option **Personnalisée** et définir votre propre période de temps dans les cases **Début** et **Fin**.

c) Dans le volet **Affichage**, sélectionnez les stratégies que vous voulez afficher dans le rapport. Par défaut, seule la stratégie **antivirus et HIPS** est sélectionnée.

4. Sur l'onglet **Options d'affichage**, sous **Afficher les résultats par**, indiquez les intervalles de temps auxquels la non conformité est mesurée, par exemple toutes les heures ou tous les jours, cliquez sur la flèche du menu déroulant et sélectionnez un intervalle.
5. Sous **Afficher les résultats sous la forme de**, sélectionnez si vous voulez afficher les résultats sous la forme de pourcentages ou de nombres.
6. Sur l'onglet **Planification**, sélectionnez **Planifier ce rapport** si vous voulez exécuter le rapport à intervalles réguliers, avec les résultats envoyés aux destinataires choisis sous la forme de pièces jointes à un email. Saisissez les dates de début et de fin ainsi que la fréquence avec laquelle le rapport sera généré, spécifiez le format et la langue de sortie et saisissez les adresses électroniques des destinataires du rapport.

10.8 Configuration du rapport Événements par utilisateur

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Configuration du rapport** pour réaliser cette tâche. Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Le rapport **Événements par utilisateur** affiche les événements de contrôle des applications, de pare-feu, de contrôle des données et de contrôle des périphériques et regroupe également les événements Web par utilisateur.

1. Cliquez sur l'icône **Rapports** dans la barre d'outils.
2. Dans la boîte de dialogue **Gestionnaire des rapports**, sélectionnez **Événements par utilisateur** et cliquez sur **Propriétés**.
3. Dans la boîte de dialogue **Propriétés - Événements par utilisateur**, sur l'onglet **Configuration**, configurez les options désirées.

a) Dans le volet **Détails du rapport**, modifiez le nom et la description du rapport, si vous le souhaitez.

b) Dans la zone de texte **Période du rapport**, dans la zone de texte **Période**, cliquez sur la flèche de déroulement et sélectionnez une période de temps.

Vous pouvez soit sélectionner une période de temps définie comme par exemple, **Le mois dernier**, soit sélectionner l'option **Personnalisée** et définir votre propre période de temps dans les cases **Début** et **Fin**.

c) Sous **Types d'événements à inclure**, sélectionnez les fonctionnalités pour lesquelles vous voulez afficher les événements.

4. Sur l'onglet **Options d'affichage**, sous **Affichage**, choisissez quels utilisateurs vous voulez que le rapport affiche.

Par défaut, le rapport affiche tous les utilisateurs ainsi que le nombre d'événements pour chacune d'entre elles. Vous pouvez le configurer pour qu'il affiche uniquement :

- les *n* premiers utilisateurs qui ont enregistré le plus d'événements (ou *n* est un nombre que vous définissez), ou
- les utilisateurs avec *m* événements ou plus (où *m* est un nombre que vous définissez).

5. Sous **Trier par**, sélectionnez si vous voulez trier les utilisateurs par le nombre d'événements ou par leur nom.

   Par défaut, le rapport répertorie les utilisateurs dans l'ordre décroissant du nombre d'événements par utilisateur. Sélectionnez **Utilisateur** si vous souhaitez qu'ils soient classés par nom dans l'ordre alphabétique.
6. Sur l'onglet **Planification**, sélectionnez **Planifier ce rapport** si vous voulez exécuter le rapport à intervalles réguliers, avec les résultats envoyés aux destinataires choisis sous la forme de pièces jointes à un email. Saisissez les dates de début et de fin ainsi que la fréquence avec laquelle le rapport sera généré, spécifiez le format et la langue de sortie et saisissez les adresses électroniques des destinataires du rapport.

10.9 Configuration du rapport Protection des terminaux administrés

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Configuration du rapport** pour réaliser cette tâche. Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Le rapport **Protection des terminaux administrés** indique le pourcentage ou le nombre d'ordinateurs protégés, récapitulés à des intervalles donnés.

1. Cliquez sur l'icône **Rapports** dans la barre d'outils.
2. Dans la boîte de dialogue **Gestionnaire des rapports**, sélectionnez **Protection des terminaux administrés** et cliquez sur **Propriétés**.
3. Dans la boîte de dialogue **Propriétés - Protection des terminaux administrés**, sur l'onglet **Configuration**, configurez les options désirées.

   a) Dans le volet **Identité du rapport**, modifiez le nom et la description du rapport, si vous le souhaitez.

   b) Dans la zone de texte **Période du rapport**, dans la zone de texte **Période**, cliquez sur la flèche de déroulement et sélectionnez une période de temps.

      Vous pouvez soit sélectionner une période de temps définie comme par exemple, **Le mois dernier**, soit sélectionner l'option **Personnalisée** et définir votre propre période de temps dans les cases **Début** et **Fin**.

   c) Dans le volet **Affichage**, sélectionnez les fonctions que vous voulez afficher dans le rapport.
4. Sur l'onglet **Options d'affichage**, sous **Afficher les résultats par**, indiquez les intervalles de temps auxquels la non conformité est mesurée, par exemple toutes les heures ou tous les jours, cliquez sur la flèche du menu déroulant et sélectionnez un intervalle.
5. Sous **Afficher les résultats sous la forme de**, sélectionnez si vous voulez afficher les résultats sous la forme de pourcentages ou de nombres.
6. Sur l'onglet **Planification**, sélectionnez **Planifier ce rapport** si vous voulez exécuter le rapport à intervalles réguliers, avec les résultats envoyés aux destinataires choisis sous la forme de pièces jointes à un email. Saisissez les dates de début et de fin ainsi que la fréquence avec laquelle le rapport sera généré, spécifiez le format et la langue de sortie et saisissez les adresses électroniques des destinataires du rapport.

10.10 Rapport Hiérarchie des mises à jour

Le rapport **Hiérarchie des mises à jour** affiche les gestionnaires de mise à jour sur votre réseau, les partages de mise à jour qu'ils gèrent et le nombre d'ordinateurs qui se mettent à jour depuis ces partages.

Vous ne pouvez pas configurer le rapport **Hiérarchie des mises à jour**. Vous pouvez exécuter le rapport comme indiqué à la section Exécution d'un rapport (page 220).

10.11 Planification d'un rapport

Si vous utilisez l'administration déléguée, vous devez disposer du droit **Configuration du rapport** pour réaliser cette tâche. Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Vous pouvez planifier un rapport à exécuter à des intervalles réguliers, avec envoi des résultats aux destinataires de votre choix sous la forme de pièces jointes à un email.

1. Cliquez sur l'icône **Rapports** dans la barre d'outils.
2. Dans la boîte de dialogue **Gestionnaire des rapports**, sélectionnez le rapport que vous voulez planifier et cliquez sur **Planifier**.
3. Dans la boîte de dialogue qui apparaît, sur l'onglet **Planification**, sélectionnez **Planifier ce rapport**.
4. Saisissez la date de début et de fin ainsi que la fréquence avec laquelle le rapport sera généré.
5. Spécifiez le format et la langue du fichier de sortie.
6. Saisissez les adresses électroniques des destinataires du rapport.

10.12 Exécution d'un rapport

1. Cliquez sur l'icône **Rapports** dans la barre d'outils.
2. Dans la boîte de dialogue **Gestionnaire des rapports**, sélectionnez le rapport que vous voulez exécuter et cliquez sur **Exécuter**.
   La fenêtre **Édition de rapports**, affichant le rapport, apparaît.

Vous pouvez changer la mise en page du rapport, l'imprimer ou l'exporter dans un fichier.

10.13 Affichage d'un rapport sous forme de tableau ou de diagramme

Certains rapports peuvent être affichés sous la forme d'un tableau et d'un diagramme. Si c'est le cas, deux onglets apparaissent, **Tableau** et **Diagramme** dans la fenêtre **Édition de rapports** affichant le rapport.

1. Cliquez sur l'icône **Rapports** dans la barre d'outils.
2. Dans la boîte de dialogue **Gestionnaire des rapports**, sélectionnez le rapport que vous voulez exécuter, par exemple, **Alertes et événements par emplacement**, et cliquez sur **Exécuter**.
   La fenêtre **Édition de rapports**, affichant le rapport, apparaît.

3. Pour voir le rapport sous la forme d'un tableau ou d'un diagramme, allez sur l'onglet approprié.

10.14 Impression d'un rapport

Pour imprimer un rapport, cliquez sur l'icône **Imprimer** de la barre d'outils en haut du rapport.

10.15 Exportation d'un rapport dans un fichier

Pour exporter un rapport dans un fichier :

1. Cliquez sur l'icône **Exporter** de la barre d'outils en haut du rapport.

2. Dans la boîte de dialogue **Exportation du rapport**, sélectionnez le type de document ou de feuille de calcul vers lequel vous souhaitez exporter le rapport.

   Les options sont :

   - PDF (Acrobat)
   - HTML
   - Microsoft Excel
   - Microsoft Word
   - Format texte enrichi (RTF)
   - Valeurs séparées par des virgules (CSV)
   - XML

3. Cliquez sur le bouton de navigation **Nom du fichier** pour sélectionner un emplacement. Puis saisissez un nom. Cliquez sur **OK**.

10.16 Modification de la mise en page du rapport

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

1. Cliquez sur l'icône de mise en page de la barre d'outils en haut du rapport.

2. Dans la boîte de dialogue **Mise en page**, définissez la taille, l'orientation et les marges de la page. Cliquez sur **OK**.
   Le rapport s'affichera ensuite avec ces paramètres de mise en page.

Ces paramètres de mise en page seront aussi utilisés lorsque vous imprimerez ou exporterez le rapport.

11 Audit

L'audit vous permet de surveiller les changements apportés dans la configuration de l'Enterprise Console et d'autres actions de l'utilisateur ou du système. Vous pouvez utiliser ces informations afin de rester en conformité aux normes réglementaires et afin de résoudre les problèmes. Vous pouvez également vous en servir pour étayer une analyse juridique en cas d'activité malveillante.

Par défaut, l'audit est désactivé. Après avoir activé l'audit, une entrée d'audit est écrite dans la base de données d'audit chaque fois que certains paramètres de configuration sont changés ou que certaines actions sont exécutées.

Remarque
Si vous utilisez l'administration déléguée, vous devez disposer du droit **Audit** pour activer ou désactiver l'audit. Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

L'entrée d'audit inclut les informations suivantes :

- Action effectuée
- Utilisateur qui a effectué l'action
- Ordinateur de l'utilisateur
- Sous-parc de l'utilisateur
- Date et heure de l'action

Toutes les tentatives réussies ou ratées d'effectuer des actions sont soumises à un audit. Par conséquent, les entrées d'audit peuvent afficher les actions effectuées sur le système et l'identité de l'utilisateur qui a lancé les actions qui ont échoué.

Les actions auditées incluent :

Catégorie	Actions
Actions de l'ordinateur	Approuver/résoudre les alertes et les erreurs, protéger un ordinateur, mettre à jour un ordinateur, supprimer un ordinateur, exécuter le contrôle intégral du système d'un ordinateur
Gestion de groupes d'ordinateurs	Créer un groupe, supprimer un groupe, déplacer un groupe, renommer un groupe, affecter un ordinateur à un groupe
Gestion des stratégies	Créer une stratégie, renommer une stratégie, dupliquer une stratégie, modifier une stratégie, affecter une stratégie à un ordinateur, réinitialiser une stratégie aux valeurs par défaut usine, supprimer une stratégie
Gestion des rôles	Créer un rôle, supprimer un rôle, renommer un rôle, dupliquer un rôle, ajouter un utilisateur à un rôle, retirer un utilisateur d'un rôle, ajouter un droit à un rôle, retirer un droit d'un rôle

Catégorie	Actions
Gestion des gestionnaires de mise à jour	Mettre à jour un gestionnaire de mise à jour, demander à un gestionnaire de mise à jour de se mettre en conformité avec la configuration, approuver les alertes, supprimer un gestionnaire de mise à jour, configurer un gestionnaire de mise à jour, ajouter un nouvel abonnement logiciels, supprimer un abonnement logiciels, renommer un abonnement logiciels, modifier un abonnement logiciels, dupliquer un abonnement logiciels
Événements système	Activer l'audit, désactiver l'audit

Vous pouvez utiliser des programmes tiers tels que Microsoft Excel, Microsoft Access, Microsoft SQL Server Reporting Services ou Crystal Reports pour accéder et analyser les données stockées dans la base de données d'audit. Retrouvez plus de renseignements sur la consultation des entrées d'audit dans le *Guide de l'utilisateur de la fonction d'audit de Sophos Enterprise Console*.

11.1 Activation ou désactivation de l'audit

Si vous utilisez l'administration déléguée, vous devez disposer du droit d'**Audit** pour pouvoir activer ou désactiver l'audit. Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Pour activer ou désactiver l'audit :

1. Dans le menu **Outils**, cliquez sur **Gérer l'audit**.
2. Dans la boîte de dialogue **Gestion de l'audit**, sélectionnez ou dessélectionnez la case à cocher **Activer l'audit** pour activer ou désactiver l'audit. Cette option est par défaut désactivée.

12 Copie ou impression des données depuis l'Enterprise Console

12.1 Copie de données depuis la liste des ordinateurs

Dans la vue **Terminaux**, vous pouvez copier les informations affichées dans la liste des ordinateurs dans le Presse-papiers, puis les coller dans un autre document dans un format séparé par des tabulations.

1. Dans la vue **Terminaux**, dans le volet **Groupes**, sélectionnez le groupe d'ordinateurs pour lesquels vous voulez copier les données.
2. Dans la liste déroulante **Vue**, sélectionnez les ordinateurs que vous souhaitez afficher, par exemple, les **Ordinateurs avec des problèmes éventuels**.
3. Si le groupe contient des sous-groupes, sélectionnez également si vous souhaitez afficher les ordinateurs **A ce niveau seulement** ou **À ce niveau et au-dessous**.
4. Dans la liste des ordinateurs, allez dans l'onglet que vous voulez afficher, par exemple, **Détails de l'antivirus**.
5. Cliquez n'importe où dans la liste des ordinateurs pour vous y concentrer.
6. Dans le menu **Édition**, cliquez sur **Copier** pour copier les données dans le Presse-papiers.

12.2 Impression de données depuis la liste des ordinateurs

Vous pouvez imprimer des informations affichées dans la liste des ordinateurs, dans la vue **Terminaux**.

1. Dans la vue **Terminaux**, dans le volet **Groupes**, sélectionnez le groupe d'ordinateurs pour lesquels vous voulez imprimer les données.
2. Dans la liste déroulante **Vue**, sélectionnez les ordinateurs que vous souhaitez afficher, par exemple, les **Ordinateurs avec des problèmes éventuels**.
3. Si le groupe contient des sous-groupes, sélectionnez également si vous souhaitez afficher les ordinateurs **A ce niveau seulement** ou **À ce niveau et au-dessous**.
4. Dans la liste des ordinateurs, allez dans l'onglet que vous voulez afficher, par exemple, **Détails de l'antivirus**.
5. Cliquez n'importe où dans la liste des ordinateurs pour vous y concentrer.
6. Dans le menu **Fichier**, cliquez sur **Imprimer**.

12.3 Copie des détails d'un ordinateur

Vous pouvez copier des informations depuis la boîte de dialogue **Détails de l'ordinateur** dans le Presse-papiers, puis les coller dans un autre document. Les informations incluent le nom de

l’ordinateur, le système d’exploitation, les versions du logiciel de sécurité installé, toutes les alertes et les erreurs à traiter, le statut de mise à jour, et ainsi de suite.

1. Dans la vue **Terminaux**, dans la liste des ordinateurs, cliquez deux fois sur l’ordinateur dont vous voulez copier les données.
2. Dans la boîte de dialogue **Détails de l’ordinateur**, cliquez sur **Copier** pour copier les données dans le Presse-papiers.

12.4 Impression des détails d’un ordinateur

Vous pouvez imprimer les informations depuis la boîte de dialogue **Détails de l’ordinateur**. Les informations incluent le nom de l’ordinateur, le système d’exploitation, les versions du logiciel de sécurité installé, toutes les alertes et les erreurs à traiter, le statut de mise à jour, et ainsi de suite.

1. Dans la vue **Terminaux**, dans la liste des ordinateurs, cliquez deux fois sur l’ordinateur dont vous voulez imprimer les données.
2. Dans la boîte de dialogue **Détails de l’ordinateur**, cliquez sur **Imprimer**.

13 Résolution des problèmes

Lorsque vous exécutez l'Assistant de protection des ordinateurs, l'installation du logiciel de sécurité peut échouer pour un certain nombre de raisons :

- L'installation automatique est impossible sur ce système d'exploitation. Effectuez une installation manuelle. Retrouvez plus de renseignements sur les autres systèmes d'exploitation (si leur protection est incluse dans votre licence) dans le Guide de démarrage de pour Linux et UNIX.
- Le système d'exploitation n'a pas pu être déterminé. Vous n'avez peut-être pas saisi votre nom d'utilisateur au format domaine\nomutilisateur lors de la recherche des ordinateurs.
- Les règles de pare-feu bloquent l'accès nécessaire au déploiement du logiciel de sécurité.

13.1 Les ordinateurs n'utilisent pas le contrôle sur accès

Si vous avez des ordinateurs sur lesquels le contrôle sur accès ne fonctionne pas :

1. Vérifiez quelle stratégie antivirus et HIPS est utilisée par ces ordinateurs.

   Retrouvez plus de renseignements à la section Vérification des stratégies utilisées par un groupe (page 27).
2. Assurez-vous que le contrôle sur accès est activé dans cette stratégie et que les ordinateurs sont conformes à la stratégie.

   Retrouvez plus de renseignements aux sections Activation ou désactivation du contrôle sur accès (page 85) et Application de la stratégie de groupe par les ordinateurs (page 34).

13.2 Le pare-feu est désactivé

S'il existe des ordinateurs dont le pare-feu est désactivé :

1. Vérifiez quelle stratégie de pare-feu est utilisée par ces ordinateurs.

   Retrouvez plus de renseignements à la section Vérification des stratégies utilisées par un groupe (page 27).
2. Assurez-vous que le pare-feu est activé dans cette stratégie et que les ordinateurs sont conformes à la stratégie.

   Retrouvez plus de renseignements aux sections Désactivation temporaire du pare-feu (page 122) et Application de la stratégie de groupe par les ordinateurs (page 34).

13.3 Le pare-feu n'est pas installé

Remarque
Si vous utilisez l'administration déléguée, vous devez disposer du droit **Recherche d'ordinateurs, protection et groupes** pour installer le pare-feu. Retrouvez plus de renseignements à la section Gestion des rôles et des sous-parcs (page 14).

Avant de tenter d'installer le pare-feu client sur les terminaux, vérifiez que les ordinateurs exécutent un système d'exploitation client Windows.

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

S'il y a des ordinateurs sur lesquels vous voulez installer le pare-feu :

1. Sélectionnez ces ordinateurs, cliquez dessus avec le bouton droit de la souris et sélectionnez **Protéger les ordinateurs**.

   L'**Assistant de protection des ordinateurs** apparaît. Cliquez sur **Suivant**.
2. Lorsque vous êtes invité à sélectionner des fonctionnalités, sélectionnez **Pare-feu**. Fermez l'assistant.

Si le problème persiste, veuillez contacter le support technique de Sophos.

13.4 Ordinateurs avec des alertes à traiter

- Retrouvez plus de renseignements sur la marche à suivre en cas de présence d'un virus ou d'une application indésirable sur vos ordinateurs à la section Nettoyage immédiat des ordinateurs (page 55).
- En cas de présence *souhaitée* d'un adware ou de toute autre application potentiellement indésirable sur vos ordinateurs, veuillez consulter la section Autorisation des adwares et des PUA (page 111).
- Si des ordinateurs sont non mis à jour, veuillez consulter la section Mise à jour des ordinateurs non à jour (page 80) pour obtenir de l'aide sur le diagnostic et le correction du problème.

Remarque
Si l'affichage de l'alerte n'est plus nécessaire, vous pouvez l'effacer. Sélectionnez le ou les ordinateurs affichant des alertes, cliquez dessus avec le bouton droit de la souris et sélectionnez **Résoudre les alertes et les erreurs**. Vous devez disposer du droit **Actualisation - nettoyage** pour approuver (effacer) les alertes et les erreurs.

13.5 Les ordinateurs ne sont pas administrés par la console

Les ordinateurs Windows Mac, Linux et UNIX doivent être administrés par l'Enterprise Console afin de pouvoir être mis à jour et sous surveillance.

Remarque
Si vous n'utilisez pas la synchronisation Active Directory (section Gestion des rôles et des sous-parcs (page 14)), les nouveaux ordinateurs ajoutés au réseau ne s'affichent pas ou ne sont pas administrés automatiquement par la console. Cliquez sur **Détecter des ordinateurs** dans la barre d'outils pour les rechercher et les placer dans le groupe **Non assigné**.

Si un ordinateur n'est pas administré, les détails le concernant sur l'onglet **État** sont grisés.

Pour lancer l'administration des ordinateurs non administrés :

1. Dans la liste déroulante **Vue**, sélectionnez **Ordinateurs non administrés**.
2. Procédez de l'une des manières suivantes :
   - Si les ordinateurs non administrés sont dans le groupe **Non assigné**, sélectionnez les ordinateurs et faites-les glisser sur le groupe dans lequel vous voulez les mettre. L'**Assistant de protection des ordinateurs** s'ouvre pour vous aider à les protéger.
   - Si ces ordinateurs sont déjà dans un groupe, sélectionnez-les puis cliquez sur le bouton droit de la souris et sélectionnez **Protéger les ordinateurs** pour installer une version administrée de Sophos Endpoint Security and Control.
3. Si l'Enterprise Console échoue dans sa tentative d'installer Sophos Endpoint Security and Control automatiquement sur certains ordinateurs, procédez à une installation manuelle.

   L'installation automatique à l'aide de l'**Assistant de protection des ordinateurs** est uniquement disponible pour les ordinateurs Windows. Si vous devez protéger des ordinateurs Mac, Linux ou UNIX, veuillez installer le logiciel manuellement.

   Retrouvez plus de renseignements sur la protection manuelle des ordinateurs Mac ou Windows dans le *Guide de démarrage avancé de Sophos Enterprise Console.*

   Retrouvez plus de renseignements sur la protection des ordinateurs Linux ou UNIX dans le *Guide de démarrage de Sophos Enterprise Console pour Linux et UNIX*.

13.6 Impossible de protéger les ordinateurs du groupe Non assigné

Le groupe **Non assigné** sert seulement à conserver les ordinateurs qui ne sont pas encore dans des groupes que vous avez créés et auxquels des stratégies peuvent être appliquées. Vous ne pouvez pas protéger les ordinateurs tant que vous ne les avez pas placés dans un groupe.

13.7 Échec d'installation de Sophos Endpoint Security and Control

Si l'**Assistant de protection des ordinateurs** ne parvient pas à installer Sophos Endpoint Security and Control sur les ordinateurs, c'est probablement parce que :

- L'Enterprise Console ne reconnaît pas le système d'exploitation exécuté par les ordinateurs. Ceci est probablement dû au fait que vous n'avez pas saisi votre nom utilisateur au format domaine \utilisateur lors de la recherche d'ordinateurs.
- L'installation automatique est impossible sur ce système d'exploitation. Effectuez une installation manuelle. Retrouvez plus d'instructions dans le *Guide de démarrage avancé de Sophos Enterprise Console*.
- Les ordinateurs exécutent un pare-feu.
- Le « Partage de fichiers simple » n'a pas été désactivé sur les ordinateurs Windows XP.
- L'option « Utiliser l'Assistant Partage » n'a pas été désactivée sur les ordinateurs Windows Vista.
- Vous avez choisi d'installer une fonction qui n'est pas prise en charge par les systèmes d'exploitation des ordinateurs.

Retrouvez une liste complète des configurations requises pour les fonctions de Sophos Endpoint Security and Control sur la page des configurations requises sur le site Web de Sophos (http://www.sophos.com/fr-fr/products/all-system-requirements).

13.8 Les ordinateurs ne sont pas mis à jour

Retrouvez plus de renseignements à la section Mise à jour des ordinateurs non à jour (page 80) pour obtenir de l'aide sur le diagnostic et la correction du problème.

13.9 Les paramètres antivirus ne s'appliquent pas sur Macintosh

Certains paramètres antivirus ne peuvent s'appliquer aux ordinateurs Mac. Dans ce cas, un avertissement apparaît sur cette page de paramètres.

Retrouvez plus de renseignements sur les paramètres de la stratégie antivirus et HIPS s'appliquant aux ordinateurs Mac dans l'article 118859 de la base de connaissances Sophos.

13.10 Les paramètres antivirus ne s'appliquent pas sur Linux ou UNIX

Certains paramètres antivirus ne s'appliquent pas aux ordinateurs Linux ou UNIX. Dans ce cas, un avertissement apparaît sur cette page de paramètres.

Vous pouvez modifier les paramètres antivirus des ordinateurs Linux à l'aide des commandes `savconfig` et `savscan` comme le décrit le *Guide de configuration de Sophos Anti-Virus pour Linux*.

Vous pouvez modifier les paramètres antivirus des ordinateurs UNIX à l'aide de la commande `savscan` comme le décrit le *Guide de configuration de Sophos Anti-Virus pour UNIX*.

13.11 L'ordinateur Linux ou UNIX n'est pas en conformité avec la stratégie

Si vous utilisez un fichier de configuration d'entreprise dans le CID, et si le fichier contient une valeur de configuration en conflit avec la stratégie, l'ordinateur apparaît comme non conforme avec la stratégie.

La sélection de l'option **Appliquer la stratégie** met l'ordinateur en conformité seulement temporairement, jusqu'à ce que la configuration de type CID soit réappliquée.

Pour résoudre le problème, parcourez le fichier de configuration d'entreprise et, le cas échéant, remplacez-le par une configuration basée sur la console.

13.12 Apparition inattendue d'un nouveau contrôle sur un ordinateur Windows

Si vous regardez la copie locale de Sophos Endpoint Security and Control sur les ordinateurs Windows, vous remarquerez qu'un nouveau « Contrôle disponible » est répertorié alors que l'utilisateur n'en a pas créé.

Ce nouveau contrôle est en fait un contrôle planifié que vous avez configuré depuis la console. Ne le supprimez pas.

13.13 Problèmes de connectivité et de délai

Si les communications entre l'Enterprise Console et un ordinateur en réseau sont lentes ou si l'ordinateur ne répond pas, il se peut qu'il y ait un problème de connectivité.

Vérifiez le rapport sur les communications réseau Sophos qui présente un aperçu de l'état actuel des communications entre un ordinateur et l'Enterprise Console. Pour voir le rapport, rendez-vous sur l'ordinateur concerné par le problème. Sur la barre des tâches, cliquez sur le bouton **Démarrer**, sélectionnez **Tous les programmes > Sophos > Sophos Endpoint Security and Control** et cliquez sur **Voir le rapport sur les communications réseau Sophos**.

Le rapport indique les zones à problèmes éventuelles et, en cas de détection d'un problème, les actions à prendre pour y remédier.

13.14 Les adwares et les PUA ne sont pas détectés

Si des adwares et autres applications potentiellement indésirables (PUA) ne sont pas détectés, assurez-vous que :

- La détection a été activée. Retrouvez plus de renseignements à la section Configuration du contrôle sur accès (page 83).
- Les applications sont sur un ordinateur exécutant Windows.

13.15 Élément partiellement détecté

Sophos Endpoint Security and Control peut signaler qu'un élément (par exemple, un cheval de Troie ou une application potentiellement indésirable) est « partiellement détecté ». Ceci signifie qu'il n'a pas trouvé tous les composants de cette application.

Pour trouver d'autres composants, il est nécessaire que vous lanciez un contrôle intégral du système du ou des ordinateurs affectés. Sur les ordinateurs exécutant Windows, vous pouvez exécuter cette opération en sélectionnant le ou les ordinateurs, en cliquant avec le bouton droit de la souris et en sélectionnant **Contrôle intégral du système**. Vous pouvez aussi configurer un contrôle planifié à la recherche d'adwares et d'autres applications potentiellement indésirables. Retrouvez plus de renseignements aux sections Configuration du contrôle sur accès (page 83) et Création d'un contrôle planifié (page 90).

Si l'application n'a toujours pas été intégralement détectée, c'est peut-être parce que :

- Vos droits d'accès sont insuffisants
- Certains lecteurs ou dossiers de l'ordinateur, contenant les composants de l'application, sont exclus du contrôle.

S'il s'agit du dernier cas, vérifiez la liste des éléments exclus du contrôle (section Exclusion d'éléments du contrôle sur accès (page 88)). Si certains éléments figurent dans la liste, supprimez-les de la liste et lancez un nouveau contrôle de l'ordinateur.

Il se peut que Sophos Endpoint Security and Control ne soit pas en mesure de détecter intégralement ou de supprimer les adwares et les applications potentiellement indésirables dont les composants sont installés sur des lecteurs réseau.

Pour plus de conseils, contactez le support technique Sophos.

13.16 Fréquentes alertes concernant les applications potentiellement indésirables

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

Ceci peut survenir parce que certains types d'application potentiellement indésirable « surveillent » les fichiers et essayent d'y accéder régulièrement. Si le contrôle sur accès est activé, Sophos Endpoint Security and Control détecte chaque accès à un fichier et envoie une alerte.

Procédez de la manière suivante :

- Désactivez le contrôle sur accès des adwares et des PUA. Vous pouvez utiliser un contrôle planifié à la place.
- Autorisez l'application (si vous désirez qu'elle soit exécutée sur vos ordinateurs). Retrouvez plus de renseignements à la section Autorisation des adwares et des PUA (page 111).
- Nettoyez le ou les ordinateurs en supprimant les applications que vous n'avez pas autorisées. Retrouvez plus de renseignements à la section Nettoyage immédiat des ordinateurs (page 55).

13.17 Échec du nettoyage

Si Sophos Endpoint Security and Control ne parvient pas à nettoyer les éléments (« Échec du nettoyage »), c'est probablement pour la raison suivante :

- Il n'a pas trouvé tous les composants d'un élément à plusieurs composants. Exécutez un contrôle intégral du système du ou des ordinateurs pour trouver les autres composants. Retrouvez plus de renseignements à la section Contrôle immédiat des ordinateurs (page 54).
- Certains lecteurs ou dossiers contenant les composants de l'élément sont exclus du contrôle. Vérifiez les éléments exclus du contrôle (section Exclusion d'éléments du contrôle sur accès (page 88)). Si certains éléments figurent dans la liste, supprimez-les de la liste.
- Vos droits d'accès sont insuffisants
- Il ne parvient pas à nettoyer ce type d'élément.
- Un fragment de virus a été découvert plutôt qu'une correspondance virale exacte.
- L'élément se trouve sur une disquette ou un CD-ROM protégé en écriture.
- L'élément se trouve sur un volume NTFS (Windows) protégé en écriture.

13.18 Guérison des effets secondaires des virus

Le nettoyage peut supprimer un virus des ordinateurs mais ne peut pas toujours neutraliser les effets secondaires.

Certains virus ne laissent aucun effet secondaire. D'autres peuvent apporter des modifications ou corrompre des données de telle manière qu'il est très difficile de les détecter. Pour gérer ce problème, procédez comme suit :

- Cliquer sur **Informations sur la sécurité** dans le menu **Aide**. Cette opération vous connecte au site Web de Sophos sur lequel vous pouvez consulter l'analyse du virus.
- Utilisez des sauvegardes ou des copies originales des programmes pour remplacer les programmes infectés. Si vous n'aviez pas de copies de sauvegarde avant l'infection, créez-les en cas de futures infections.

Il est parfois possible de récupérer des données sur les disques endommagés par un virus. Sophos peut vous fournir des utilitaires pour réparer les dommages occasionnés par certains virus. Veuillez contacter le support technique de Sophos pour obtenir plus de conseils.

13.19 Guérison des effets secondaires des applications

Le nettoyage supprime les applications indésirables mais ne peut pas toujours neutraliser les effets secondaires.

Certaines applications modifient le système d'exploitation, par exemple, en changeant vos paramètres de connexion Internet. Sophos Endpoint Security and Control ne peut pas toujours restaurer tous les paramètres. Par exemple, si une application a modifié la page d'accueil de l'explorateur, Sophos Endpoint Security and Control ne peut pas savoir quelle page d'accueil était utilisée auparavant.

Certaines applications installent des utilitaires, tels que des fichiers .dll ou .ocx sur votre ordinateur. Si un utilitaire est inoffensif (c'est-à-dire qu'il ne possède pas les « qualités » d'une application potentiellement indésirable), par exemple, une bibliothèque de langue, et qu'il ne fait pas partie intégrante de l'application, il se peut que Sophos Endpoint Security and Control ne le détecte pas en tant que partie de l'application. Dans ce cas, le nettoyage n'entraînera pas la suppression du fichier de votre ordinateur.

Parfois une application, telle qu'un adware (logiciel publicitaire), fait partie d'un programme que vous avez installé de manière intentionnelle, et sa présence est requise pour pouvoir exécuter le programme. Si vous supprimez cette application, l'exécution de ce programme peut s'interrompre sur l'ordinateur.

Procédez comme suit :

- Cliquer sur **Informations sur la sécurité** dans le menu **Aide**. Cette opération vous connecte au site Web de Sophos sur lequel vous pouvez consulter l'analyse de l'application.
- Utiliser des sauvegardes pour restaurer les paramètres de votre système ou les programmes que vous désirez utiliser. Si vous n'aviez pas de copies de sauvegarde avant l'incident, créez-les en cas de futurs incidents.

Veuillez contacter le support technique Sophos pour obtenir plus de renseignements ou de conseils sur la manière de guérir les effets secondaires d'un adware ou d'une application potentiellement indésirable.

13.20 Le contrôle des données ne détecte pas les fichiers téléchargés en amont via les navigateurs intégrés

Le contrôle des données intercepte les documents qui sont téléchargés en amont via des navigateurs web autonomes. Il n'intercepte pas les documents téléchargés en amont via les navigateurs intégrés dans des applications tierces (par exemple, Lotus Notes). Si vous avez une application tierce avec un navigateur intégré et voulez surveiller tous les documents téléchargés en amont, vous devez configurer l'application pour le lancement d'un navigateur externe.

13.21 Le contrôle des données n'effectue pas le contrôle des fichiers téléchargés ou joints

Si vous excluez les fichiers distants du contrôle sur accès dans la stratégie antivirus et HIPS, le contrôle des données n'effectue pas le contrôle des fichiers téléchargés ou joints à partir d'un emplacement réseau à l'aide d'une application surveillée, par exemple, un client de messagerie, un navigateur web ou un client de messagerie instantanée (IM). Dans ce cas, le contrôle des données utilise la même série d'exclusions que l'utilitaire de contrôle sur accès Sophos Anti-Virus (InterCheck ™). Ainsi, si le contrôle des fichiers distants est désactivé, il n'envoie aucun fichier distant au contrôle des données.

Retrouvez plus de renseignements sur la configuration des exclusions du contrôle sur accès à la section Exclusion d'éléments du contrôle sur accès (page 88).

Remarque
Le contrôle des données n'utilise pas les exclusions du contrôle sur accès lorsque les fichiers sont copiés ou déplacés à l'aide de l'Explorateur Windows. Dans ce cas, le contrôle des données intercepte les fichiers lors de leur transfert sur les périphériques de stockage surveillés à partir d'un emplacement réseau, par exemple, lorsque des fichiers sont copiés sur un périphérique de stockage amovible ou que des données sont gravées sur des supports optiques.

13.22 Un gestionnaire de mise à jour désinstallé demeure affiché dans la console

Suite à la désinstallation d'un gestionnaire de mise à jour supplémentaire, il se peut que ce dernier demeure affiché dans la vue **Gestionnaires de mise à jour** dans l'Enterprise Console.

Pour supprimer le gestionnaire de mise à jour de la console, sélectionnez-le, cliquez dessus avec le bouton droit de la souris et cliquez sur **Supprimer**.

14 Glossaire

Événement de synchronisation Active Directory	Événement qui a lieu lors de la synchronisation avec Active Directory.
Sous-parc actif	Sous-parc qui apparaît dans le volet Groupes.
Éditeur avancé de la Liste de contrôle du contenu	Éditeur qui permet de créer une Liste de contrôle du contenu composée d'un résultat, d'un décompte maximum, d'une expression régulière et d'un score de déclenchement à atteindre avant qu'il y ait correspondance avec la Liste de contrôle du contenu.
Gestionnaire d'applications	Boîte de dialogue qui vous permet d'autoriser ou de créer de nouvelles règles pour les applications qui ont été bloquées par Sophos Client Firewall.
Audit	Fonction qui vous permet de surveiller les changements dans la configuration de l'Enterprise Console et d'autres actions de l'utilisateur et du système.
Protection automatique	Déploiement des logiciels de sécurité (installation et application des stratégies de sécurité) sur tous les ordinateurs dans un conteneur Active Directory dès qu'ils sont synchronisés avec l'Enterprise Console.
Catégorie	Marque spécifique utilisée pour classer les Listes de contrôle du contenu des SophosLabs en fonction de leur type, du règlement qui définit leur contenu ou de la région à laquelle elles s'appliquent.
Liste de contrôle du contenu (LCC)	Ensemble de conditions qui spécifient le contenu d'un fichier, par exemple, des numéros de carte de crédit ou de débit ou les détails d'un compte bancaire ainsi que d'autres formes d'informations d'identification personnelles. Il existe deux types de Liste de contrôle du contenu : la Liste de contrôle du contenu des SophosLabs et la Liste de contrôle du contenu personnalisée.
Règle de contenu	Règle contenant une ou plusieurs Listes de contrôle du contenu et spécifiant l'action prise si l'utilisateur tente de transférer dans la destination spécifiée des données qui correspondent à toutes les Listes de contrôle du contenu.
Application contrôlée	Application non malveillante qu'une entreprise peut, si elle le souhaite, détecter ou bloquer car elle fragilise la productivité ou les performances du réseau.
Données contrôlées	Fichiers qui remplissent les conditions du contrôle des données.

Périphérique contrôlé	Périphérique sujet au contrôle des périphériques.
Niveau critique	Valeur qui déclenche le changement de l'état de sécurité d'un élément en Critique.
Liste de contrôle du contenu personnalisée	Liste de contrôle du contenu créée par un client Sophos. Il existe deux façons de créer une Liste de contrôle du contenu personnalisée : en créant une liste simple de termes recherchés avec une condition de recherche spécifiée comme « un de ces termes » ou en utilisant un éditeur avancé de Liste de contrôle du contenu.
Tableau de bord	Offre une visibilité immédiate de l'état de sécurité du réseau.
Événement du tableau de bord	Événement où un indicateur du tableau de bord dépasse le niveau critique. Une alerte par email générée lorsqu'un événement se produit sur le tableau de bord.
Contrôle des données	Fonction qui réduit la perte accidentelle de données depuis les stations de travail. Elle se déclenche lorsque l'utilisateur d'une station de travail essaie de transférer un fichier qui répond aux critères définis dans la stratégie et dans les règles de contrôle des données. Par exemple, lorsqu'un utilisateur tente de copier une feuille de calcul contenant une liste de données clients dans un dispositif de stockage amovible ou de télécharger en amont un document marqué comme confidentiel dans un compte de messagerie web, le contrôle des données va, s'il est configuré pour cela, bloquer le transfert.
Protection contre la perte de données (DLP)	Voir *Contrôle des données*.
Base de données	Composant de Sophos Enterprise Console qui archive les détails sur les ordinateurs du réseau.
Sous-parc par défaut	Sous-parc qui a, à sa racine, le nœud racine du serveur de l'arborescence et le groupe **Non assignés**. Il apparaît par défaut lorsque vous ouvrez l'Enterprise Console pour la première fois.
Contrôle des périphériques	Fonction pour réduire la perte accidentelle de données des stations de travail et restreindre l'introduction de logiciels depuis l'extérieur du réseau. Elle prend les mesures appropriées lorsqu'un utilisateur tente d'utiliser sur son poste un périphérique de stockage non autorisé ou un périphérique de réseau.
Réputation des téléchargements	La réputation d'un fichier téléchargé à partir d'Internet. La réputation est calculée en fonction de l'ancienneté, de la source, de la prévalence, de l'analyse détaillée et d'autres caractéristiques du fichier. Elle permet d'établir si un fichier est sain ou s'il représente un danger potentiel pouvant endommager l'ordinateur de l'utilisateur s'il est téléchargé.

Parc	Voir *Parc informatique*.
Périphérique exempté	Périphérique explicitement exclu du contrôle des périphériques.
Expression	Voir *Expression régulière.*
Règle de correspondance de fichier	Règle qui spécifie une action prise si l'utilisateur tente de transférer dans la destination spécifiée un fichier avec un nom spécifique ou d'un type donné, par exemple, le blocage du transfert des bases de données dans des dispositifs de stockage amovibles.
Groupe	Groupe d'ordinateurs administrés définis dans Sophos Enterprise Console.
Indicateur de bon fonctionnement	Terme générique utilisé pour les icônes décrivant l'état de sécurité d'une section ou d'un élément du tableau de bord, ou l'état global du réseau.
HIPS (système de prévention des intrusions sur l'hôte)	Technologie de sécurité pour assurer la protection contre les fichiers suspects, les virus non identifiés et tout comportement suspect.
Parc informatique	Environnement informatique de l'entreprise, y compris les ordinateurs, le réseau, etc.
Détection du trafic malveillant	Fonction qui détecte les communications entre les ordinateurs compromis et les serveurs de commande et de contrôle des pirates informatiques.
Ordinateur administré	Ordinateur sur lequel Remote Management System (RMS) est installé et sur lequel Sophos Enterprise Console peut installer et mettre à jour les logiciels, et éditer des rapports.
Console d'administration	Composant de Sophos Enterprise Console qui vous permet de protéger et d'administrer les ordinateurs.
Serveur d'administration	Composant de Sophos Enterprise Console qui gère la mise à jour et les communications avec les ordinateurs en réseau.
Décompte maximum	Nombre maximum de correspondances d'une expression régulière pouvant être comptabilisées jusqu'au résultat total.
Ordinateur obsolète	Ordinateur ne disposant pas des logiciels Sophos à jour.
Évaluation des correctifs	Évalue le nombre de correctifs installés sur les ordinateurs et identifie les correctifs manquants.
Stratégie	Groupe de paramètres, par exemple, pour la mise à jour, appliqué à un groupe ou à des groupes d'ordinateurs.
Application potentiellement indésirable (PUA)	Application non malveillante en soi mais dont la présence est généralement considérée comme inappropriée par la majorité des réseaux professionnels.

Quantité	Volume du type de données clé de la Liste de contrôle du contenu devant être trouvé dans un fichier avant qu'il y ait correspondance avec la Liste de contrôle du contenu.
Clé de quantité	Type de données clé défini dans une Liste de contrôle du contenu, auquel est appliqué le paramètre de quantité. Par exemple, pour une Liste de contrôle du contenu contenant des numéros de cartes de crédit ou de débit, la quantité spécifie le nombre de numéros de cartes de crédit ou de débit à trouver avant qu'il y ait correspondance avec la Liste de contrôle du contenu.
Région	Portée de la Liste de contrôle du contenu des SophosLabs. La région spécifie le pays auquel s'applique la Liste de contrôle du contenu (pour les listes spécifiques aux pays) ou indique « global » (pour les listes globales applicables à tous pays).
Expression régulière	Chaine de caractères de recherche utilisant des caractères spéciaux pour une correspondance avec un modèle de texte présent dans un fichier. Le contrôle des données utilise la syntaxe Perl 5 des expressions régulières.
Droit	Série de permissions pour l'exécution de certaines tâches dans l'Enterprise Console.
Rôle	Série de droits qui déterminent l'accès à l'Enterprise Console.
Administration déléguée	Fonctionnalité qui vous permet de définir quels ordinateurs sont accessibles à l'utilisateur et quelles tâches il peut effectuer selon son rôle dans l'entreprise.
Rootkit	Cheval de Troie ou technologie utilisée pour dissimuler la présence d'un objet malveillant (processus, fichier, clé de registre ou port réseau) à l'utilisateur de l'ordinateur ou à l'administrateur.
Règle	Règle spécifiant l'action prise si un fichier remplit certaines conditions. Il existe deux types de règles de contrôle des données : la règle de correspondance de fichier et la règle de contenu.
Résultat	Nombre ajouté au résultat total d'une Liste de contrôle du contenu en cas de correspondance d'une expression régulière.
Nœud racine serveur	Nœud principal de l'arborescence dans le volet **Groupes**, qui inclut le dossier **Non assignés**.
Sophos Live Protection	Fonction qui utilise la technologie dans le Cloud pour décider instantanément si un fichier suspect est une menace et prendre les mesures spécifiées dans la configuration du nettoyage antivirus de Sophos.

Sophos Update Manager (SUM)	Programme qui télécharge les logiciels et les mises à jour de sécurité Sophos depuis le site Web de Sophos ou depuis un autre serveur de mise à jour dans les emplacements de mise à jour partagés.
Règle définie par Sophos	Règle fournie par Sophos en guise d'exemple. Les règles définies par Sophos ne sont pas mises à jour par Sophos.
Liste de contrôle du contenu des SophosLabs	Liste de contrôle du contenu fournie et administrée par Sophos. Sophos peut mettre à jour les Listes de contrôle du contenu des SophosLabs ou en créer de nouvelles avant de les mettre à disposition dans l'Enterprise Console. Le contenu des Listes de contrôle du contenu des SophosLabs ne peut pas être modifié. Par contre, la quantité peut être définie pour chacune de ces listes.
Sous-parc	Partie nommée du parc informatique, contenant un sous-ensemble d'ordinateurs et de groupes.
Administration des sous-parcs	Fonctionnalité restreignant les ordinateurs et les groupes disponibles pour des opérations.
Abonnement logiciels	Ensemble des versions d'un logiciel pour une variété de plates-formes, sélectionnées par l'utilisateur, qu'Update Manager télécharge et maintient à jour. Une version peut être indiquée pour chaque plate-forme prise en charge (par exemple, « Recommended » pour Windows).
Détection des comportements suspects	Analyse dynamique du comportement de tous les programmes s'exécutant sur le système afin de détecter et de bloquer toute activité qui semble malveillante.
Fichier suspect	Fichier qui présente une combinaison de caractéristiques qui sont généralement, mais pas exclusivement, rencontrées dans les virus.
Intervalle de synchronisation	Période après laquelle un point de synchronisation dans l'Enterprise Console est synchronisé avec le conteneur Active Directory sélectionné.
Point de synchronisation (pour une arborescence Active Directory)	Groupe Sophos Enterprise Console dans lequel le contenu d'un conteneur Active Directory sélectionné (groupes et ordinateurs ou groupes seulement) sera ajouté pour synchronisation, sans que sa structure ne soit modifiée.
Synchronisation avec Active Directory	Synchronisation unidirectionnelle d'un ou de plusieurs groupes Sophos Enterprise Console avec des unités organisationnelles ou conteneurs Active Directory.
Groupe synchronisé	Tout groupe au-dessous du point de synchronisation.

Administrateur système	Rôle préconfiguré disposant des droits complets d'administration des logiciels de sécurité Sophos sur le réseau et des rôles dans l'Enterprise Console. Le rôle Administrateur système ne peut pas être supprimé ou voir ses droits ou son nom changés et le groupe Sophos Full Administrators Windows ne peut pas être supprimé de ce rôle. Les autres utilisateurs et groupes peuvent être ajoutés ou supprimés du rôle.
Label	Description appliquée à la Liste de contrôle du contenu SophosLabs pour identifier le contenu ou la portée de cette liste. Il existe trois types d'identifiant : type, règlement et région.
Protection antialtération	Fonction qui empêche les programmes malveillants connus et les utilisateurs non autorisés (administrateurs locaux et utilisateurs avec peu d'expérience technique) de désinstaller les logiciels de sécurité de Sophos ou de les désactiver par le biais de l'interface Sophos Endpoint Security and Control.
Niveau seuil	Valeur qui déclenche le changement de l'état de sécurité d'un élément en Avertissement ou Critique.
Résultat total	Somme des résultats d'une Liste de contrôle du contenu, en fonction du contenu correspondant.
Résultat de déclenchement	Nombre de fois qu'une expression régulière doit être trouvée avant qu'il y ait correspondance avec une Liste de contrôle du contenu.
Type de fichier véritable	Type de fichier identifié par l'analyse de la structure d'un fichier par opposition à son extension. Cette méthode est plus fiable.
Type	Critères en fonction desquels les Listes de contrôle du contenu des SophosLabs sont classées. Par exemple, une Liste de contrôle du contenu définissant des détails de passeports, des adresses postales ou des adresses électroniques appartient au type Informations personnellement identifiables.
Gestionnaire de mise à jour	Voir *Sophos Update Manager.*
Niveau d'alerte	Valeur qui déclenche le changement de l'état de sécurité d'un élément en Avertissement.
Contrôle du Web	Fonction qui vous permet de définir et d'appliquer les stratégies d'accès au Web de votre entreprise et de voir des rapports sur les habitudes de navigation sur le Web. Vous pouvez autoriser ou bloquer l'accès des utilisateurs à certaines catégories de sites Web et les utilisateurs peuvent également être avertis s'ils visitent des sites Web enfreignant les stratégies de votre entreprise.

Protection Web	Fonction qui détecte les menaces sur les pages Web. Cette fonction bloque les sites qui ont hébergé du contenu malveillant par le passé et empêche également tout téléchargement malveillant. La protection Web fait partie de la stratégie antivirus et HIPS.

15 Support technique

Vous bénéficiez du support technique des produits Sophos de l'une des manières suivantes :

- Rendez-vous sur le forum Sophos Community en anglais sur community.sophos.com/ et recherchez d'autres utilisateurs rencontrant le même problème que le vôtre.
- Rendez-vous sur la base de connaissances du support de Sophos sur www.sophos.com/fr-fr/support.aspx.
- Téléchargez la documentation des produits sur www.sophos.com/fr-fr/support/documentation.aspx.
- Ouvrez un incident support sur https://secure2.sophos.com/fr-fr/support/contact-support/support-query.aspx.

16 Mentions légales

Index

A

B

C

D

E

F

G

H

I

J

L

M

N

O

P

R

S

T

U

V

W