À propos de Sophos Endpoint Security and Control

La version 10.3 de Sophos Endpoint Security and Control est une suite intégrée de logiciels de sécurité.

Sophos Anti-Virus détecte et nettoie les virus, chevaux de Troie, vers et spywares, ainsi que les adwares et toutes autres applications potentiellement indésirables. Notre technologie HIPS (Host Intrusion Prevention System, système de prévention des intrusions sur l'hôte) peut également protéger votre ordinateur contre les fichiers suspects et les rootkits.

La **surveillance des comportements Sophos** utilise notre technologie HIPS pour assurer la protection des ordinateurs contre les menaces du jour zéro ou non identifiées et contre les comportements suspects.

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

La **protection Web Sophos** assure une protection étendue contre les menaces Web en empêchant l'accès aux emplacements qui sont connus pour héberger des malwares. Elle empêche les ordinateurs d'extrémité d'accéder à ces sites en effectuant une recherche en temps réel dans la base de données en ligne de Sophos répertoriant les sites Web malveillants.

Le **contrôle des applications Sophos** bloque les applications non autorisées tels que celles de voix sur IP, de messagerie instantanée, de partage de fichiers et de jeux.

Le **contrôle des périphériques Sophos** bloque les périphériques de stockage externes non autorisés et les technologies de connexion sans fil.

Le **contrôle des données Sophos** empêche toute fuite accidentelle d'informations d'identification personnelles depuis des ordinateurs

administrés.

Le **contrôle Web de Sophos** permet d'assurer la protection, le contrôle et l'édition de rapports des ordinateurs itinérants ou qui ne font pas partie du réseau d'entreprise.

Sophos Client Firewall empêche le vol et la communication d'informations sensibles par des vers, des chevaux de Troie et des spywares ainsi que toute intrusion de pirates informatiques.

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

La **protection antialtération Sophos** vous permet d'interdire aux utilisateurs non autorisés (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.

À propos de la page d'accueil

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

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

À propos des groupes Sophos

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

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

Groupe Windows	Groupe Sophos
Administrateurs	SophosAdministrator
Super Utilisateurs	SophosPowerUser
Utilisateurs	SophosUser

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

- Contrôle sur accès
- Contrôle par clic droit

SophosUsers

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

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

SophosPowerUsers

Les SophosPowerUsers ont les mêmes droits que les SophosUsers et

disposent en plus des droits suivants :

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

SophosAdministrators

SophosAdministrators peut utiliser et configurer n'importe quelle partie de Sophos Endpoint Security and Control.

Remarque : si la protection antialtération est activée, un SophosAdministrator doit connaître le mot de passe de la protection antialtération pour pouvoir effectuer les tâches suivantes :

- Configurer le contrôle sur accès.
- Configurer la détection des comportements suspects.
- Désactiver la protection antialtération.

Pour plus d'informations, reportez-vous à la section *À propos de la protection antialtération sur cet ordinateur*.

Ajout d'un utilisateur au groupe Sophos

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

Pour ajouter un utilisateur au groupe Sophos :

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

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

Remarques

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

Configuration des droits utilisateur pour le gestionnaire de quarantaine

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

1. Cliquez sur **Accueil** > **Antivirus et HIPS** > **Configurer l'antivirus et HIPS** > **Configuration** > **Droits utilisateur pour le gestionnaire de quarantaine**.
2. Sélectionnez le type d'utilisateurs qui va effectuer chaque type d'actions.

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

Option	Description
Nettoyer les secteurs	L'utilisateur peut nettoyer les secteurs de démarrage de disquette.
Nettoyer les fichiers	L'utilisateur peut nettoyer les documents et les programmes.
Supprimer les fichiers	L'utilisateur peut supprimer les fichiers infectés.
Déplacer les fichiers	L'utilisateur peut déplacer les fichiers infectés dans un autre dossier.
Autoriser	L'utilisateur autorise l'exécution d'éléments suspects, d'adwares et de PUA (Potentially Unwanted Application, application potentiellement indésirable) sur l'ordinateur. Cette option s'applique au **Gestionnaire d'autorisation** et au **Gestionnaire de quarantaine**.

À propos du contrôle sur accès et du contrôle à la demande

Contrôle sur accès

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

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

Retrouvez plus d'informations à la section *Configuration du contrôle sur accès*.

Contrôle à la demande

Les contrôles à la demande assurent une protection supplémentaire. Comme le nom l'indique, c'est sur votre demande que le contrôle à la demande est lancé. Vous pouvez contrôler tout ce que vous voulez que ce soit un seul fichier ou tout un ordinateur.

Retrouvez plus d'informations à la section *Types de contrôle à la demande*.

À propos du bon usage relatif au contrôle sur accès

Cette section contient des recommandations pour vous aider à tirer le meilleur profit du contrôle sur accès.

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. Pour plus d'informations sur les paramètres conseillés du contrôle sur accès, consultez l'article 114345 de la base de connaissances du support Sophos (*http://www.sophos.com/fr-fr/support/knowledgebase/114345.aspx*).

Configuration du contrôle sur accès

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 d'informations sur l'utilisation de la stratégie antivirus et HIPS avec un logiciel de chiffrement dans l'article 12790 de la base de connaissances du support de Sophos *http://www.sophos.com/fr-fr/support/knowledgebase/12790.aspx*.

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

Par défaut, Sophos Anti-Virus détecte et nettoie les menaces suivantes au cours d'un contrôle sur accès :

- virus
- chevaux de Troie
- vers
- spywares

Pour configurer le contrôle sur accès :

1. Cliquez sur **Accueil** > **Antivirus et HIPS** > **Configurer l'antivirus et HIPS** > **Configuration** > **Contrôle sur accès**.
2. 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.
Au moment de renommer	Contrôle des fichiers lorsqu'ils sont renommés.

À l'écriture	Contrôle des fichiers lorsqu'ils sont enregistrés ou créés.

3. 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	Fichier qui affiche une combinaison de caractéristiques qui sont généralement, mais pas exclusivement, rencontrées chez les virus.

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

Option	Description
Permettre l'accès aux lecteurs avec secteurs de démarrage infectés	Activez cette option afin de permettre l'accès à un support ou périphérique amovible dont le secteur de démarrage est infecté tel qu'un CD-ROM d'initialisation, une disquette ou un lecteur flash USB. Utilisez uniquement cette option après avoir demandé conseil auprès du support technique de Sophos. Reportez-vous également à la section *Autorisation d'accès aux lecteurs avec secteurs de démarrage infectés* de la rubrique *Résolution des problèmes*.

Contrôler tous les fichiers	Nous vous conseillons de conserver cette option **désactivée** car elle ralentit considérablement les performances de l'ordinateur. Nous vous conseillons de contrôler tous les fichiers uniquement au cours d'un contrôle hebdomadaire.
Contrôler dans les fichiers archive	Activez cette option pour contrôler le contenu des fichiers archives ou compressés. Effectuez uniquement cette opération si vous téléchargez et distribuez ces fichiers sans extraire leur contenu. Nous vous conseillons de conserver cette option **désactivée** car elle ralentit considérablement le contrôle. Vous continuerez à être protégé contre les menaces 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 vous ouvrez 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	Activez cette option pour exécuter 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). **Remarque :** cette option est uniquement disponible sur les systèmes d'exploitation 32

bits.

Désactivation temporaire du contrôle sur accès

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

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

1. Cliquez sur **Accueil** > **Antivirus et HIPS** > **Configurer l'antivirus et HIPS** > **Configuration** > **Contrôle sur accès**.
2. Dessélectionnez la case **Activer le contrôle sur accès pour cet ordinateur**.

Configuration du nettoyage sur accès

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

Pour configurer le nettoyage sur accès :

1. Cliquez sur **Accueil** > **Antivirus et HIPS** > **Configurer l'antivirus et HIPS** > **Configuration** > **Contrôle sur accès**.
2. Cliquez sur l'onglet **Nettoyage**.
3. Pour nettoyer automatiquement les fichiers infectés, sous **Virus/spywares**, sélectionnez la case **Nettoyer automatiquement les éléments contenant des virus/spywares**.

   Remarque : si vous activez cette option, le nettoyage de certains virus/spywares déclenchera un contrôle intégral du système qui va essayer de nettoyer *tous* les virus sur votre ordinateur. Cette opération peut prendre du temps.

4. Sous **Virus/spywares**, sélectionnez l'action que Sophos Anti-Virus doit prendre contre les éléments infectés si vous avez déactivé le nettoyage automatique ou en cas d'échec du nettoyage automatique :

Option	Description
Refuser l'accès uniquement	Sophos Anti-Virus vous demande de confirmer ce que vous souhaitez faire avant de continuer. Il s'agit du paramètre par défaut.
Supprimer Refuser l'accès et déplacer	Utilisez uniquement ces paramètres après avoir demandé conseil auprès du support technique de Sophos. Sinon, utilisez le gestionnaire de quarantaine pour nettoyer votre ordinateur des

dans	virus/spywares détectés par Sophos Anti-Virus. Reportez-vous à la section *Traitement des virus/spywares en quarantaine*.

5. Sous **Fichiers suspects**, sélectionnez l'action que Sophos Anti-Virus doit prendre lorsqu'il trouve des fichiers contenant du code qui est habituellement utilisé dans des programmes malveillants :

Option	Description
Refuser l'accès	Sophos Anti-Virus vous demande de confirmer ce que vous souhaitez faire avant de continuer. Il s'agit du paramètre par défaut.
Supprimer Refuser l'accès et déplacer dans	Utilisez uniquement ces paramètres après avoir demandé conseil auprès du support technique de Sophos. Utilisez plutôt le gestionnaire de quarantaine pour nettoyer votre ordinateur des fichiers suspects détectés par Sophos Anti-Virus. Reportez-vous à la section *Traitement des fichiers suspects en quarantaine*.

Réinitialisation des sommes de contrôle des fichiers contrôlés

La liste des sommes de contrôle des fichiers contrôlés est réinitialisée lors de la mise à jour de Sophos Anti-Virus ou au redémarrage de votre ordinateur. La liste est alors actualisée avec de nouvelles données à mesure que les fichiers sont contrôlés par Sophos Anti-Virus.

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

Pour réinitialiser les sommes de contrôle des fichiers contrôlés :

1. Cliquez sur **Accueil** > **Antivirus et HIPS** > **Configurer l'antivirus et HIPS** > **Configuration** > **Contrôle sur accès**.
2. Sur l'onglet **Contrôle**, cliquez sur **Vider la mémoire cache**.

Spécification des extensions de fichier pour le contrôle sur accès

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

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

1. Cliquez sur **Accueil** > **Antivirus et HIPS** > **Configurer l'antivirus et HIPS** > **Configuration** > **Contrôle sur accès**.
2. Cliquez sur l'onglet **Extensions** et paramétrez les options comme décrit ci-dessous :

   Contrôler tous les fichiers

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

   Me permettre de gérer exactement ce qui est contrôlé

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

   ATTENTION : la liste des extensions inclut les types de fichiers que nous conseillons de contrôler. Comme expliqué ci-dessous, modifiez la liste avec grande précaution.

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

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

   Pour changer l'extension d'un fichier dans la liste,

sélectionnez l'extension et cliquez sur **Modifier**.

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

Ajout, modification ou suppression des exclusions du contrôle sur accès

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

Pour modifier la liste des fichiers, dossiers et lecteurs qui sont exclus du contrôle sur accès :

1. Cliquez sur **Accueil** > **Antivirus et HIPS** > **Configurer l'antivirus et HIPS** > **Configuration** > **Contrôle sur accès**.
2. Cliquez sur l'onglet **Exclusions** et choisissez ensuite l'une des options suivantes.
    - Pour spécifier un fichier, un dossier ou un lecteur à exclure du contrôle sur accès, cliquez sur **Ajouter**.
    - Pour supprimer une exclusion, cliquez sur **Supprimer**.
    - Pour modifier une exclusion, cliquez sur **Modifier**.
3. Pour ajouter ou modifier un élément exclus, dans la boîte de dialogue **Exclusion d'un élément**, sélectionnez le **Type d'élément**.

    Le type d'élément **Tous les fichiers distants** sert à exclure les fichiers qui ne sont pas stockés sur des lecteurs locaux. Vous pouvez sélectionner cette option si vous voulez augmenter la vitesse d'accès à ces fichiers et si vous faites confiance aux emplacements de fichiers distants disponibles.
4. Spécifiez le **Nom de l'élément** à l'aide du bouton **Parcourir** ou en le saisissant dans la zone de texte.

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

Retrouvez plus d'informations sur la spécification des noms d'élément à la section *Spécification des noms de fichier et des chemins des éléments d'exclusion du contrôle*.

Spécification des noms de fichier et des chemins des éléments d'exclusion du contrôle

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.

Exclusion d'un fichier spécifique

Spécifiez 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\Users\Documents\CV.doc

Remarque : 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 d'informations à la section *http://www.sophos.com/fr-fr/support/knowledgebase/13045.aspx*.

Exclusion de tous les fichiers du même nom

Spécifiez un nom de fichier sans son chemin afin d'exclure tous les fichiers du même nom sur tout le système de fichiers :

spacer.gif

Exclusion de tout le contenu du lecteur ou du partage réseau

Spécifiez une lettre de lecteur ou un nom de partage réseau pour exclure tout le contenu présent sur ce lecteur ou ce partage réseau :

C:

\\Server\<nom du partage>\

Remarque : lorsque vous indiquez un partage réseau, pensez à inclure la barre oblique finale.

Exclusion d'un dossier spécifique

Spécifiez 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

Exclusion de tous les dossiers du même nom

Spécifiez 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. Par exemple, \Outils\logs exclut les dossiers suivants :

C:\Outils\logs

\\Serveur\Outils\logs

Remarque : vous devez spécifier le chemin complet jusqu'à la lettre du lecteur ou du nom de partage réseau. Ainsi, dans l'exemple ci-dessus, la spécification simple de \logs n'exclut aucun fichier.

Caractères joker ? et *

Utilisez le caractère joker ? 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 correspond à fichier.txtfichier1.txt et fichier12.txt, mais pas à fichier123.txt.

Utilisez le caractère joker * dans un nom de fichier ou une extension au format [nom de fichier].* ou *.[extension]:

Correct

fichier.*

*.txt

Incorrect

fichier*.txt

fichier.txt*

fichier.*txt

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.

Types de contrôle à la demande

Contrôle par clic droit

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

- *Exécution d'un contrôle par clic droit*

Contrôle personnalisé

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

- *Exécution d'un contrôle personnalisé*
- *Planification d'un contrôle personnalisé*

Contrôle intégral de l'ordinateur

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

- *Exécution d'un contrôle intégral de l'ordinateur*

Spécification des extensions de fichier pour le contrôle à la demande

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

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

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

   Contrôler tous les fichiers

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

   Me permettre de gérer exactement ce qui est contrôlé

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

   ATTENTION : la liste des extensions inclut les types de fichiers que nous conseillons de contrôler. Comme expliqué ci-dessous, modifiez la liste avec grande précaution.

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

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

   Pour changer l'extension d'un fichier dans la liste,

sélectionnez l'extension et cliquez sur **Modifier**.

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

Ajout, modification ou suppression des exclusions du contrôle à la demande

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

La procédure décrite ci-dessous s'applique à **tous** les contrôles à la demande. Pour plus d'informations sur l'exclusion d'éléments spécifiques d'un contrôle personnalisé, reportez-vous à la section *Création d'un contrôle personnalisé*.

Pour modifier la liste des fichiers, dossiers et lecteurs exclus du contrôle à la demande :

1. Cliquez sur **Accueil** > **Antivirus et HIPS** > **Configurer l'antivirus et HIPS** > **Configuration** > **Extensions et exclusions à la demande**.
2. Cliquez sur l'onglet **Exclusions** et choisissez ensuite l'une des options suivantes.
    - Pour spécifier un fichier, un dossier ou un lecteur à exclure du contrôle à la demande, cliquez sur **Ajouter**.
    - Pour supprimer une exclusion, cliquez sur **Supprimer**.
    - Pour modifier une exclusion, cliquez sur **Modifier**.
3. Pour ajouter ou modifier un élément exclus, dans la boîte de dialogue **Exclusion d'un élément**, sélectionnez le **Type d'élément**.
4. Spécifiez le **Nom de l'élément** à l'aide du bouton **Parcourir** ou en le saisissant dans la zone de texte.

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

Retrouvez plus d'informations sur la spécification des noms d'élément à la section *Spécification des noms de fichier et des chemins des éléments d'exclusion du contrôle*.

Configuration du contrôle par clic droit

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

Par défaut, Sophos Anti-Virus détecte et nettoie les menaces suivantes au cours d'un contrôle par clic droit :

- virus
- chevaux de Troie
- vers
- spywares
- adwares et autres applications potentiellement indésirables (PUA)

Pour configurer le contrôle sur par clic droit :

1. Cliquez sur **Accueil** > **Antivirus et HIPS** > **Configurer l'antivirus et HIPS** > **Configuration** > **Contrôle par clic droit**.
2. 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	Fichier qui affiche une combinaison de caractéristiques qui sont généralement, mais pas

exclusivement, rencontrées chez les virus.

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

Option	Description
Contrôler tous les fichiers	Nous vous conseillons de conserver cette option **désactivée** car elle ralentit considérablement les performances de l'ordinateur. Nous vous conseillons de contrôler tous les fichiers uniquement au cours d'un contrôle hebdomadaire.
Contrôler dans les fichiers archive	Activez cette option pour contrôler le contenu des fichiers archives ou compressés. Effectuez uniquement cette opération si vous téléchargez et distribuez ces fichiers sans extraire leur contenu. Nous vous conseillons de conserver cette option **désactivée** car elle ralentit considérablement le contrôle. Vous continuerez à être protégé contre les menaces 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 vous ouvrez 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.

Configuration du nettoyage par clic droit

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

Pour configurer le nettoyage par clic droit :

1. Cliquez sur **Accueil** > **Antivirus et HIPS** > **Configurer l'antivirus et HIPS** > **Configuration** > **Contrôle par clic droit**.
2. Cliquez sur l'onglet **Nettoyage**.
3. Pour nettoyer automatiquement les fichiers infectés, sous **Virus/spywares**, sélectionnez la case **Nettoyer automatiquement les éléments contenant des virus/spywares**.
4. Sélectionnez l'action que Sophos Anti-Virus doit prendre contre les éléments infectés si vous n'avez pas activé le nettoyage automatique ou en cas d'échec du nettoyage automatique :

Option	Description
Journaliser uniquement	La seule action prise par Sophos Anti-Virus est l'enregistrement des éléments infectés dans le journal du contrôle. Reportez-vous à la section *Consultation du journal du contrôle*. Il s'agit du paramètre par défaut.
Supprimer Déplacer dans	Utilisez uniquement ces paramètres après avoir demandé conseil auprès du support technique de Sophos. Sinon, utilisez le gestionnaire de quarantaine pour nettoyer votre ordinateur des virus/spywares détectés par Sophos Anti-Virus. Reportez-vous à la section *Traitement des virus/spywares en quarantaine*.

5. Sous **Fichiers suspects**, sélectionnez l'action que Sophos Anti-Virus doit prendre lorsqu'il trouve des fichiers contenant du code qui est habituellement utilisé dans des programmes malveillants :

Option	Description
Journaliser uniquement	La seule action prise par Sophos Anti-Virus est l'enregistrement des éléments infectés dans le journal du contrôle. Il s'agit du paramètre par défaut.
Supprimer Déplacer dans	Utilisez uniquement ces paramètres après avoir demandé conseil auprès du support technique de Sophos. Sinon, utilisez le gestionnaire de quarantaine pour nettoyer votre ordinateur des virus/spywares détectés par Sophos Anti-Virus. Reportez-vous à la section *Traitement des fichiers suspects en quarantaine*.

6. Pour supprimer tous les composants d'adwares et d'applications potentiellement indésirables (PUA) connus des ordinateur de tous vos utilisateurs, sous **Adwares et PUA**, sélectionnez la case **Nettoyer automatiquement les adwares et PUA**.

   Le nettoyage ne répare pas tous les changements que l'adware ou la PUA a déjà apporté.

   - Retrouvez plus d'informations sur la consultation des détails sur les effets secondaires de l'adware ou de la PUA sur le site Web de Sophos à la section *Informations sur le nettoyage*.
   - Retrouvez plus d'informations sur le nettoyage de votre ordinateur des adwares et des PUA à l'aide du gestionnaire de quarantaine à la section *Traitement*

des adwares et des PUA en quarantaine.

Exécution d'un contrôle par clic droit

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

1. À l'aide de l'Explorateur Windows, ou sur le bureau, sélectionnez le fichier, le dossier ou le lecteur de disque dur que vous voulez contrôler.

   Vous pouvez sélectionner plusieurs fichiers et dossiers.

2. Cliquez avec le bouton droit de la souris sur la sélection et cliquez sur **Contrôler avec Sophos Anti-Virus**.

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

Création d'un contrôle personnalisé

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

   Retrouvez plus d'informations sur la page d'**Accueil** à la section *À propos de la page d'accueil*.

2. Cliquez sur **Paramétrer un nouveau contrôle**.
3. Dans la zone de texte **Nom du contrôle**, saisissez un nom de contrôle.
4. Dans le volet **Eléments à contrôler**, sélectionnez les lecteurs et les dossiers que vous souhaitez contrôler. Pour cela, sélectionnez la case à cocher située à gauche de chaque lecteur ou dossier. Pour en savoir plus sur les icônes qui apparaissent dans les cases à cocher, reportez-vous à la section *Représentation des éléments à contrôler*.

   Remarque : les lecteurs ou dossiers non disponibles (parce qu'ils sont hors connexion ou supprimés) sont affichés avec une police de caractères barrés. Ils sont supprimés du volet **Eléments à contrôler** lorsqu'ils sont dessélectionnés ou si la sélection de leur lecteur ou dossier(s) parent a été modifiée.

5. Pour configurer davantage le contrôle, cliquez sur **Configurer ce contrôle**. (pour plus d'informations, reportez-vous à la section *Configuration d'un contrôle personnalisé*).
6. Pour planifier le contrôle, cliquez sur **Planifier ce contrôle**. (pour plus d'informations, reportez-vous à la section *Planification d'un contrôle personnalisé*).
7. Cliquez sur **Enregistrer** pour enregistrer le contrôle ou sur **Enregistrer et démarrer** pour enregistrer et exécuter le contrôle.

Représentation des éléments à contrôler

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

Icône	Explication
	L'élément et tous les sous-éléments *ne sont pas* sélectionnés pour le contrôle.
	L'élément et tous les sous-éléments *sont* sélectionnés pour le contrôle.
	L'élément est partiellement sélectionné : l'élément n'est pas sélectionné, mais certains éléments secondaires sont sélectionnés pour le contrôle.
	L'élément et tous les sous-éléments sont exclus de ce contrôle donné.
	L'élément est partiellement exclu : l'élément n'est pas sélectionné, mais certains éléments secondaires sont exclus de ce contrôle particulier.
	L'élément et tous les sous-éléments sont exclus de tous les contrôles à la demande à cause d'une exclusion à la demande qui a été paramétrée. Pour plus d'informations, reportez-vous à la section *Ajout, modification ou suppression des exclusions du contrôle sur accès*.

Configuration d'un contrôle personnalisé

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

Par défaut, Sophos Anti-Virus détecte et nettoie les menaces suivantes au cours d'un contrôle personnalisé :

- virus
- chevaux de Troie
- vers
- spywares
- adwares et autres applications potentiellement indésirables (PUA)
- rootkits

Pour configurer un contrôle personnalisé :

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

   Retrouvez plus d'informations sur la page d'**Accueil** à la section *À propos de la page d'accueil*.
2. Dans la liste des **Contrôles disponibles**, sélectionnez le contrôle que vous souhaitez modifier et cliquez sur **Modifier**.
3. Cliquez sur **Configurer ce contrôle**.
4. Sous **Rechercher les**, paramétrez les options comme décrit ci-dessous.

Option	Description
	Un adware affiche de la publicité (par exemple, des messages intempestifs), qui affecte la productivité des utilisateurs et les performances du système.

Adwares et PUA	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	Fichier qui affiche une combinaison de caractéristiques qui sont généralement, mais pas exclusivement, rencontrées chez les virus.
Rootkits	Si vous êtes membre du groupe SophosAdministrator, le contrôle à la recherche des rootkits est toujours exécuté lorsque vous effectuez un contrôle intégral de l'ordinateur. Vous pouvez aussi effectuer un contrôle à la recherche des rootkits dans le cadre d'un contrôle personnalisé.

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

Option	Description
Contrôler tous les fichiers	Nous vous conseillons de contrôler tous les fichiers uniquement lors d'un contrôle hebdomadaire. En effet, le contrôle de tous les fichiers affecte les performances de votre ordinateur.
Contrôler dans les	Activez cette option pour contrôler le contenu des fichiers archives ou compressés. Effectuez uniquement cette opération si vous téléchargez et distribuez ces fichiers sans extraire leur contenu. Nous vous conseillons de conserver cette option **désactivée** car elle ralentit considérablement le contrôle. Vous continuerez à être protégé contre les menaces dans les archives ou dans les fichiers compressés car tous les composants d'une

fichiers archive	archive ou d'un fichier compressé caractéristiques d'un programme malveillant seront bloqués par le contrôle sur accès : ▪ Lorsque vous ouvrez 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	Activez cette option pour exécuter 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). **Remarque :** cette option est uniquement disponible sur les systèmes d'exploitation 32 bits.
Exécuter le contrôle avec une priorité inférieure	Sur Windows Vista et supérieur, exécutez le contrôle personnalisé avec une priorité plus faible afin que l'impact soit minimal sur les applications de l'utilisateur.

Configuration du nettoyage pour un contrôle personnalisé

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

Pour configurer le nettoyage pour un contrôle personnalisé :

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

   Retrouvez plus d'informations sur la page d'**Accueil** à la section *À propos de la page d'accueil*.

2. Dans la liste des **Contrôles disponibles**, sélectionnez le contrôle que vous souhaitez modifier et cliquez sur **Modifier**.
3. Cliquez sur **Configurer ce contrôle**.
4. Cliquez sur l'onglet **Nettoyage**.
5. Pour nettoyer automatiquement les fichiers infectés, sous **Virus/spywares**, sélectionnez la case **Nettoyer automatiquement les fichiers contenant des virus/spywares**.
6. Sélectionnez l'action que Sophos Anti-Virus doit prendre contre les éléments infectés si vous n'avez pas activé le nettoyage automatique ou en cas d'échec du nettoyage automatique :

Option	Description
Journaliser uniquement	Pour le contrôle personnalisé, la seule action prise par Sophos Anti-Virus est l'enregistrement des éléments infectés dans le journal. Reportez-vous à la section *Consultation du journal du contrôle personnalisé*. Il s'agit du paramètre par défaut.
	Utilisez uniquement ces paramètres après avoir demandé conseil auprès du support technique

Supprimer	de Sophos.
Déplacer dans	Sinon, utilisez le gestionnaire de quarantaine pour nettoyer votre ordinateur des virus/spywares détectés par Sophos Anti-Virus. Reportez-vous à la section *Traitement des virus/spywares en quarantaine*.

7. Sous **Fichiers suspects**, sélectionnez l'action que Sophos Anti-Virus doit prendre lorsqu'il trouve des fichiers contenant du code qui est habituellement utilisé dans des programmes malveillants :

Option	Description
Journaliser uniquement	La seule action prise par Sophos Anti-Virus est l'enregistrement des éléments infectés dans le journal du contrôle. Il s'agit du paramètre par défaut.
Supprimer	Utilisez uniquement ces paramètres après avoir demandé conseil auprès du support technique de Sophos.
Déplacer dans	Sinon, utilisez le gestionnaire de quarantaine pour nettoyer votre ordinateur des virus/spywares détectés par Sophos Anti-Virus. Reportez-vous à la section *Traitement des fichiers suspects en quarantaine*.

8. Pour supprimer tous les composants d'adwares et d'applications potentiellement indésirables (PUA) connus des ordinateur de tous vos utilisateurs, sous **Adwares et PUA**, sélectionnez la case **Nettoyer automatiquement les adwares et PUA**.

   Le nettoyage ne répare pas tous les changements que l'adware ou la PUA a déjà apporté.

- Retrouvez plus d'informations sur la consultation des détails sur les effets secondaires de l'adware ou de la PUA sur le site Web de Sophos à la section *Informations sur le nettoyage*.
- Retrouvez plus d'informations sur le nettoyage de votre ordinateur des adwares et des PUA à l'aide du gestionnaire de quarantaine à la section *Traitement des adwares et des PUA en quarantaine*.

Planification d'un contrôle personnalisé

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

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

   Retrouvez plus d'informations sur la page d'**Accueil** à la section *À propos de la page d'accueil*.

2. Dans la liste des **Contrôles disponibles**, sélectionnez le contrôle que vous souhaitez modifier et cliquez sur **Modifier**.
3. Cliquez sur **Planifier ce contrôle**.
4. Dans la boîte de dialogue **Planification du contrôle**, sélectionnez **Activer la planification**.

   Sélectionnez le(s) jour(s) d'exécution du contrôle.

   Ajoutez la ou les heures en cliquant sur **Ajouter**.

   Si nécessaire, supprimez ou modifiez une heure en la sélectionnant et en cliquant respectivement sur **Supprimer** ou **Modifier**.

5. Saisissez le *nom utilisateur* et le *mot de passe*. Assurez-vous que le mot de passe soit bien rempli.

   Le contrôle planifié s'exécute avec les droits d'accès de cet utilisateur.

Remarque : si le contrôle détecte les composants d'une menace dans la mémoire et que vous n'avez pas paramétré ce contrôle pour qu'il effectue le nettoyage automatique des virus/spywares, le contrôle s'arrête. 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.

Exécution d'un contrôle personnalisé

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

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

   Retrouvez plus d'informations sur la page d'**Accueil** à la section *À propos de la page d'accueil*.

2. Dans la liste des **Contrôles disponibles**, sélectionnez le contrôle que vous souhaitez exécuter et cliquez sur **Démarrer**.

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

Remarque : si le contrôle détecte les composants d'une menace dans la mémoire et que vous n'avez pas paramétré ce contrôle pour qu'il effectue le nettoyage automatique des virus/spywares, le contrôle s'arrête. 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.

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

Attribution d'un nouveau nom à un contrôle personnalisé

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

   Retrouvez plus d'informations sur la page d'**Accueil** à la section *À propos de la page d'accueil*.

2. Dans la liste des **Contrôles disponibles**, sélectionnez le contrôle que vous souhaitez modifier et cliquez sur **Modifier**.
3. Dans la zone de texte **Nom du contrôle**, saisissez le nouveau nom du contrôle.

Consultation du journal du contrôle personnalisé

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

   Retrouvez plus d'informations sur la page d'**Accueil** à la section *À propos de la page d'accueil*.

2. Dans la liste des **Contrôles disponibles**, cliquez sur **Récapitulatif** pour ce contrôle personnalisé.
3. Dans la boîte de dialogue **Récapitulatif**, cliquez sur le lien présent en bas.

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

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

Consultation du récapitulatif du contrôle personnalisé

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

   Retrouvez plus d'informations sur la page d'**Accueil** à la section *À propos de la page d'accueil*.

2. Dans la liste des **Contrôles disponibles**, cliquez sur **Récapitulatif** pour ce contrôle personnalisé.

Suppression d'un contrôle personnalisé

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

   Retrouvez plus d'informations sur la page d'**Accueil** à la section *À propos de la page d'accueil*.

2. Dans la liste des **Contrôles disponibles**, sélectionnez le contrôle que vous souhaitez supprimer, puis cliquez sur **Supprimer**.

Exécution d'un contrôle intégral de l'ordinateur

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

Sur la page d'**Accueil**, sous **Antivirus et HIPS**, cliquez sur **Contrôler cet ordinateur**.

Retrouvez plus d'informations sur la page d'**Accueil** à la section *À propos de la page d'accueil*.

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

Remarque : si le contrôle détecte les composants d'une menace dans la mémoire, il s'arrête. 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.

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

À propos de la 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 runtime peut intercepter des menaces qui ne peuvent pas être détectées avant exécution. La surveillance des comportements utilise les méthodes de détection runtime suivantes pour intercepter les menaces :

- Détection des comportements malveillants et suspects
- 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 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 de la surveillance des comportements

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

Si vous êtes un membre du groupe SophosAdministrator, vous pouvez activer la surveillance des comportements.

1. Cliquez sur **Accueil** > **Antivirus et HIPS** > **Configurer l'antivirus et HIPS** > **Configuration** > **Surveillance des comportements**.
2. Dans la boîte de dialogue **Configuration de la surveillance des comportements**, sélectionnez la case **Activer la surveillance des comportements**.

Blocage des comportements malveillants

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

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.

Si vous êtes un membre du groupe SophosAdministrator, vous pouvez modifier les paramètres de détection et de signalement des comportements malveillants :

1. Cliquez sur **Accueil** > **Antivirus et HIPS** > **Configurer l'antivirus et HIPS** > **Configuration** > **Surveillance des comportements**.
2. Dans la boîte de dialogue **Configuration de la surveillance des comportements**, sélectionnez la case **Activer la surveillance des comportements**.
3. Pour alerter l'administrateur et bloquer les comportements malveillants, sélectionnez la case **Détecter les comportements malveillants**.

Prévention des comportements suspects

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

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.

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

1. Cliquez sur **Accueil** > **Antivirus et HIPS** > **Configurer l'antivirus et HIPS** > **Configuration** > **Surveillance des comportements**.
2. Dans la boîte de dialogue **Configuration de la surveillance des comportements**, sélectionnez la case **Activer la surveillance des comportements**.
3. Sélectionnez la case **Détecter les comportements malveillants**.
4. Pour alerter l'administrateur et bloquer les processus suspects, sélectionnez la case **Détecter les comportements suspects**.
5. Pour alerter l'administrateur mais ne pas bloquer les processus suspects, sélectionnez la case **Alerter uniquement, ne pas bloquer les comportements suspects**.

Pour une protection renforcée, nous vous conseillons d'effectuer un contrôle à la recherche de fichiers suspects. Pour de plus amples informations, reportez-vous aux rubriques suivantes :

- *Configuration du contrôle sur accès*

- *Configuration du contrôle par clic droit*
- *Configuration d'un contrôle personnalisé*

Prévention des dépassements de la mémoire tampon

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

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.

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

1. Cliquez sur **Accueil** > **Antivirus et HIPS** > **Configurer l'antivirus et HIPS** > **Configuration** > **Surveillance des comportements**.
2. Dans la boîte de dialogue **Configuration de la surveillance des comportements**, sélectionnez la case **Activer la surveillance des comportements**.
3. Pour alerter l'administrateur et bloquer les dépassements de la mémoire tampon, sélectionnez la case **Détecter les dépassements de la mémoire tampon**.
4. Pour alerter l'administrateur mais ne pas bloquer les dépassements de la mémoire tampon, sélectionnez la case **Alerter uniquement, ne pas bloquer**.

À propos de la protection Live Sophos

La protection Live Sophos détermine si un fichier suspect est une menace et, en cas de menace, prend immédiatement les mesures spécifiées dans la configuration du nettoyage de Sophos Anti-Virus.

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

La protection Live Sophos utilise les options suivantes :

- **Activer la protection Live**

  Si un contrôle antivirus sur un ordinateur d'extrémité a identifié un fichier comme suspect, mais ne peut pas l'identifier davantage comme sain ou malveillant d'après les fichiers d'identités des menaces (IDE) stockés sur l'ordinateur, certaines données de ce fichier (comme sa somme de contrôle ou d'autres attributs) 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.

- **Envoyer automatiquement les échantillons de fichiers à Sophos**

  Si un fichier est considéré suspect, mais ne peut pas être formellement identifié comme étant malveillant à partir de ses seules données, vous pouvez autoriser Sophos à demander un échantillon de ce fichier. Si l'option est activée et si Sophos n'a pas déjà d'échantillon de ce fichier, ce dernier sera soumis automatiquement.

L'envoi d'échantillons de fichiers à Sophos nous aide à améliorer en permanence la détection des malwares sans aucun risque de faux positifs.

Activation ou désactivation des options de la protection Live Sophos

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

Si vous êtes membre du groupe SophosAdministrator, vous pouvez activer ou désactiver les options de la protection Live Sophos :

1. Cliquez sur **Accueil** > **Antivirus et HIPS** > **Configurer l'antivirus et HIPS** > **Configuration** > **Protection Live Sophos**.
2. Dans la boîte de dialogue **Protection Live Sophos** :
    - Pour activer ou désactiver l'envoi des échantillons de fichiers à Sophos, sélectionnez ou dessélectionnez la case à cocher **Activer la protection Live**.
    - Pour activer ou désactiver l'envoi d'échantillons de fichiers à Sophos, sélectionnez ou dessélectionnez la case à cocher **Envoyer automatiquement les échantillons de fichiers à Sophos**.

      Cette option est uniquement disponible si vous avez déjà sélectionné **Activer la protection Live**.

Remarque

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

Affichage du journal de la protection Live Sophos

Les données de fichiers envoyées à Sophos en vue d'un contrôle en ligne et les mises à jour de l'état des fichiers une fois le contrôle terminé sont consignées dans le journal de contrôle de cet ordinateur.

Si la protection Live Sophos est activée, le journal affiche :

- Le chemin de chaque fichier dont les données ont été envoyées à Sophos.
- L'heure à laquelle les données ont été envoyées.
- La raison de l'échec de l'envoi des données (si elle est connue).
- L'état actuel du fichier (par exemple, “virus/spyware” si le fichier a été identifié comme malveillant).

Pour afficher le journal du contrôle :

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

  Retrouvez plus d'informations sur la page d'**Accueil** à la section *À propos de la page d'accueil*.

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

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

À propos de la protection Web Sophos

La protection Web Sophos fournit une protection étendue contre les menaces Web. Elle fonctionne en passant en revue les URL de sites Web dans la base de données en ligne Sophos de sites Web infectés, puis en bloquant l'accès à tout site Web connu pour héberger du malware.

Les navigateurs suivantes prennent en charge la protection Web :

- Internet Explorer
- Firefox
- Google Chrome
- Safari
- Opera

Lorsque l'accès à un site Web malveillant est bloqué, l'événement est enregistré dans le journal de contrôle. Pour plus d'informations sur la visualisation du journal de contrôle, reportez-vous à la section *Consultation du journal du contrôle*.

Déblocage de l'accès aux sites Web malveillants

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

Pour débloquer l'accès aux sites Web malveillants :

1. Cliquez sur **Accueil** > **Antivirus et HIPS** > **Configurer l'antivirus et HIPS** > **Configuration** > **Protection Web**.
2. Dans la liste **Bloquer l'accès aux sites Web malveillants**, cliquez sur **Inactif**.

   Pour plus d'informations sur l'autorisation d'un site Web classé comme malveillant, reportez-vous à la section *Autorisation de l'utilisation d'un site Web*.
3. Dans la liste **Contrôle des téléchargements**, cliquez sur **Inactif**, **Actif** ou **Identique au contrôle sur accès**.

   Le paramètre **Identique au contrôle sur accès** conserve vos paramètres existants du contrôle *sur accès*.

À propos de la recherche des applications contrôlées

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

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

Pour plus d'informations sur le contrôle sur accès, reportez-vous à la section *À propos du contrôle sur accès et du contrôle à la demande*.

Désactivation de la recherche des applications contrôlées

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

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

Pour désactiver la recherche des applications contrôlées :

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

Autorisation des adwares et des PUA

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

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

Pour autoriser les adwares et les PUA :

1. Cliquez sur **Accueil** > **Antivirus et HIPS** > **Configurer l'antivirus et HIPS** > **Configuration** > **Autorisation**.
2. Sur l'onglet **Adwares ou PUA**, dans la liste **Adwares ou PUA connus**, sélectionnez l'adware ou la PUA.
3. Cliquez sur **Ajouter**.

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

Remarque : vous pouvez aussi autoriser des adwares et des PUA dans le gestionnaire de quarantaine. Retrouvez plus d'informations sur la façon de procéder à la section *Traitement des adwares et des PUA en quarantaine*.

Blocage des adwares et des PUA autorisés

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

1. Cliquez sur **Accueil** > **Antivirus et HIPS** > **Configurer l'antivirus et HIPS** > **Configuration** > **Autorisation**.
2. Sur l'onglet **Adwares ou PUA**, dans la liste **Adwares ou PUA connus**, sélectionnez l'adware ou la PUA que vous souhaitez bloquer.
3. Cliquez sur **Supprimer**.

Autorisation d'éléments suspects

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

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

1. Cliquez sur **Accueil** > **Antivirus et HIPS** > **Configurer l'antivirus et HIPS** > **Configuration** > **Autorisation**.
2. Cliquez sur l'onglet correspondant au type d'élément qui a été détecté (par exemple, **Dépassement de la mémoire tampon**).
3. Dans la liste **Connus**, sélectionnez l'élément suspect.
4. Cliquez sur **Ajouter**.

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

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

- *Traitement des fichiers suspects en quarantaine*
- *Traitement des comportements suspects en quarantaine*

Préautorisation d'éléments suspects

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

Pour préautoriser un élément suspect :

1. Cliquez sur **Accueil** > **Antivirus et HIPS** > **Configurer l'antivirus et HIPS** > **Configuration** > **Autorisation**.
2. Cliquez sur l'onglet correspondant au type d'élément qui a été détecté (par exemple, **Dépassement de la mémoire tampon**).
3. Cliquez sur **Nouveau**.
4. Recherchez l'élément suspect et cliquez deux fois dessus.

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

Autorisation de l'utilisation d'un site Web

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

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

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

Pour autoriser l'utilisation d'un site Web :

1. Cliquez sur **Accueil** > **Antivirus et HIPS** > **Configurer l'antivirus et HIPS** > **Configuration** > **Autorisation**.
2. Cliquez sur l'onglet **Sites Web**.
3. Cliquez sur **Ajouter**.
4. Saisissez le nom du domaine ou l'adresse IP.

Le site Web apparaît dans la liste **Sites Web autorisés**.

À propos du gestionnaire de quarantaine

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

- Aucune option de nettoyage (nettoyer, supprimer, déplacer) n'a été choisie pour le type de contrôle qui a détecté l'élément.
- Une option de nettoyage a été choisie pour le type de contrôle qui a détecté l'élément mais l'option a échoué.
- L'élément a plusieurs infections et contient encore des menaces supplémentaires.
- La menace a seulement été partiellement détectée et un contrôle intégral de l'ordinateur est nécessaire pour la détecter totalement. Pour savoir comment procéder, reportez-vous à la rubrique *Exécution d'un contrôle intégral de l'ordinateur*.
- L'élément affiche un comportement suspect.
- L'élément est une application contrôlée.

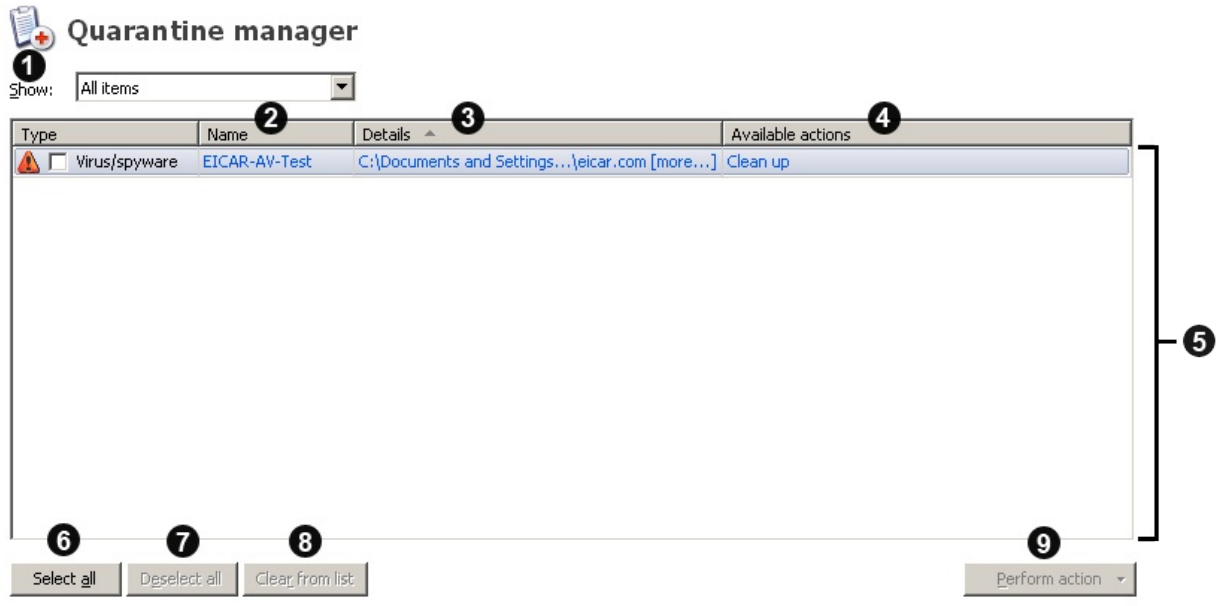
Remarque : les adwares, les PUA et les infections à plusieurs composants détectés lors du contrôle sur accès sont toujours répertoriés dans le gestionnaire de quarantaine. Le nettoyage automatique des adwares, PUA et des infections à plusieurs composants n'est pas disponible pour le contrôle sur accès.

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

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

Organisation du gestionnaire de quarantaine

Le gestionnaire de quarantaine contient tous les éléments détectés et vous permet de vous en occuper. Les éléments de la fenêtre **Gestionnaire de quarantaine** figurent ci-dessous :



1	Cliquez sur la liste **Afficher** pour filtrer le type d'éléments affichés.
2	L'identité de l'élément, y compris un lien vers son analyse sur le site Web de Sophos.
3	Le nom et l'emplacement de l'élément. Si l'élément est associé à un rootkit, il apparaît comme *Caché*. Si un lien **plus** apparaît près du nom de fichier, cela signifie que l'élément est infecté par une infection à plusieurs composants. Cliquez sur le lien pour voir la liste des autres composants faisant partie de l'infection. Si certains composants sont associés à un rootkit, la boîte de dialogue indique que certains composants sont cachés.
4	L'opération que vous pouvez exécuter pour traiter l'élément. Sauf si l'élément est caché, trois actions sont disponibles : **Nettoyer**, **Supprimer** et **Déplacer**.

	Si vous cliquez sur l'une des actions, celle-ci est effectuée immédiatement sur l'élément suite à la confirmation. Les fichiers cachés peuvent seulement être nettoyés.
❺	La liste des éléments qui ont été détectés. Pour trier les éléments, cliquez sur l'un des en-têtes de colonnes.
❻	Cliquez sur **Tout sélectionner** pour exécuter la même action sur tous les éléments. Pour dessélectionner un élément, dessélectionnez sa case à cocher dans la colonne **Type**.
❼	Si vous avez sélectionné tous les éléments et souhaitez effacer la sélection, cliquez sur **Tout dessélectionner**. Pour sélectionner un élément, cliquez sur sa case à cocher dans la colonne **Type**.
❽	Cliquez sur **Effacer de la liste** pour supprimer les éléments sélectionnés de la liste **sans** les traiter. Ceci ne supprime pas les éléments du disque.
❾	Cliquez sur **Lancer une action** pour afficher une liste d'actions que vous pouvez effectuer sur les éléments sélectionnés.

Traitement des virus/spywares en quarantaine

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

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

   Retrouvez plus d'informations sur la page d'**Accueil** à la section *À propos de la page d'accueil*.

2. Dans la liste **Afficher**, cliquez sur **Virus/spywares**.

Les informations concernant chaque élément apparaissent dans les colonnes.

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

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

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

Traitement des éléments infectés

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

Sélectionner tout/Dessélectionner tout

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

Effacer de la liste

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

Lancer une action

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

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

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

  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.

L'action disponible passe à l'état **Nettoyage** jusqu'à la fin du contrôle.

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

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

Retrouvez plus d'informations sur la manière de contacter le support technique à la section *Support technique*.

Pour configurer les actions que vous pouvez exécutez, reportez-vous à la rubrique *Configuration des droits utilisateur pour le gestionnaire de quarantaine*.

Traitement des adwares et des PUA en quarantaine

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

   Retrouvez plus d'informations sur la page d'**Accueil** à la section *À propos de la page d'accueil*.

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

Les informations concernant chaque élément apparaissent dans les colonnes.

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

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

Actions disponibles affiche les actions que vous pouvez effectuer sur l'élément. Deux actions disponibles (Autoriser et Nettoyer) sont décrites ci-dessous. Si vous cliquez sur l'une des actions, celle-ci est effectuée sur l'élément suite à la confirmation.

Traitement des adwares et des PUA

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

Sélectionner tout/Dessélectionner tout

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

Effacer de la liste

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

Lancer une action

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

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

Remarque : pour supprimer totalement de votre ordinateur certains adwares et PUA constitués de plusieurs composants ou pour nettoyer des fichiers cachés, redémarrez votre ordinateur. Si c'est le cas, vous aurez la possibilité de redémarrer votre ordinateur immédiatement ou

ultérieurement. Les étapes finales de nettoyage seront exécutées après le redémarrage de l'ordinateur.

Pour configurer les actions que vous pouvez exécuter, reportez-vous à la rubrique *Configuration des droits utilisateur pour le gestionnaire de quarantaine*.

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

Traitement des fichiers suspects en quarantaine

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

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

   Retrouvez plus d'informations sur la page d'**Accueil** à la section *À propos de la page d'accueil*.

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

Les informations concernant chaque élément apparaissent dans les colonnes.

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

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

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

Traitement des fichiers suspects

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

Sélectionner tout/Dessélectionner tout

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

Effacer de la liste

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

Lancer une action

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

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

ATTENTION : parfois, si vous supprimez ou déplacez un fichier infecté, il est possible que votre ordinateur ne fonctionne plus correctement

parce qu'il ne parvient pas à trouver le fichier.

Pour configurer les actions que vous pouvez exécuter, reportez-vous à la rubrique *Configuration des droits utilisateur pour le gestionnaire de quarantaine*.

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

Traitement des comportements suspects en quarantaine

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

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

   Retrouvez plus d'informations sur la page d'**Accueil** à la section *À propos de la page d'accueil*.

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

Les informations concernant chaque élément apparaissent dans les colonnes.

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

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

Actions disponibles affiche les actions que vous pouvez effectuer sur l'élément. Si vous avez activé le blocage de tout comportement suspect, la seule opération disponible est l'opération Autoriser décrite ci-dessous. Si vous cliquez sur l'action, celle-ci est effectuée sur l'élément suite à la confirmation.

Traitement du comportement suspect

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

Sélectionner tout/Dessélectionner tout

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

Effacer de la liste

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

Lancer une action

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

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

Pour configurer les actions que vous pouvez exécuter, reportez-vous à la rubrique *Configuration des droits utilisateur pour le gestionnaire de quarantaine*.

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

Traitement des applications contrôlées en quarantaine

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

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

   Retrouvez plus d'informations sur la page d'**Accueil** à la section *À propos de la page d'accueil*.

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

Les informations concernant chaque élément apparaissent dans les colonnes.

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

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

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

Traitement des applications contrôlées

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

Sélectionner tout/Dessélectionner tout

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

Effacer de la liste

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

À propos du nettoyage

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

- Suppression des virus/spywares à partir de secteurs de démarrage du disque, de documents, de programmes et de toute autre chose pour lesquelles un contrôle a été sélectionné
- Déplacement ou suppression du fichier suspect
- Suppression de l'élément d'adware ou de PUA

Lorsque Sophos Anti-Virus nettoie automatiquement les éléments contenant un virus/spyware, il supprime tous les éléments qui sont clairement détectés en tant que programmes malveillants et essaye de désinfecter tous les éléments qui ont été infectés. Ces fichiers désinfectés doivent être considérés comme étant définitivement endommagés, en effet le contrôle antivirus n'et pas en mesure de savoir quel était le contenu du fichier avant que celui-ci ne soit endommagé.

Nettoyage des documents

Le nettoyage des documents ne répare en aucune façon les effets secondaires du virus/spyware dans le document. Reportez-vous à la section *Informations sur le nettoyage* pour savoir comment retrouver plus de détails sur les effets secondaires du virus sur le site Web de Sophos.

Nettoyage des programmes

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

Nettoyage des menaces de page Web

Le nettoyage n'est pas requis pour les menaces détectées par le contrôle des pages web car ces menaces ne sont pas téléchargées sur votre ordinateur.

Remarque : le nettoyage d'une menace n'annulera pas forcément toutes les actions exécutées par la menace sur cet ordinateur. Par exemple, si la menace a changé la valeur du paramètre, il se peut que le processus de nettoyage ne reconnaisse pas le paramètre d'origine. Vérifiez la configuration de l'ordinateur. Le nettoyage des documents infectés ne répare pas les modifications que la menace a apportées au document.

Informations sur le nettoyage

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

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

Informations via l'alerte sur le bureau

Si le contrôle sur accès est activé sur votre ordinateur, Sophos Anti-Virus affiche une alerte sur le bureau lorsqu'une menace est trouvée.

Dans la boîte de message, cliquez sur le nom de la menace sur laquelle vous souhaitez en savoir plus. Sophos Anti-Virus vous connecte à l'analyse de la menace sur le site Web de Sophos.

Informations via la boîte de dialogue de progression du contrôle

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

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

Informations via le gestionnaire de quarantaine

1. Sur la page d'**Accueil**, sous **Antivirus et HIPS**, cliquez sur **Gérer les éléments en quarantaine**. Retrouvez plus d'informations sur la page d'**Accueil** à la section *À propos de la page d'accueil*.
2. Dans la colonne **Nom**, cliquez sur le nom de la menace sur laquelle vous souhaitez en savoir plus.

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

Configuration de la messagerie de bureau pour l'antivirus

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

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

1. Cliquez sur **Accueil** > **Antivirus et HIPS** > **Configurer l'antivirus et HIPS** > **Alertes** > **Messagerie**.
2. Dans la boîte de dialogue **Messagerie**, cliquez sur l'onglet **Messagerie de bureau**. Paramétrez les options comme décrit ci-dessous.

   Activation de la messagerie de bureau

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

   Messages à envoyer

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

   Message défini par l'utilisateur

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

   Remarque : les messages définis par l'utilisateur ne seront pas affichés sous Windows 8.

Configuration de l'alerte par courriel pour l'antivirus

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

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

1. Cliquez sur **Accueil** > **Antivirus et HIPS** > **Configurer l'antivirus et HIPS** > **Alertes** > **Messagerie**.
2. Dans la boîte de dialogue **Messagerie**, cliquez sur l'onglet **Alerte par courriel**. Paramétrez les options comme décrit ci-dessous.

   Activer les alertes par courriel

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

   Messages à envoyer

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

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

   Destinataires

   Cliquez sur **Ajouter** ou sur **Supprimer** pour respectivement ajouter ou supprimer des adresses électroniques auxquelles

les alertes par courriel doivent être envoyées. Cliquez sur **Modifier** pour changer l'adresse électronique que vous avez ajoutée.

Configurer SMTP

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

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

Configuration de la messagerie SNMP pour l'antivirus

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

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

1. Cliquez sur **Accueil** > **Antivirus et HIPS** > **Configurer l'antivirus et HIPS** > **Alertes** > **Messagerie**.
2. Dans la boîte de dialogue **Messagerie**, cliquez sur l'onglet **Messagerie SNMP**. Paramétrez les options comme décrit ci-dessous.

   Activer la messagerie SNMP

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

   Messages à envoyer

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

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

   Destination de déroutement SNMP

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

Nom de la communauté SNMP

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

Tester

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

Configuration de la journalisation des événements antivirus

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

1. Cliquez sur **Accueil** > **Antivirus et HIPS** > **Configurer l'antivirus et HIPS** > **Alertes** > **Messagerie**.
2. Dans la boîte de dialogue **Messagerie**, cliquez sur l'onglet **Journal des événements**. Paramétrez les options comme décrit ci-dessous.

   Activer la journalisation des événements

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

   Messages à envoyer

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

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

Configuration du journal du contrôle

Le journal du contrôle de cet ordinateur est archivé aux emplacements suivants :

Windows Vista, Windows 7, Windows 8, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012	C:\ProgramData\Sophos\Sophos Anti-Virus\logs\SAV.txt
Autres plates-formes Windows	C:\Documents and Settings\All Users\Application Data\Sophos\Sophos Anti-Virus\logs\SAV.txt

1. Cliquez sur **Accueil** > **Antivirus et HIPS** > **Voir le journal de l'antivirus et HIPS** > **Configurer le journal**.
2. Dans la boîte de dialogue **Configuration de la journalisation pour cet ordinateur**, définissez les options comme décrit ci-dessous.

   Niveau de journalisation

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

   Journalisation de l'archivage

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

Consultation du journal du contrôle

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

Retrouvez plus d'informations sur la page d'**Accueil** à la section *À propos de la page d'accueil*.

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

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

À propos du contrôle des périphériques sur cet ordinateur

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

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

Quels types de périphériques sont contrôlés ?

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

Stockage

- Périphériques de stockage amovible (par exemple, les clés USB à mémoire flash, les lecteurs de cartes PC et les lecteurs de disques durs externes)
- Lecteurs de supports optiques (lecteurs de CD-ROM/DVD/Blu-ray)
- Lecteurs de disquette
- Périphériques de stockage amovibles sécurisés (par exemple, les clés USB chiffrées)

Réseau

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

La stratégie de contrôle des périphériques de cet ordinateur peut être en mode **Bloquer le pont**, ce qui désactive les adaptateurs réseau sans fil ou modem lorsque l'ordinateur est connecté à un réseau physique (généralement, via une connexion Ethernet). Une fois l'ordinateur déconnecté du réseau physique, les adaptateurs réseau sans fil ou modem sont réactivés de manière transparente.

Courte portée

- Interfaces Bluetooth
- Infrarouge (interfaces infrarouge IrDA)

Supports

- MTP/PTP

Désactivation temporaire du contrôle des périphériques

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

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

Pour désactiver le contrôle des périphériques sur cet ordinateur :

1. Dans le menu **Configuration**, cliquez sur **Contrôle des périphériques**.
2. Dessélectionnez la case **Activer le contrôle des périphériques Sophos**.

Configuration du journal du contrôle des périphériques

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

Consultation du journal du contrôle des périphériques

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

Retrouvez plus d'informations sur la page d'**Accueil** à la section *À propos de la page d'accueil*.

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

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

À propos du contrôle des données sur cet ordinateur

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

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

Désactivation temporaire du contrôle des données

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

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

1. Dans le menu **Configuration**, cliquez sur **Contrôle des données**.
2. Dessélectionnez la case **Activer le contrôle des données Sophos**.

Comment ajouter un fichier dans un périphérique de stockage ?

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

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

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

Configuration du journal du contrôle des données

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

Consultation du journal du contrôle des données

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

Retrouvez plus d'informations sur la page d'**Accueil** à la section *À propos de la page d'accueil*.

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

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

À propos du contrôle du Web sur cet ordinateur

Grâce au contrôle Web de Sophos, les ordinateurs itinérants ou qui ne font pas partie du réseau d'entreprise bénéficient d'une protection, d'un contrôle et de la possibilité de créer des rapports.

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.

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

Le contrôle du Web est activé ou désactivé par une stratégie émise par une console d'administration. En revanche, si vous êtes un membre du groupe SophosAdministrator, vous pouvez désactiver temporairement le contrôle du Web sur cet ordinateur. Retrouvez plus d'informations sur la manière de procéder à la section *Désactivation temporaire du contrôle du Web*.

Désactivation temporaire du contrôle du Web

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

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

Pour désactiver le contrôle du Web sur cet ordinateur :

1. Dans le menu **Configuration**, cliquez sur **Contrôle du Web**.
2. Dessélectionnez la case **Activer le contrôle du Web**.

Introduction au pare-feu

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

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

Pare-feu administré depuis une console d'administration

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

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

Pare-feu administré depuis cet ordinateur

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

Pour plus d'informations sur la création de règles, reportez-vous à la section *À propos de la configuration du pare-feu*.

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

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

Pour plus d'informations, reportez-vous à la section *Passage en mode non interactif*.

Qu'est ce que le mode interactif ?

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

Pour plus d'informations sur le traitement des messages depuis le pare-feu, reportez-vous à la section *À propos du mode interactif*.

Le mode interactif n'est pas disponible sous Windows 8. Vous devez ajouter des règles de stratégies spécifiques pour autoriser ou bloquer les applications. Autrement, vous pouvez utiliser l'observateur des événements dans la console d'administration pour gérer les règles d'application de manière interactive.

À propos de la configuration du pare-feu

Vous pouvez configurer le pare-feu de plusieurs façons différentes puis l'activer. Par contre, si une console d'administration est utilisée pour administrer Sophos Endpoint Security and Control sur cet ordinateur, il se peut que vous perdiez tous les changements que vous avez effectués.

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

- *Activation du mode interactif*
- *Filtrage des messages ICMP*
- *Autorisation de tout le trafic sur un réseau local (LAN)*
- *Autorisation des téléchargements FTP*
- *Création d'une règle globale*
- *Autorisation d'une application*
- *Autorisation de lancement des processus cachés aux applications*
- *Autorisation d'utilisation des rawsockets aux applications*
- *Utilisation des sommes de contrôle pour authentifier les applications*

Désactivation temporaire du pare-feu

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

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

1. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Configurer le pare-feu**.

   Retrouvez plus d'informations sur la page d'**Accueil** à la section *À propos de la page d'accueil*.

2. Sous **Configurations**, sélectionnez la case **Autoriser tout le trafic** pour l'emplacement principal ou l'emplacement secondaire.

Autorisation des courriels

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

1. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Configurer le pare-feu**.

   Retrouvez plus d'informations sur la page d'**Accueil** à la section *À propos de la page d'accueil*.
2. Sous **Configurations**, cliquez sur le bouton **Configurer** correspondant à l'emplacement que vous souhaitez configurer.
3. Cliquez sur l'onglet **Applications**
4. Cliquez sur **Ajouter**, recherchez l'application de messagerie et cliquez deux fois dessus.

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

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

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

Autorisation d'utilisation d'un navigateur Web

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

1. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Configurer le pare-feu**.

   Retrouvez plus d'informations sur la page d'**Accueil** à la section *À propos de la page d'accueil*.

2. Sous **Configurations**, cliquez sur le bouton **Configurer** correspondant à l'emplacement que vous souhaitez configurer.
3. Cliquez sur l'onglet **Applications**
4. Cliquez sur **Ajouter**, recherchez l'application de navigateur Web et cliquez deux fois dessus.

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

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

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

Autorisation des téléchargements FTP

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

1. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Configurer le pare-feu**.

   Retrouvez plus d'informations sur la page d'**Accueil** à la section *À propos de la page d'accueil*.
2. Sous **Configurations**, cliquez sur le bouton **Configurer** correspondant à l'emplacement que vous souhaitez configurer.
3. Cliquez sur l'onglet **Applications**.
4. Cliquez sur **Ajouter**, recherchez l'application FTP et cliquez deux fois dessus.

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

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

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

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

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

1. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Configurer le pare-feu**.

   Retrouvez plus d'informations sur la page d'**Accueil** à la section *À propos de la page d'accueil*.

2. Sous **Configurations**, cliquez sur le bouton **Configurer** correspondant à l'emplacement que vous souhaitez configurer.

3. Sur l'onglet **Réseau local**, procédez de l'une des manières suivantes :

   - Cliquez sur **Détecter le réseau local** pour détecter le réseau local sur lequel se trouve votre ordinateur et ajoutez-le à la liste des adresses réseau.
   - Cliquez sur **Ajouter**. Dans la boîte de dialogue **Sélection de l'adresse**, sélectionnez le **Format de l'adresse**, saisissez le nom de domaine ou l'adresse IP et cliquez sur **Ajouter**.

     Remarque : si vous sélectionnez **Réseau local (détecté automatiquement)**, vous n'avez pas besoin de saisir quoi que ce soit. Cette option n'est pas disponible actuellement sous Windows 8. Retrouvez plus d'informations sur la détection du réseau local à la section *À propos de la détection du réseau local*.

4. Cliquez sur **OK** pour fermer la boîte de dialogue **Sélection de l'adresse**.

5. 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.

Autorisation de tous les partages de fichiers et d'imprimantes sur un réseau local (LAN)

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

Pour autoriser le partage de fichiers et d'imprimantes sur un réseau local (LAN) :

1. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Configurer le pare-feu**.

   Retrouvez plus d'informations sur la page d'**Accueil** à la section *À propos de la page d'accueil*.

2. Sous **Configurations**, cliquez sur le bouton **Configurer** correspondant à l'emplacement que vous souhaitez configurer.
3. Sur l'onglet **Réseau local**, procédez de l'une des manières suivantes :
   - Cliquez sur **Détecter le réseau local** pour détecter le réseau local sur lequel se trouve votre ordinateur et ajoutez-le à la liste des adresses réseau.
   - Cliquez sur **Ajouter**. Dans la boîte de dialogue **Sélection de l'adresse**, sélectionnez le **Format de l'adresse**, saisissez le nom de domaine ou l'adresse IP et cliquez sur **Ajouter**.

     Remarque : si vous sélectionnez **Réseau local (détecté automatiquement)**, vous n'avez pas besoin de saisir quoi que ce soit. Cette option n'est pas disponible actuellement sous Windows 8. Retrouvez plus d'informations sur la détection du réseau local à la section *À propos de la détection du réseau local*.

4. Cliquez sur **OK** pour fermer la boîte de dialogue **Sélection de l'adresse**.
5. Dans la liste des **Paramètres du réseau local**, sélectionnez la case **NetBIOS** pour autoriser le partage de fichiers et d'imprimantes sur un réseau local.

Retrouvez plus d'informations sur le blocage ou l'autorisation du partage de fichiers et d'imprimantes sur d'autres réseaux locaux que ceux figurant dans la liste des **Paramètres du réseau local** aux sections suivantes :

- *Blocage du partage de fichiers et d'imprimantes non désiré*
- *Autorisation d'un contrôle plus souple du partage de fichiers et d'imprimantes*

Retrouvez plus d'informations sur l'autorisation de tout le trafic sur un réseau local à la section *Autorisation de tout le trafic sur un réseau local (LAN)*.

Autorisation d'un 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 :

1. Autorisez le partage de fichiers et d'imprimantes sur d'autres réseaux locaux (LAN) que ceux figurant dans la liste **Paramètres du réseau local**. Cette opération permet aux règles de pare-feu de traiter le trafic NetBIOS sur ces réseaux locaux.
2. Créez des règles globales à haute priorité qui autorisent la communication vers/depuis les hôtes avec les ports et protocoles NetBIOS appropriés. Nous vous 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. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Configurer le pare-feu**.

   Retrouvez plus d'informations sur la page d'**Accueil** à la section *À propos de la page d'accueil*.
2. Sous **Configurations**, cliquez sur le bouton **Configurer** correspondant à l'emplacement que vous souhaitez configurer.
3. Sur l'onglet **Réseau local**, dessélectionnez la case **Bloquer le partage de fichiers et d'imprimantes pour d'autres réseaux**.

Blocage du partage de fichiers et d'imprimantes non désiré

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. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Configurer le pare-feu**.

   Retrouvez plus d'informations sur la page d'**Accueil** à la section *À propos de la page d'accueil*.

2. Sous **Configurations**, cliquez sur le bouton **Configurer** correspondant à l'emplacement que vous souhaitez configurer.
3. Sur l'onglet **Réseau local**, sélectionnez la case **Bloquer le partage de fichiers et d'imprimantes pour d'autres réseaux**.

Autorisation d'une application

1. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Configurer le pare-feu**.

   Retrouvez plus d'informations sur la page d'**Accueil** à la section *À propos de la page d'accueil*.

2. Sous **Configurations**, cliquez sur le bouton **Configurer** correspondant à l'emplacement que vous souhaitez configurer.
3. Cliquez sur l'onglet **Applications**
4. Cliquez sur **Ajouter**, recherchez l'application et cliquez deux fois dessus.

L'application est autorisée et considérée comme fiable.

Les applications 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*
- *Application de règles d'applications prédéfinies*

Blocage d'une application

1. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Configurer le pare-feu**.

   Retrouvez plus d'informations sur la page d'**Accueil** à la section *À propos de la page d'accueil*.

2. Sous **Configurations**, cliquez sur le bouton **Configurer** correspondant à l'emplacement que vous souhaitez configurer.
3. Cliquez sur l'onglet **Applications**
4. Si l'application ne figure pas dans la liste, cliquez sur **Ajouter**, recherchez l'application et cliquez deux fois dessus.
5. Sélectionnez l'application dans la liste et cliquez sur **Bloquer**.

Blocage d'IPv6

1. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Configurer le pare-feu**.

   Retrouvez plus d'informations sur la page d'**Accueil** à la section *À propos de la page d'accueil*.

2. Sous **Configurations**, cliquez sur le bouton **Configurer** correspondant à l'emplacement que vous souhaitez configurer.

3. Selon le système d'exploitation utilisé :

   - Sous Windows 7 et sous des systèmes d'exploitation plus anciens, sur l'onglet **Général**, sous **Blocage**, sélectionnez **Bloquer les paquets IPv6**.
   - Sous Windows 8, sur l'onglet **Règles globales**, sélectionnez **Bloquer tout le trafic IPv6**.

Activation ou désactivation de l'utilisation des sommes de contrôle

Si vous activez l'utilisation des sommes de contrôle pour authentifier les applications, celles-ci sont identifiées automatiquement selon leurs sommes de contrôle selon que vous les acceptiez ou les bloquiez (vous pouvez également ajouter manuellement les sommes de contrôle). 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. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Configurer le pare-feu**.

   Retrouvez plus d'informations sur la page d'**Accueil** à la section *À propos de la page d'accueil*.

2. Sous **Configurations**, cliquez sur le bouton **Configurer** correspondant à l'emplacement que vous souhaitez configurer.
3. Selon le système d'exploitation utilisé :

   - Sous Windows 7 et sous des systèmes d'exploitation plus anciens, sous le volet **Blocage**, dessélectionnez la case à cocher **Utiliser les sommes de contrôle pour authentifier les applications**.
   - Sous Windows 8, cliquez sur l'onglet **Applications**, et dessélectionnez la case à cocher **Utiliser les sommes de contrôle pour authentifier les applications**.

   Pour activer l'utilisation des sommes de contrôle pour authentifier les applications, sélectionnez la case à cocher.

Activation ou désactivation du blocage des processus modifiés

Remarque : cette option n'est pas disponible sous Windows 8 car elle est gérée automatiquement par la technologie HIPS de Sophos Anti-Virus.

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. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Configurer le pare-feu**.

   Retrouvez plus d'informations sur la page d'**Accueil** à la section *À propos de la page d'accueil*.

2. Sous **Configurations**, cliquez sur le bouton **Configurer** correspondant à l'emplacement que vous souhaitez configurer.

3. Sur l'onglet **Général**, sous **Blocage**, dessélectionnez la case **Bloquer les processus si la mémoire est modifiée par une autre application (système d'exploitation 32 bits uniquement)** pour désactiver le blocage des processus modifiés.

   Pour activer le blocage des processus modifiés, sélectionnez cette case à cocher.

Si le pare-feu détecte un processus modifié dans la mémoire, il ajoute une règle pour empêcher l'accès au réseau à ce processus modifié.

Remarques

- Nous ne conseillons pas la désactivation permanente du blocage des processus modifiés. Désactivez cette option uniquement lorsque cela est nécessaire.
- Le blocage des processus modifiés n'est pas pris en charge sur les versions 64 bits de Windows.
- Seul le processus modifié est bloqué. Le programme effectuant la modification n'est pas bloqué et a donc accès au réseau.

Filtrage des messages ICMP

Les messages ICMP (Internet Control Message Protocol) autorisent les ordinateurs d'un réseau à partager les informations sur les erreurs et sur leur état. Vous pouvez autoriser ou bloquer des types spécifiques de messages ICMP entrants ou sortants.

Filtrez uniquement les messages ICMP si vous êtes familier avec les protocoles réseau. Pour plus d'explications sur les types de message ICMP, reportez-vous à la section *Explication des types de message ICMP*.

Pour filtrer les messages ICMP :

1. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Configurer le pare-feu**.

   Retrouvez plus d'informations sur la page d'**Accueil** à la section *À propos de la page d'accueil*.

2. Sous **Configurations**, cliquez sur le bouton **Configurer** correspondant à l'emplacement que vous souhaitez configurer.
3. Cliquez sur l'onglet **ICMP**. L'interface diffère selon le système d'exploitation :
   - Sous Windows 7 et sous des systèmes d'exploitation plus anciens, sélectionnez la case **Entrant** ou **Sortant** pour autoriser les types de messages entrants ou sortants spécifiés.
   - Sous Windows 8, les types de messages ICMP sont divisés par catégories. Vous pouvez sélectionner les paramètres communs dans la liste déroulante ou cliquez sur le bouton **Détails** pour voir ou modifier les paramètres.

Explication des types de message ICMP

Rapport d'erreur sur le réseau

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.

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.

Résolution des problèmes du réseau

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**.

Adresse réseau IPv4 et configuration du routage

Rediriger
: 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 répondra par une **Annonce routeur**.

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.

Restauration des paramètres par défaut du pare-feu

1. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Configurer le pare-feu**.

   Retrouvez plus d'informations sur la page d'**Accueil** à la section *À propos de la page d'accueil*.

2. Sous **Gestion de la configuration**, cliquez sur **Valeurs par défaut**.

À propos du mode interactif

Remarque : le mode interactif n'est pas disponible sous Windows 8. Vous devez ajouter des règles de stratégies spécifiques pour autoriser ou bloquer les applications. Autrement, vous pouvez utiliser l'observateur des événements dans la console d'administration pour gérer les règles d'application de manière interactive.

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

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

- *Boîtes de dialogue d'apprentissage des processus cachés*
- *Boîtes de dialogue d'apprentissage des protocoles*
- *Boîtes de dialogue d'apprentissage des applications*
- *Boîtes de dialogue d'apprentissage des rawsockets*
- *Boîtes de dialogue d'apprentissage des sommes de contrôle*

Activation du mode interactif

1. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Configurer le pare-feu**.

   Retrouvez plus d'informations sur la page d'**Accueil** à la section *À propos de la page d'accueil*.

2. Sous **Configurations**, cliquez sur le bouton **Configurer** correspondant à l'emplacement que vous souhaitez configurer.

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

Passage en mode non interactif

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 :

1. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Configurer le pare-feu**.

   Retrouvez plus d'informations sur la page d'**Accueil** à la section *À propos de la page d'accueil*.

2. Sous **Configurations**, cliquez sur le bouton **Configurer** correspondant à l'emplacement que vous souhaitez configurer.
3. Sur l'onglet **Général**, sous **Mode de fonctionnement**, cliquez sur **Autoriser par défaut** ou sur **Bloquer par défaut**.

Boîtes de dialogue d'apprentissage des processus cachés

On parle de processus caché lorsqu'une application en lance une autre afin qu'elle lui trouve un accès au réseau. Des applications malveillantes utilisent parfois 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.

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

- *Activation des boîtes de dialogue d'apprentissage des processus cachés*

Activation des boîtes de dialogue d'apprentissage des processus cachés

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

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

Pour activer les boîtes de dialogue de processus cachés :

1. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Configurer le pare-feu**.

   Retrouvez plus d'informations sur la page d'**Accueil** à la section *À propos de la page d'accueil*.

2. Sous **Configurations**, cliquez sur le bouton **Configurer** correspondant à l'emplacement que vous souhaitez configurer.
3. Cliquez sur l'onglet **Processus**.
4. Sélectionnez la case **Avertir à propos des nouveaux lanceurs de programme**.

Boîtes de dialogue d'apprentissage des protocoles

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

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

Boîtes de dialogue d'apprentissage des applications

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

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

Boîtes de dialogue d'apprentissage des rawsockets

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

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

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

- *Activation des boîtes de dialogue d'apprentissage des rawsockets*

Activation des boîtes de dialogue d'apprentissage des rawsockets

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

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

Pour activer les boîtes de dialogue des rawsockets :

1. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Configurer le pare-feu**.

   Retrouvez plus d'informations sur la page d'**Accueil** à la section *À propos de la page d'accueil*.

2. Sous **Configurations**, cliquez sur le bouton **Configurer** correspondant à l'emplacement que vous souhaitez configurer.
3. Cliquez sur l'onglet **Processus**.
4. Sélectionnez la case **Avertir à propos de l'utilisation des rawsockets**.

Boîtes de dialogue d'apprentissage des sommes de contrôle

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

La boîte de dialogue d'apprentissage des sommes de contrôle apparaît uniquement si vous utilisez les sommes de contrôle pour authentifier les applications. Retrouvez plus d'informations à la section *Activation ou désactivation de l'utilisation des sommes de contrôle*.

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

Sélectionnez l'une des options suivantes :

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

À propos des fichiers de configuration du pare-feu

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

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

Exportation d'un fichier de configuration du pare-feu

1. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Configurer le pare-feu**.

   Retrouvez plus d'informations sur la page d'**Accueil** à la section *À propos de la page d'accueil*.

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

Importation d'un fichier de configuration du pare-feu

1. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Configurer le pare-feu**.

   Retrouvez plus d'informations sur la page d'**Accueil** à la section *À propos de la page d'accueil*.

2. Cliquez sur **Importer**.
3. Sélectionnez un fichier de configuration et cliquez sur **Ouvrir**.
4. Suivez les instructions à l'écran.

À propos des règles du pare-feu

Règles globales

Les règles globales s'appliquent à toutes les communications réseau et aux applications même si elles ont des règles d'applications.

Règles d'applications

Vous pouvez avoir une ou plusieurs règles pour une application. Vous pouvez soit utiliser des règles prédéfinies créées par Sophos soit créer des règles personnalisées qui vous procureront un contrôle précis sur l'accès autorisé à une application.

Retrouvez plus d'informations sur les paramètres des règles globales et d'applications par défaut dans l'article *http://www.sophos.com/fr-fr/support/knowledgebase/57757.aspx*.

À propos de l'ordre dans lequel les règles sont appliquées

Pour les connexions qui utilisent les rawsockets, seules les règles globales sont vérifiées.

Pour les connexions qui n'utilisent *pas* les rawsockets, de nombreuses règles sont vérifiées selon que la connexion 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 actuellement sous Windows 8.

> **Remarque :** si vous n'avez pas changé le mode de fonctionnement, le pare-feu est en mode **Bloquer par défaut**.

À propos de la détection du réseau local

Remarque : cette option n'est pas disponible actuellement sous Windows 8.

Vous pouvez affecter le réseau local de cet ordinateur à des règles de pare-feu.

Le pare-feu détermine le réseau local de cet ordinateur lorsqu'il démarre, 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 très prudents si vous utilisez des règles du réseau local dans le cadre de configurations pouvant être utilisées dans des emplacements "en dehors du bureau". Retrouvez plus d'informations à la section *Création d'une configuration secondaire*.

Création d'une règle globale

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. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Configurer le pare-feu**.

   Retrouvez plus d'informations sur la page d'**Accueil** à la section *À propos de la page d'accueil*.

2. Sous **Configurations**, cliquez sur le bouton **Configurer** correspondant à l'emplacement que vous souhaitez configurer.
3. Cliquez sur l'onglet **Règles globales**.
4. Cliquez sur **Ajouter**.
5. Sous **Nom de la règle**, saisissez un nom pour la règle.

   Le nom de la règle doit être unique dans la liste des règles. Deux règles globales ne peuvent pas avoir le même nom.

6. Sous Windows 8, sous le champ **Protocole**, sélectionnez le protocole que vous voulez utiliser.
7. Pour appliquer la règle avant toute règle d'applications ou toute règle globale à priorité normale, sélectionnez la case à cocher **Priorité plus haute que les règles d'applications**.

   Retrouvez plus d'informations sur l'ordre dans lequel les règles sont appliquées à la section *À propos de l'ordre dans lequel les règles sont appliquées*.

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**. Cette option est uniquement disponible pour les règles TCP.
    - Pour autoriser les réponses depuis l'ordinateur distant qui seront basées sur la connexion initiale, sélectionnez **Inspection dynamique**. Cette option est uniquement disponible pour les règles UDP.

    Remarque : sous Windows 8, ces options n'apparaissent 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.

Modification d'une règle globale

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

Pour modifier une règle globale :

1. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Configurer le pare-feu**.

   Retrouvez plus d'informations sur la page d'**Accueil** à la section *À propos de la page d'accueil*.

2. Sous **Configurations**, cliquez sur le bouton **Configurer** correspondant à l'emplacement que vous souhaitez configurer.
3. Cliquez sur l'onglet **Règles globales**.
4. Dans la liste **Règle**, sélectionnez la règle que vous souhaitez modifier.
5. Cliquez sur **Modifier**.

   Pour plus d'informations sur le paramétrage des règles globales, reportez-vous à la section *Création d'une règle globale*.

Copie d'une règle globale

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

1. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Configurer le pare-feu**.

   Retrouvez plus d'informations sur la page d'**Accueil** à la section *À propos de la page d'accueil*.

2. Sous **Configurations**, cliquez sur le bouton **Configurer** correspondant à l'emplacement que vous souhaitez configurer.
3. Cliquez sur l'onglet **Règles globales**.
4. Dans la liste **Règle**, sélectionnez la règle que vous souhaitez copier.
5. Cliquez sur **Copier**.

Suppression d'une règle globale

1. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Configurer le pare-feu**.

   Retrouvez plus d'informations sur la page d'**Accueil** à la section *À propos de la page d'accueil*.

2. Sous **Configurations**, cliquez sur le bouton **Configurer** correspondant à l'emplacement que vous souhaitez configurer.
3. Cliquez sur l'onglet **Règles globales**.
4. Dans la liste **Règle**, sélectionnez la règle que vous souhaitez supprimer.
5. Cliquez sur **Supprimer**.

Modification de l'ordre dans lequel les règles sont appliquées

Les règles globales sont appliquées dans l'ordre dans lequel elles apparaissent en partant du haut de la liste.

Pour modifier l'ordre dans lequel les règles globales sont appliquées :

1. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Configurer le pare-feu**.

   Retrouvez plus d'informations sur la page d'**Accueil** à la section *À propos de la page d'accueil*.
2. Sous **Configurations**, cliquez sur le bouton **Configurer** correspondant à l'emplacement que vous souhaitez configurer.
3. Cliquez sur l'onglet **Règles globales**.
4. Dans la liste **Règle**, cliquez sur la règle que vous souhaitez faire monter ou descendre dans la liste.
5. Cliquez sur **Monter** ou **Descendre**.

Application de règles d'applications prédéfinies

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. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Configurer le pare-feu**.

   Retrouvez plus d'informations sur la page d'**Accueil** à la section *À propos de la page d'accueil*.

2. Sous **Configurations**, cliquez sur le bouton **Configurer** correspondant à l'emplacement que vous souhaitez configurer.
3. Cliquez sur l'onglet **Applications**
4. Sélectionnez l'application dans la liste et cliquez sur la flèche près du bouton **Personnaliser**.
5. Passez votre curseur sur **Ajouter des règles prédéfinies** et cliquez sur une règle prédéfinie.

Création d'une règle d'applications

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

1. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Configurer le pare-feu**.

   Retrouvez plus d'informations sur la page d'**Accueil** à la section *À propos de la page d'accueil*.

2. Sous **Configurations**, cliquez sur le bouton **Configurer** correspondant à l'emplacement que vous souhaitez configurer.
3. Cliquez sur l'onglet **Applications**.
4. Sélectionnez l'application dans la liste et cliquez sur **Personnaliser**.

   Vous pouvez aussi cliquer deux fois sur l'application dans la liste.

5. Dans la boîte de dialogue **Règles d'applications**, cliquez sur **Ajouter**.
6. Sous **Nom de la règle**, saisissez un nom pour la règle.

   Le nom de la règle doit être unique dans la liste des règles. Deux règles d'applications ne peuvent pas avoir le même nom, en revanche, deux applications peuvent chacune avoir une règle portant le même nom.

7. Sous Windows 8, sous le champ **Protocole**, sélectionnez le protocole que vous voulez utiliser.
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**. Cette option est uniquement disponible pour les règles TCP.
- Pour autoriser les réponses depuis l'ordinateur distant qui seront basées sur la connexion initiale, sélectionnez **Inspection dynamique**. Cette option est uniquement disponible pour les règles UDP.

Remarque : sous Windows 8, ces options n'apparaissent 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.

Modification d'une règle d'applications

1. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Configurer le pare-feu**.

   Retrouvez plus d'informations sur la page d'**Accueil** à la section *À propos de la page d'accueil*.

2. Sous **Configurations**, cliquez sur le bouton **Configurer** correspondant à l'emplacement que vous souhaitez configurer.
3. Cliquez sur l'onglet **Applications**
4. Sélectionnez l'application dans la liste et cliquez sur **Personnaliser**.

   Vous pouvez aussi cliquer deux fois sur l'application dans la liste.

5. Dans la boîte de dialogue **Règles d'applications**, cliquez sur **Modifier**.
6. Sous **Nom de la règle**, saisissez un nom pour la règle.

   Le nom de la règle doit être unique dans la liste des règles. Deux règles d'applications ne peuvent pas avoir le même nom, en revanche, deux applications peuvent chacune avoir une règle portant le même nom.

7. Sous Windows 8, sous le champ **Protocole**, sélectionnez le protocole que vous voulez utiliser.
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**. Cette option est uniquement disponible pour les règles TCP.

- Pour autoriser les réponses depuis l'ordinateur distant qui seront basées sur la connexion initiale, sélectionnez **Inspection dynamique**. Cette option est uniquement disponible pour les règles UDP.

Remarque : sous Windows 8, ces options n'apparaissent 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.

Copie d'une règle d'applications

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

1. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Configurer le pare-feu**.

   Retrouvez plus d'informations sur la page d'**Accueil** à la section *À propos de la page d'accueil*.

2. Sous **Configurations**, cliquez sur le bouton **Configurer** correspondant à l'emplacement que vous souhaitez configurer.
3. Cliquez sur l'onglet **Applications**
4. Sélectionnez l'application dans la liste et cliquez sur **Personnaliser**.

   Vous pouvez aussi cliquer deux fois sur l'application dans la liste.

5. Dans la boîte de dialogue **Règles d'applications**, sélectionnez la règle que vous voulez copier et cliquez sur **Copier**.

Suppression d'une règle d'applications

1. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Configurer le pare-feu**.

   Retrouvez plus d'informations sur la page d'**Accueil** à la section *À propos de la page d'accueil*.

2. Sous **Configurations**, cliquez sur le bouton **Configurer** correspondant à l'emplacement que vous souhaitez configurer.
3. Cliquez sur l'onglet **Applications**.
4. Sélectionnez l'application dans la liste et cliquez sur **Personnaliser**.
5. Dans la boîte de dialogue **Règles d'applications**, sélectionnez la règle que vous voulez supprimer et cliquez sur **Supprimer**.

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

Les règles d'applications sont appliquées dans l'ordre dans lequel elles apparaissent en partant du haut de la liste.

Pour modifier l'ordre dans lequel les règles d'applications sont appliquées :

1. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Configurer le pare-feu**.

   Retrouvez plus d'informations sur la page d'**Accueil** à la section *À propos de la page d'accueil*.

2. Sous **Configurations**, cliquez sur le bouton **Configurer** correspondant à l'emplacement que vous souhaitez configurer.
3. Cliquez sur l'onglet **Applications**
4. Sélectionnez l'application dans la liste et cliquez sur **Personnaliser**.

   Vous pouvez aussi cliquer deux fois sur l'application dans la liste.

5. Dans la liste **Règle**, cliquez sur la règle que vous souhaitez faire monter ou descendre dans la liste.
6. Cliquez sur **Monter** ou **Descendre**.

Autorisation de lancement des processus cachés aux applications

Remarque : cette option n'est pas disponible sous Windows 8 car elle est gérée automatiquement par la technologie HIPS de Sophos Anti-Virus.

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.

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

Pour autoriser des applications à lancer des processus cachés :

1. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Configurer le pare-feu**.

   Retrouvez plus d'informations sur la page d'**Accueil** à la section *À propos de la page d'accueil*.
2. Sous **Configurations**, cliquez sur le bouton **Configurer** correspondant à l'emplacement que vous souhaitez configurer.
3. Cliquez sur l'onglet **Processus**.
4. Dans la zone supérieure, cliquez sur le bouton **Ajouter**.
5. Recherchez l'application et cliquez deux fois dessus.

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

- *Activation du mode interactif*
- *Activation des boîtes de dialogue d'apprentissage des*

processus cachés

Autorisation d'utilisation des rawsockets aux applications

Remarque : cette option n'est pas disponible sous Windows 8. Le pare-feu traite les rawsockets de la même manière qu'il traite les sockets ordinaires.

Certaines applications peuvent accéder au réseau par le biais des rawsockets, et ainsi avoir le contrôle sur tous les aspects des données qu'elles envoient sur le réseau.

Les applications malveillantes exploitent les rawsockets en contrefaisant leur adresse IP ou en envoyant des messages corrompus.

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

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

1. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Configurer le pare-feu**.

   Retrouvez plus d'informations sur la page d'**Accueil** à la section *À propos de la page d'accueil*.
2. Sous **Configurations**, cliquez sur le bouton **Configurer** correspondant à l'emplacement que vous souhaitez configurer.
3. Cliquez sur l'onglet **Processus**.
4. Dans la zone inférieure, cliquez sur le bouton **Ajouter**.
5. Recherchez l'application et cliquez deux fois dessus.

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

- *Activation du mode interactif*
- *Activation des boîtes de dialogue d'apprentissage des rawsockets*

Utilisation des sommes de contrôle pour authentifier les applications

Chaque version d'une application a une somme de contrôle unique. Le pare-feu peut utiliser cette somme de contrôle pour décider si une application est autorisée ou non.

Par défaut, le pare-feu vérifie la somme de contrôle de chaque application qui s'exécute. Si la somme de contrôle est inconnue ou a changé, le pare-feu la bloque ou (en mode interactif) demande à l'utilisateur ce qu'il doit faire.

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

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

1. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Configurer le pare-feu**.

   Retrouvez plus d'informations sur la page d'**Accueil** à la section *À propos de la page d'accueil*.
2. Sous **Configurations**, cliquez sur le bouton **Configurer** correspondant à l'emplacement que vous souhaitez configurer.
3. Cliquez sur l'onglet **Sommes de contrôle**.
4. Cliquez sur **Ajouter**.
5. Recherchez l'application et cliquez deux fois dessus.

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

- *Activation du mode interactif*
- *Activation des boîtes de dialogue d'apprentissage des*

processus cachés

À propos de la 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 votre ordinateur selon l'emplacement actuel de l'adaptateur réseau.

Cette fonction est généralement utilisée lorsque vous travaillez depuis chez vous sur votre ordinateur portable professionnel. Vous utilisez deux connexions réseau en même temps :

- Pour votre usage professionnel, vous vous connectez au réseau de votre entreprise par le biais d'un client VPN et d'un **adaptateur réseau virtuel**.
- Pour votre usage privé, vous vous connectez à votre 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".

Paramétrage de la connexion intuitive

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 qui sera utilisée 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**.

L'emplacement actif est affiché dans le volet **État** de la fenêtre **Sophos Endpoint Security and Control**. Si les deux configurations ont été appliquées, **Active** = **Toutes les deux**.

Important : la configuration secondaire passe du mode **Interactif** au mode **Bloquer par défaut** lorsque les deux conditions suivantes sont rencontrées :

- Les deux emplacements sont actifs.
- La configuration principale n'est *pas* interactive.

Définition des emplacements principaux

1. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Configurer le pare-feu**.

   Retrouvez plus d'informations sur la page d'**Accueil** à la section *À propos de la page d'accueil*.

2. Cliquez sur l'onglet **Détection de l'emplacement**.
3. Sous **Méthode de détection**, cliquez sur le bouton **Configurer** correspondant à la méthode que vous souhaitez utiliser pour définir vos emplacements principaux :

Option	Description
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.

4. Suivez les instructions à l'écran.

Création d'une configuration secondaire

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

1. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Configurer le pare-feu**.

   Retrouvez plus d'informations sur la page d'**Accueil** à la section *À propos de la page d'accueil*.

2. Sélectionnez la case à cocher **Ajout d'une configuration pour un second emplacement**.

Paramétrez maintenant la configuration de votre emplacement secondaire. Pour plus d'informations sur la manière de procéder, reportez-vous à la section *À propos de la configuration du pare-feu* et aux autres rubriques de la section *Configuration du pare-feu*.

ATTENTION : si cet ordinateur est un 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. Pour cette raison, nous vous conseillons d'être très vigilants lors de l'utilisation de règles de réseau local comme configurations secondaires.

Sélection de la configuration à appliquer

1. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Configurer le pare-feu**.

   Retrouvez plus d'informations sur la page d'**Accueil** à la section *À propos de la page d'accueil*.

2. Dans l'onglet **Général**, sous **Emplacement appliqué**, cliquez sur l'une des options suivantes :

Option	Description
Appliquer la configuration pour l'emplacement détecté	Le pare-feu applique soit la configuration principale, soit la configuration secondaire à chaque connexion réseau selon les paramètres de détection de la connexion intuitive selon l'emplacement (comme le décrit la section *Paramétrage de la connexion intuitive*).
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.

À propos des rapports du pare-feu

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

Modifications d'état du pare-feu

Le pare-feu signale les modifications d'état suivantes :

- Modifications du mode de fonctionnement
- Modifications de la version du logiciel
- Modifications de la configuration du pare-feu pour autoriser tout le trafic
- Modifications du pare-feu pour qu'il soit conforme à la stratégie

Lorsque vous travaillez en mode interactif, la configuration de votre pare-feu peut volontairement différer de la stratégie appliquée par la console d'administration. Dans ce cas, vous pouvez décider de ne **pas** envoyer d'alertes "Diffère de la stratégie" à la console d'administration lorsque vous modifiez certaines parties de la configuration de votre pare-feu.

Pour plus d'informations, reportez-vous à la section *Activation ou désactivation du signalement des modifications locales*.

Événements du pare-feu

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

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

Pour plus d'informations, reportez-vous à la section *Désactivation du signalement du trafic réseau inconnu*

Activation ou désactivation du signalement des modifications locales

Remarque : cette option n'est pas disponible sous Windows 8.

Si la configuration de votre pare-feu diffère de la stratégie, vous pouvez **désactiver le signalement des modifications locales**.

La désactivation du signalement des modifications locales empêche le pare-feu d'envoyer des alertes "diffère de la stratégie" à la console d'administration concernant les modifications apportées aux règles globales, aux applications, aux processus ou aux sommes de contrôle. Vous pouvez vouloir faire ceci, par exemple, lorsque vous travaillez en mode interactif, car il s'agit de paramètres qui peuvent être changés à l'aide des boîtes de dialogue d'apprentissage.

Si la configuration du pare-feu sur cet ordinateur est prévue pour être conforme à la stratégie, **activez le signalement des modifications locales**.

Pour désactiver le signalement des modifications locales :

1. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Configurer le pare-feu**.

   Retrouvez plus d'informations sur la page d'**Accueil** à la section *À propos de la page d'accueil*.

2. Sous **Configurations**, cliquez sur le bouton **Configurer** correspondant à l'emplacement que vous souhaitez configurer.

3. Dans l'onglet **Général**, sous **Rapport**, effacez la case à cocher **Afficher une alerte sur la console d'administration lors de modifications locales des règles globales, des applications, des processus ou des sommes de contrôle** pour désactiver le signalement des modifications locales.

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

Désactivation du signalement du trafic réseau inconnu

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

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

1. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Configurer le pare-feu**.

   Retrouvez plus d'informations sur la page d'**Accueil** à la section *À propos de la page d'accueil*.

2. Sous **Configurations**, cliquez sur le bouton **Configurer** correspondant à l'emplacement que vous souhaitez configurer.
3. Dans l'onglet **Général**, sous **Blocage**, sélectionnez la case à cocher **Utiliser les sommes de contrôle pour authentifier les applications**.
4. Sous **Signalement**, dessélectionnez la case à cocher **Signaler les applications et le trafic inconnus à la console d'administration**.

Désactivation du signalement des erreurs de pare-feu

Important : nous vous déconseillons de désactiver en permanence le signalement des erreurs de pare-feu. Désactivez le signalement seulement si vous avez besoin.

Pour empêcher le pare-feu de signaler les erreurs à la console d'administration :

1. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Configurer le pare-feu**.

   Retrouvez plus d'informations sur la page d'**Accueil** à la section *À propos de la page d'accueil*.

2. Sous **Configurations**, cliquez sur le bouton **Configurer** correspondant à l'emplacement que vous souhaitez configurer.
3. Dans l'onglet **Général**, sous **Signalement**, dessélectionnez la case à cocher **Signaler les erreurs à la console d'administration**.

Configuration de la messagerie de bureau

Vous pouvez contrôler les messages que le pare-feu affiche sur le bureau.

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

1. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Configurer le pare-feu**.

   Retrouvez plus d'informations sur la page d'**Accueil** à la section *À propos de la page d'accueil*.

2. Sous **Configurations**, cliquez sur le bouton **Configurer** correspondant à l'emplacement que vous souhaitez configurer.
3. Dans l'onglet **Général**, sous **Messagerie de bureau**, procédez ainsi :
   - Pour afficher les informations sur les alertes et les erreurs du pare-feu, sélectionnez la case à cocher **Afficher les alertes et les erreurs**.
   - Pour afficher les informations sur les applications et le trafic inconnus, sélectionnez la case à cocher **Afficher les applications et le trafic inconnus**.

À propos du visualiseur de journaux du pare-feu

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

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

Ouverture du visualiseur de journaux du pare-feu

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

Retrouvez plus d'informations sur la page d'**Accueil** à la section *À propos de la page d'accueil*.

Configuration de la journalisation du pare-feu

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

1. Sur la page **Accueil**, sous **Pare-feu**, cliquez sur **Configurer le pare-feu**.

   Retrouvez plus d'informations sur la page d'**Accueil** à la section *À propos de la page d'accueil*.

2. Cliquez sur l'onglet **Journal**.
3. Pour gérer la taille de la base de données du journal des événements du pare-feu, sélectionnez l'une des options suivantes :
   - Pour permettre à la base de données de croître sans limites, cliquez sur **Conserver tous les enregistrements**.
   - Pour effacer les anciens enregistrements, cliquez sur **Effacer les anciens enregistrements** et configurez les **Paramètres de nettoyage du journal**.
4. Sous **Paramètres de nettoyage du journal**, sélectionnez une ou plusieurs des options suivantes :
   - Cliquez sur la case à cocher **Supprimer les enregistrements après** et saisissez ou sélectionnez un chiffre dans la zone **Jours**.
   - Cliquez sur la case à cocher **Ne pas garder plus de** et saisissez ou sélectionnez un chiffre dans la zone **Enregistrements**.
   - Cliquez sur la case à cocher **Conserver la taille sous** et saisissez ou sélectionnez un chiffre dans la zone **Mo**.

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

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

   Retrouvez plus d'informations sur la page d'**Accueil** à la section *À propos de la page d'accueil*.

2. Dans le menu **Affichage**, cliquez sur **Disposition**.
3. Dans la boîte de dialogue **Personnalisation de la vue**, sélectionnez les éléments à cacher ou à afficher :
   - L'**Arborescence** apparaît dans le volet gauche.
   - La **Barre d'outils** apparaît en haut du visualiseur de journaux du pare-feu.
   - La **Barre de description** apparaît au-dessus des données dans le volet droit.
   - La **Barre d'état** apparaît au bas du visualiseur de journaux du pare-feu.

Personnalisation du format des données

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

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

Pour personnaliser le format des données :

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

   Retrouvez plus d'informations sur la page d'**Accueil** à la section *À propos de la page d'accueil*.
2. Dans le menu **Affichage**, cliquez sur **Personnaliser**.
3. Sélectionnez les options souhaitées.

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

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

   Retrouvez plus d'informations sur la page d'**Accueil** à la section *À propos de la page d'accueil*.

2. Cliquez sur un élément dans l'arborescence pour afficher des colonnes dans le volet des détails.
3. Dans le menu **Affichage**, sélectionnez **Ajouter/Supprimer des colonnes**.

   Vous pouvez aussi cliquer avec le bouton droit de la souris sur l'un des en-têtes de colonnes.

4. Dans la boîte de dialogue **Colonnes**, effectuez l'une des opérations suivantes :

   - Pour cacher une colonne, dessélectionnez la case lui correspondant.
   - Pour afficher une colonne, sélectionnez la case lui correspondant.

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

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

   Retrouvez plus d'informations sur la page d'**Accueil** à la section *À propos de la page d'accueil*.

2. Cliquez sur un élément dans l'arborescence pour afficher des colonnes dans le volet des détails.
3. Dans le menu **Affichage**, sélectionnez **Ajouter/Supprimer des colonnes**.

   Vous pouvez aussi cliquer avec le bouton droit de la souris sur l'un des en-têtes de colonnes.

4. Dans la boîte de dialogue **Colonnes**, cliquez sur un nom de colonne, puis cliquez sur **Vers le haut** ou **Vers le bas** pour changer la position de la colonne.

Remarques

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

Filtrage des enregistrements dans un journal de pare-feu

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

Pour filtrer les enregistrements du journal du pare-feu :

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

   Retrouvez plus d'informations sur la page d'**Accueil** à la section *À propos de la page d'accueil*.
2. Dans l'arborescence, sélectionnez un journal.
3. Dans le menu **Action**, cliquez sur **Ajouter un filtre**.
4. Suivez les instructions de l'assistant de **Filtrage**.

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

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

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

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

   Retrouvez plus d'informations sur la page d'**Accueil** à la section *À propos de la page d'accueil*.

2. Dans l'arborescence, sélectionnez un journal.
3. Cliquez avec le bouton droit de la souris sur la liste des enregistrements, puis cliquez sur **Exporter tous les enregistrements**.
4. Dans la zone **Nom du fichier**, saisissez un nom de fichier.
5. Dans la liste **Type de fichier**, cliquez sur le type de fichier désiré.

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

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

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

   Retrouvez plus d'informations sur la page d'**Accueil** à la section *À propos de la page d'accueil*.

2. Dans l'arborescence, sélectionnez un journal.
3. Sélectionnez les enregistrements que vous voulez exporter.

   Si les enregistrements se mettent à jour rapidement, dans le menu **Affichage**, dessélectionnez la case à cocher **Rafraîchir automatiquement**.

4. Dans le menu **Action**, cliquez sur **Exporter les enregistrements sélectionnés**.
5. Dans la zone **Nom du fichier**, saisissez un nom de fichier.
6. Dans la liste **Type de fichier**, cliquez sur le type de fichier désiré.

Mise à jour immédiate

Par défaut, Sophos AutoUpdate est planifié pour se mettre à jour toutes les 10 minutes si vous êtes connecté en permanence au réseau de votre entreprise, ou toutes les 60 minutes si vous êtes connecté en permanence à Internet.

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

Pour une mise à jour immédiate :

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

Planification des mises à jour

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

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

1. Dans le menu **Configuration**, cliquez sur **Mise à jour**.
2. Cliquez sur l'onglet **Planification**.
3. Sélectionnez **Activer les mises à jour automatiques**, puis saisissez la fréquence (en minutes) à laquelle Sophos AutoUpdate se mettra à jour.

   Si les fichiers mis à jour sont téléchargés depuis le réseau de votre entreprise, leurs mises à jour est effectuée par défaut toutes les 10 minutes.

   Si les fichiers mis à jour sont téléchargés via Internet à partir du serveur Sophos, Sophos AutoUpdate pourra uniquement procéder à la mise à jour toutes les 60 minutes.

Création d'une source pour les mises à jour

Si vous souhaitez que Sophos AutoUpdate se mette à jour automatiquement, vous devez spécifier l'endroit à partir duquel il doit télécharger les mises à jour.

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

   Pour télécharger les mises à jour directement depuis Sophos via Internet, sélectionnez **Sophos** dans la liste **Adresse**.
4. Dans la zone **Nom utilisateur**, saisissez le nom utilisateur du compte qui sera utilisé pour accéder au serveur de mise à jour.

   Si le nom utilisateur doit être qualifié pour indiquer le domaine, utilisez la forme *domaine**nomutilisateur*.
5. Dans le champ **Mot de passe**, saisissez le mot de passe du compte qui sera utilisé pour accéder au serveur de mise à jour.

Création d'une source alternative pour les mises à jour

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

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

   Pour télécharger les mises à jour directement depuis Sophos via Internet, sélectionnez **Sophos** dans la liste **Adresse**.
4. Dans la zone **Nom utilisateur**, saisissez le nom utilisateur du compte qui sera utilisé pour accéder au serveur de mise à jour.

   Si le nom utilisateur doit être qualifié pour indiquer le domaine, utilisez la forme *domaine**nomutilisateur*.
5. Dans le champ **Mot de passe**, saisissez le mot de passe du compte qui sera utilisé pour accéder au serveur de mise à jour.

Mise à jour via un serveur proxy

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

1. Dans le menu **Configuration**, cliquez sur **Mise à jour**.
2. Cliquez sur l'onglet **Emplacement principal** ou **Emplacement secondaire**.
3. Cliquez sur **Détails du proxy**.
4. Sélectionnez la case à cocher **Accéder à l'emplacement via un proxy**.
5. Saisissez l'**Adresse** et le numéro du **Port** du serveur proxy.
6. Saisissez un **Nom utilisateur** et un **Mot de passe** qui donnent accès au serveur proxy.

   Si le nom utilisateur doit être qualifié pour indiquer le domaine, utilisez la forme *domaine\nomutilisateur*.

Mise à jour via une connexion par modem

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

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

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

Limitation de la bande passante utilisée pour la mise à jour

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

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

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

Journalisation de l'activité de mise à jour

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

1. Dans le menu **Configuration**, cliquez sur **Mise à jour**.
2. Cliquez sur l'onglet **Journalisation**.
3. Sélectionnez la case à cocher **Enregistrer l'activité de Sophos AutoUpdate**.
4. Dans la zone **Taille maximale du journal**, tapez ou sélectionnez la taille maximale en Mo pour le journal.
5. Dans la liste **Niveau du journal**, sélectionnez **Normal** ou **Détaillé**.

   La journalisation détaillée fournit des informations sur beaucoup plus d'activités que le journal normal c'est pourquoi il prend du volume plus rapidement. Utilisez cette option seulement lorsque vous avez besoin d'un journal détaillé pour la résolution des problèmes.

Consultation du fichier journal de mise à jour

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

À propos de la protection antialtération sur cet ordinateur

La protection antialtération vous permet d'interdire aux utilisateurs non autorisés (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 la protection contre les programmes malveillants spécifiquement conçus pour corrompre le fonctionnement du système d'exploitation afin d'éviter d'être détecté. Ce type de malware sera uniquement détecté en effectuant un contrôle à la recherche de menaces et de comportements suspects. Pour plus d'informations, reportez-vous à la section Sophos Anti-Virus (chapitre 4).

Que signifie la protection antialtération pour les utilisateurs de cet ordinateur ?

SophosUsers et SophosPowerUsers

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.

Les membres de SophosUsers ou SophosPowerUsers ne peuvent pas activer ou désactiver la protection antialtération.

Pour plus d'informations sur les tâches que chaque groupe Sophos est autorisé à effectuer, reportez-vous à la section *À propos des groupes Sophos*.

SophosAdministrators

Les membres du groupe SophosAdministrator peuvent activer ou désactiver la protection antialtération.

Si une console d'administration est utilisée pour administrer Sophos Endpoint Security and Control sur cet ordinateur, la stratégie de protection antialtération définie dans la console détermine la configuration de la protection antialtération et le mot de passe. Si la protection antialtération est activée depuis la console, veuillez demander à votre administrateur de vous fournir un mot de passe si vous devez effectuer l'une des tâches mentionnées précédemment.

Si vous êtes un membre du groupe SophosAdministrator et que la protection antialtération est activée, vous devez connaître le mot de passe de la protection antialtération pour effectuer les tâches suivantes :

- Reconfigurer les paramètres du contrôle sur accès ou de la détection des comportements suspects. Pour plus d'informations, reportez-vous à la section *Saisie du mot de passe de la protection antialtération pour configurer le logiciel*.

- Désactiver la protection antialtération. Pour plus d'informations, reportez-vous à la section *Désactivation de la protection antialtération*.
- Désinstaller les composants de Sophos Endpoint Security and Control (Sophos Anti-Virus, Sophos Client Firewall, Sophos AutoUpdate, Sophos Remote Management System) via le Panneau de configuration.
- Désinstaller Sophos SafeGuard Disk Encryption à l'aide du Panneau de configuration.

Un SophosAdministrator qui ne connaît pas le mot de passe ne sera pas en mesure d'effectuer d'autres tâches à l'exception de celles mentionnées précédemment.

Si la protection antialtération est désactivée, et si le mot de passe de la protection antialtération a été défini auparavant, utilisez l'option **Authentifier l'utilisateur** pour vous identifier avant de pouvoir réactiver la protection antialtération. Toutes les autres options de configuration à disposition du groupe SophosAdministrators sont activées lorsque la protection antialtération est désactivée. Pour plus d'informations sur la réactivation de la protection antialtération, reportez-vous à la section *Réactivation de la protection antialtération*.

Activation de la protection antialtération

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

Lorsque Sophos Endpoint Security and Control est installé pour la première fois, la protection antialtération est désactivée. Si vous êtes un SophosAdministrator, vous pouvez activer la protection antialtération.

Pour activer la protection antialtération :

1. Sur la page d'**Accueil**, sous **Protection antialtération**, cliquez sur **Configurer la protection antialtération**.

   Retrouvez plus d'informations sur la page d'**Accueil** à la section *À propos de la page d'accueil*.

2. Dans la boîte de dialogue **Configuration de la protection antialtération**, sélectionnez la case **Activer la protection antialtération**.
3. Cliquez sur **Définir** sous le champ **Mot de passe**. Dans la boîte de dialogue **Mot de passe de la protection antialtération**, saisissez et confirmez le mot de passe.

   Conseil : le mot de passe doit contenir au minimum 8 caractères incluant une combinaison de chiffres et de lettres majuscules et minuscules.

Désactivation de la protection antialtération

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

Si vous êtes un membre du groupe SophosAdministrator, vous pouvez désactiver la protection antialtération.

Pour désactiver la protection antialtération :

1. Si vous ne vous êtes pas encore identifié et que l'option **Configurer la protection antialtération** est indisponible sur la page d'**Accueil**, suivez les instructions de la section *Saisie du mot de passe de la protection antialtération pour configurer le logiciel* avant de passer à l'étape 2.
2. Sur la page d'**Accueil**, sous **Protection antialtération**, cliquez sur **Configurer la protection antialtération**.

   Retrouvez plus d'informations sur la page d'**Accueil** à la section *À propos de la page d'accueil*.
3. Dans la boîte de dialogue **Configuration de la protection antialtération**, dessélectionnez la case **Activer la protection antialtération** et cliquez sur **OK**.

Réactivation de la protection antialtération

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

Si vous êtes membre du groupe SophosAdministrator, vous pouvez réactiver la protection antialtération.

Pour réactiver la protection antialtération :

1. Sur la page d'**Accueil**, sous **Protection antialtération**, cliquez sur **Authentifier l'utilisateur**.

   Retrouvez plus d'informations sur la page d'**Accueil** à la section *À propos de la page d'accueil*.
2. Dans la boîte de dialogue **Authentification de la protection antialtération** , saisissez le mot de passe de la protection antialtération et cliquez sur **OK**.
3. Sur la page d'**Accueil**, sous **Protection antialtération**, cliquez sur **Configurer la protection antialtération**.
4. Dans la boîte de dialogue **Configuration de la protection antialtération**, sélectionnez la case **Activer la protection antialtération**.

À propos du mot de passe de la protection antialtération

Lorsque la protection antialtération est activée, vous devez saisir le mot de passe de la protection antialtération pour configurer le contrôle sur accès, configurer la détection des comportements suspects ou désactiver la protection antialtération. Vous devez être un membre du groupe SophosAdministrator pour effectuer de telles opérations.

Il vous suffit de saisir le mot de passe de la protection antialtération une seule fois après avoir ouvert Sophos Endpoint Security and Control. Si vous fermez Sophos Endpoint Security and Control et le rouvrez, vous devez saisir de nouveau le mot de passe.

Si vous souhaitez désinstaller un des composants de Sophos Endpoint Security and Control, vous devez saisir le mot de passe de la protection antialtération avant de pouvoir désactiver la protection antialtération et ensuite désinstaller le logiciel.

Si la protection antialtération est désactivée, et si le mot de passe de la protection antialtération a été défini auparavant, vous devez d'abord saisir le mot de passe avant de pouvoir réactiver la protection antialtération.

Pour activer la protection antialtération, vous devez saisir le mot de passe si :

- Vous aviez déjà activé la protection antialtération, créé un mot de passe pour la protection antialtération puis désactivé la protection antialtération.
- Un mot de passe de la protection antialtération a été créé dans la console d'administration mais la protection antialtération n'est pas activée.

Saisie du mot de passe de la protection antialtération pour configurer le logiciel

Si vous êtes membre du groupe SophosAdministrator, vous pouvez vous authentifier en saisissant le mot de passe de la protection antialtération.

Pour vous authentifier :

1. Sur la page d'**Accueil**, sous **Protection antialtération**, cliquez sur **Authentifier l'utilisateur**.

   Retrouvez plus d'informations sur la page d'**Accueil** à la section *À propos de la page d'accueil*.

2. Dans la boîte de dialogue **Authentification de la protection antialtération** , saisissez le mot de passe de la protection antialtération et cliquez sur **OK**.

Changement du mot de passe de la protection antialtération

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

Vous devez être membre du groupe SophosAdministrator pour pouvoir changer le mot de passe de la protection antialtération.

Pour changer le mot de passe de la protection antialtération :

1. Si vous ne vous êtes pas encore identifié et que l'option **Configurer la protection antialtération** est indisponible sur la page d'**Accueil**, suivez les instructions de la section *Saisie du mot de passe de la protection antialtération pour configurer le logiciel* avant de passer à l'étape 2.
2. Sur la page d'**Accueil**, sous **Protection antialtération**, cliquez sur **Configurer la protection antialtération**.

   Retrouvez plus d'informations sur la page d'**Accueil** à la section *À propos de la page d'accueil*.
3. Dans la boîte de dialogue **Configuration de la protection antialtération**, cliquez sur **Changer** sous le champ **Mot de passe**.
4. 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.

Désinstallation des logiciels de sécurité Sophos

Si vous êtes membre du groupe SophosAdministrator, vous pouvez désinstaller les logiciels de sécurité Sophos via le Panneau de configuration :

- Les composants de Sophos Endpoint Security and Control (Sophos Anti-Virus, Sophos Client Firewall, Sophos AutoUpdate, Sophos Remote Management System).
- Sophos SafeGuard Disk Encryption

Pour désinstaller les logiciels de sécurité Sophos lorsque la protection antialtération est activée :

1. Sur la page d'**Accueil**, sous **Protection antialtération**, cliquez sur **Authentifier l'utilisateur**.

   Retrouvez plus d'informations sur la page d'**Accueil** à la section *À propos de la page d'accueil*.

2. Dans la boîte de dialogue **Authentification de la protection antialtération** , saisissez le mot de passe de la protection antialtération et cliquez sur **OK**.
3. Sur la page d'**Accueil**, sous **Protection antialtération**, cliquez sur **Configurer la protection antialtération**.
4. Dans la boîte de dialogue **Configuration de la protection antialtération**, dessélectionnez la case **Activer la protection antialtération** et cliquez sur **OK**.

   La protection antialtération est désactivée.

5. Dans le **Panneau de configuration**, ouvrez **Ajout/Suppression de programmes**, recherchez les logiciels que vous voulez supprimer et cliquez sur **Modifier/Supprimer** ou **Supprimer**. Suivez à l'écran les instructions de désinstallation des logiciels.

Consultation du journal de la protection antialtération

Le journal de la protection antialtération affiche deux types d'événement :

- 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.

Vous devez être membre du groupe SophosAdministrator pour pouvoir consulter le journal de la protection antialtération.

Pour consulter le journal de la protection antialtération :

Sur la page d'**Accueil**, sous **Protection antialtération**, cliquez sur **Voir le journal de la protection antialtération**.

Retrouvez plus d'informations sur la page d'**Accueil** à la section *À propos de la page d'accueil*.

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

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

À propos des échecs de la mise à jour

Pour en savoir plus sur un échec de mise à jour, consultez le journal de la mise à jour : pour plus d'informations sur la manière de procéder, reportez-vous à la section *Consultation du fichier journal de mise à jour*.

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

- *Sophos Endpoint Security and Control contacte une source incorrecte pour les mises à jour*
- *Sophos Endpoint Security and Control ne peut pas utiliser votre serveur proxy*
- *La mise à jour automatique n'est pas correctement planifiée*
- *La source des mises à jour n'est pas gérée*

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

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

   Retrouvez plus d'informations sur la configuration de l'**Emplacement principal** à la section *Création d'une source pour les mises à jour*.

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

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

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

   Retrouvez plus d'informations sur la saisie des détails du proxy à la section *Mise à jour via un serveur proxy*.

La mise à jour automatique n'est pas correctement planifiée

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

La source des mises à jour n'est pas gérée

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

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

Menace non nettoyée

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

Le nettoyage automatique est désactivé

Si Sophos Anti-Virus n'a pas tenté de nettoyage, vérifiez que le nettoyage automatique a été activé. Pour plus d'informations sur l'activation du nettoyage automatique, consultez les rubriques suivantes :

- *Configuration du nettoyage sur accès*
- *Configuration du nettoyage par clic droit*
- *Configuration du nettoyage pour un contrôle personnalisé*

Le nettoyage automatique des adwares et des PUA n'est pas disponible pour le contrôle sur accès.

Échec du nettoyage

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

Un contrôle intégral du système est nécessaire

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

1. Pour contrôler toutes les unités de disque dur, secteurs de démarrage compris, de l'ordinateur, choisissez la fonction **Contrôler cet ordinateur**. Pour plus d'informations, reportez-vous à la section *Exécution d'un contrôle intégral de l'ordinateur*.
2. Si la menace n'a pas encore été complètement détectée, c'est peut-être parce que vos droits d'accès sont insuffisants ou que certaines unités ou dossiers de votre ordinateur, contenant les composants de la menace, sont exclus du contrôle. Pour plus d'informations, reportez-vous à la section *Ajout, modification ou suppression des exclusions du contrôle sur accès*. Vérifiez la liste des éléments exclus du contrôle. Si certains éléments figurent dans la liste, supprimez-les de la liste et lancez un nouveau contrôle de l'ordinateur.

Le support amovible est protégé en écriture

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

Le volume NTFS est protégé en écriture

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

Un fragment de virus/spyware a été signalé

Sophos Anti-Virus ne nettoie pas de fragment de virus/spyware parce qu'il n'a pas trouvé de correspondance exacte du virus. Reportez-vous à la section *Fragment de virus/spyware signalé*.

Fragment de virus/spyware signalé

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

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

- *Mise à jour immédiate*
- *Exécution d'un contrôle intégral de l'ordinateur*

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

- *Support technique*

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

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

La majorité des nouveaux virus ou éléments de spywares sont fondés sur ceux déjà existants afin que les fragments de code classiques d'un virus ou d'un élément de spyware connu puissent apparaître comme nouveau. Si un fragment de virus/spyware est signalé, il est possible que Sophos Anti-Virus ait détecté un nouveau virus ou élément de spyware, qui pourrait devenir actif.

Virus corrompu

Les programmes de duplication de la majorité des virus contiennent des bogues qui provoquent une infection incorrecte des fichiers cibles. Une partie inactive du virus (il peut s'agir d'une partie importante) apparaît dans le fichier host et elle est détectée par Sophos Anti-Virus. Un virus corrompu ne peut pas se propager.

Base de données contenant un virus ou un élément de spyware

Lors de l'exécution d'un contrôle intégral de l'ordinateur, Sophos Anti-Virus peut signaler la présence d'un fragment de virus/spyware dans un fichier de base de données. Si c'est la cas, ne supprimez pas la base de données. Veuillez contacter le support technique de Sophos pour obtenir plus de conseils.

Retrouvez plus d'informations sur la manière de contacter le support technique à la section *Support technique*.

Menace partiellement détectée

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

- *Exécution d'un contrôle intégral de l'ordinateur*

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

- *Ajout, modification ou suppression des exclusions du contrôle à la demande*

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

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

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

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

Ralentissement de l'ordinateur

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

1. Cliquez sur **Contrôler cet ordinateur** pour détecter tous les composants de la PUA. Pour plus d'informations, reportez-vous à la section *Exécution d'un contrôle intégral de l'ordinateur*.

   Remarque : si, après le contrôle, l'application est partiellement détectée, reportez-vous à l'étape 2 de la rubrique *Menace partiellement détectée*.

2. Nettoyez l'adware ou la PUA de votre ordinateur. Pour savoir comment procéder, reportez-vous à la rubrique *Traitement des adwares et des PUA en quarantaine*.

Autorisation d'accès aux lecteurs avec secteurs de démarrage infectés

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

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

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

1. Cliquez sur **Accueil** > **Antivirus et HIPS** > **Configurer l'antivirus et HIPS** > **Configuration** > **Contrôle sur accès**.
2. Sur l'onglet **Contrôle**, sélectionnez la case à cocher **Permettre l'accès aux lecteurs avec secteurs de démarrage infectés**.

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

Accès impossible aux zones de Sophos Endpoint Security and Control

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

Pour plus d'informations sur les groupes d'utilisateurs Sophos, reportez-vous à la section *À propos des groupes Sophos*.

Récupération suite aux effets secondaires des virus

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

Effets secondaires des virus

Certains virus ne laissent aucun effet secondaire à traiter. D'autres peuvent avoir des effets secondaires si violents qu'ils nécessite la restauration du disque dur par vos soins.

Certains virus modifient progressivement et imperceptiblement les données. Ce type de corruption est difficile à détecter.

Actions à mener

Il est très important de lire l'analyse de la menace sur le site Web de Sophos et de vérifier soigneusement les documents après désinfection. Reportez-vous à la section *Informations sur le nettoyage* pour savoir comment voir sur le site Web de Sophos les détails sur les effets secondaires du virus.

Il est indispensable que vous disposiez de sauvegardes saines. Si vous ne disposez pas de sauvegardes, commencez à en créer afin de prévenir 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.

Retrouvez plus d'informations sur la manière de contacter le support technique à la section *Support technique*.

Guérison des effets secondaires des adwares et des PUA

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

Le système d'exploitation a été modifié

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

Utilitaires non nettoyés

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

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

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

Actions à mener

Il est très important que vous lisiez l'analyse de la menace sur le site Web de Sophos. Reportez-vous à la rubrique *Informations sur le nettoyage* pour savoir comment voir sur le site Web de Sophos les détails sur les effets secondaires d'un adware ou d'un PUA.

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

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

Retrouvez plus d'informations sur la manière de contacter le support technique à la section *Support technique*.

Erreur de mot de passe

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

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

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

Message d'erreur "Échec du service"

Symptômes

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

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

Causes

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

Résolution du problème

1. À l'aide de Windows, ouvrez les Services.
2. Procédez de l'une des manières suivantes :
    - En cas de message d'erreur `Antivirus et HIPS : échec du service`, cliquez avec le bouton droit de la souris sur **Sophos Anti-Virus** et cliquez ensuite sur **Redémarrer**.
    - En cas de message d'erreur `Pare-feu : échec du service`, cliquez avec le bouton droit de la souris sur le gestionnaire du **Sophos Client Firewall** et cliquez ensuite sur **Redémarrer**.

Remarques

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

La base de données du journal du pare-feu est corrompue

Symptôme

Lors de l'utilisation du visualiseur du journal du pare-feu, le message d'erreur suivant apparaît "La base de données du journal de Sophos Client Firewall est corrompue."

Cause

La base de données du journal des événements du pare-feu est corrompue et doit être recréée.

Résolution du problème

Vous devez être membre du groupe d'administrateurs Windows sur cet ordinateur pour effectuer cette tâche.

1. À l'aide de Windows, ouvrez les Services.
2. Cliquez avec le bouton droit de la souris sur le gestionnaire du **Sophos Client Firewall** et cliquez ensuite sur **Arrêter**.
3. À l'aide de l'Explorateur Windows, naviguez jusqu'à C:\Documents and Settings\All Users\Application Data\Sophos\Sophos Client Firewall\logs.

   Pour voir le dossier caché, vous devez afficher les fichiers et dossiers cachés dans l'Explorateur Windows.
4. Supprimez op_data.mdb.
5. Dans Services, cliquez avec le bouton droit de la souris sur le gestionnaire de **Sophos Client Firewall** et cliquez ensuite sur **Démarrer**.

Remarques

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

Glossaire

Adwares et applications potentiellement indésirables
: Un adware affiche de la publicité, comme des messages intempestifs, qui affecte la productivité des utilisateurs et l'efficacité du système. Une application potentiellement indésirable (PUA, potentially unwanted application) est une application qui n'est pas malveillante en soi mais qui est généralement inappropriée sur une majeure partie des réseaux professionnels.

Analyse comportementale runtime
: Analyse dynamique effectuée par la détection des comportements suspects et par celle des dépassements de la mémoire tampon.

Application contrôlée
: Application interdite d'exécution sur votre ordinateur par la stratégie de sécurité de votre entreprise.

Application fiable
: Application disposant de l'accès complet et inconditionnel à Internet.

Arborescence
: Vue qui contrôle quelles données la visionneuse de journaux affiche dans sa vue des données.

Barre de description
: Dans la visionneuse de journaux, barre qui apparaît au-dessus de la vue des données et qui contient le nom de l'élément couramment sélectionnée dans l'arborescence.

Bloqué
: État indiquant que l'accès réseau a été refusé à des applications (y compris des processus cachés), connexions, protocoles, messages ICMP, etc.

Boîte de dialogue d'apprentissage
: Boîte de dialogue demandant à l'utilisateur de choisir d'autoriser ou de bloquer une activité réseau lorsqu'une application inconnue en demande l'accès.

Configuration principale

Configuration du pare-feu utilisée sur le réseau d'entreprise auquel l'utilisateur se connecte pour son activité professionnelle quotidienne.

Configuration secondaire

Configuration du pare-feu utilisée lorsque les utilisateurs ne sont pas connectés au réseau d'entreprise principal mais à un autre réseau tel le réseau sans fil d'un hôtel ou d'un aéroport ou tout autre réseau d'entreprise.

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.

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.

Contrôle normal

Contrôle seulement les parties d'un fichier susceptibles d'être infectées par un virus.

Contrôle par clic droit

Contrôle d'un ou de plusieurs fichiers dans Windows Explorer ou sur le Bureau que vous lancez à l'aide d'un menu de raccourcis.

Contrôle planifié

Contrôle de l'ordinateur ou de certaines parties de ce dernier, qui s'exécute à des heures définies.

Contrôle sur accès
Votre méthode principale de protection contre les menaces. À chaque fois que vous copiez, déplacez ou ouvrez un fichier ou démarrez un programme, Sophos Anti-Virus contrôle le fichier ou le programme et lui accorde l'accès uniquement s'il ne représente aucune menace pour votre ordinateur ou si son utilisation a été autorisée.

Contrôle à la demande
Contrôle que vous lancez. Vous pouvez utiliser un contrôle à la demande pour tout contrôler, que ce soit un fichier unique ou tout fichier de votre ordinateur sur lesquels vous avez les droits de lecture.

Contrôle étendu
Contrôle toutes les parties d'un fichier.

Correspondance
Doit être égal au contenu défini dans une Liste de Contrôle de Contenu.

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.

Détection des dépassements de la mémoire tampon
Détecte les attaques par dépassement de la mémoire tampon.

Erreur de contrôle
Erreur lors du contrôle d'un fichier, par exemple l'accès refusé.

Événement de menace
Détection ou désinfection d'une menace.

Événement de pare-feu
Situation qui a lieu lorsqu'une application inconnue ou le système

d'exploitation sur un ordinateur tente de communiquer avec un autre ordinateur par le biais d'une connexion réseau d'une manière qui n'a pas été requise par les applications s'exécutant sur cet ordinateur.

Fichier d'identité virale (IDE)
Fichier qui permet à Sophos Anti-Virus de détecter et de désinfecter un virus, ver ou un cheval de Troie particulier.

Fichier suspect
Fichier qui présente une combinaison de caractéristiques qui sont généralement, mais pas exclusivement, rencontrées dans les virus.

Gestionnaire d'autorisation
Module qui vous permet d'autoriser les adwares et PUA, les fichiers suspects et les applications qui révèlent un comportement suspect et un dépassement de la mémoire tampon.

Gestionnaire de quarantaine
Module qui permet de visualiser et de traiter les éléments qui ont été placés en quarantaine.

ICMP
Abréviation de "Internet Control Message Protocol." Il s'agit d'un protocole Internet multiréseau qui fournit des corrections d'erreur et toutes autres informations concernant le traitement des paquets d'adresses IP.

Inspection dynamique (stateful)
Technologie de pare-feu qui conserve un tableau des connexions réseau TCP et UDP actives. Seuls les paquets correspondant à un état de connexion connu seront autorisés par le pare-feu. Tous les autres seront rejetés.

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.

Messagerie instantanée
Catégorie d'applications contrôlées comprenant des applications clientes de messagerie instantanée (par exemple, MSN).

Mode de fonctionnement
Paramètre qui détermine si le pare-feu agit sur consultation de l'utilisateur (mode interactif) ou automatiquement (modes non interactif).

Mode interactif
Mode dans lequel le pare-feu affiche une ou plusieurs boîtes de dialogue d'apprentissage lorsqu'il détecte du trafic réseau pour lequel il n'a pas de règle spécifiée.

Mode non interactif
Mode dans lequel le pare-feu bloque ou autorise tout le trafic réseau pour lequel il n'a pas de règle spécifiée.

Mémoire système
Mémoire agissant comme un pont entre les applications et le traitement des données proprement dit effectué au niveau des matériels. Elle est utilisée par le système d'exploitation.

NetBIOS
Abréviation de "Network Basic Input/Output System." Il s'agit d'un logiciel qui fournit une interface entre le système d'exploitation, le bus d'entrée/sortie et le réseau. Presque tous les réseaux locaux de type Windows sont basés sur NetBIOS.

Nettoyage
Le nettoyage élimine les menaces sur votre ordinateur en supprimant un virus d'un fichier ou d'un secteur de démarrage, en déplaçant ou en supprimant un fichier suspect ou en supprimant un élément d'adware ou de PUA. Il n'est pas disponible pour les menaces détectées par le contrôle des pages web car les menaces ne sont pas téléchargées sur votre ordinateur. C'est la raison pour laquelle aucune mesure n'est nécessaire.

Nettoyage automatique
Nettoyage effectué sans votre intervention ou consentement.

Nettoyage manuel

Nettoyage exécuté grâce à des désinfecteurs ou des utilitaires spéciaux, ou en supprimant des fichiers manuellement.

Paramètres de nettoyage du journal

Paramètres qui contrôlent quand les enregistrements sont supprimés.

Paramètres de processus

Paramètres qui spécifient si l'accès réseau devrait être autorisé à des processus modifiés ou cachés.

Paramètres ICMP

Paramètres spécifiant quels types de communications d'administration réseau sont autorisées.

Processus caché

Application qui lance parfois un autre processus caché afin qu'il lui trouve un accès au réseau. Des applications malveillantes peuvent utiliser cette technique pour échapper aux pare-feu : au lieu de le faire elles-mêmes, elles lancent une application fiable pour qu'elle accède au réseau.

Protection antialtération

Fonction qui empêche les utilisateurs non autorisés (administrateurs locaux et utilisateurs avec peu d'expérience technique) et les malwares inconnus de désinstaller les logiciels de sécurité de Sophos ou de les désactiver par le biais de l'interface Sophos Endpoint Security and Control.

Protection Live Sophos

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.

Protocole réseau

Ensemble de règles et de normes prévues pour permettre aux ordinateurs de se connecter les uns aux autres via un réseau et d'échanger des informations avec le moins d'erreurs possibles.

Périphérique de stockage

Périphériques de stockage amovibles (lecteurs flash USB, lecteurs PC Card et disques durs externes), lecteurs de CD/DVD, lecteurs de disquette et périphériques de stockage amovibles sécurisés (lecteurs flash USB SanDisk Cruzer Enterprise, Kingston Data Traveller, IronKey Enterprise, et IronKey Basic avec chiffrement de matériel).

Rawsocket

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

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 d'application

Règle qui s'applique uniquement aux paquets de données transférées via le réseau vers ou depuis une application donnée.

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.

Règle globale à haute priorité

Règle appliquée avant toute autre règle globale ou d'application.

Règle personnalisée

Règle créée par l'utilisateur pour spécifier les circonstances dans lesquelles l'exécution d'une application est autorisée.

Règle système

Règle appliquée à tous les applications et qui autorise ou bloque l'activité réseau d'un système de bas niveau.

Règles globales

Règles appliquées à toutes les connexions réseau et aux applications qui n'ont pas encore de règle. Leur priorité est inférieure à celles définies sur la page Réseau local. Elles sont également une priorité moins élevée que les règles d'applications (sauf mention contraire de l'utilisateur).

Somme de contrôle

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.

Spyware

Un programme qui s'installe sur l'ordinateur de l'utilisateur de manière furtive, par subterfuge et/ou par abus de la crédulité de l'utilisateur et qui envoie, sans son autorisation ou à son insu, des informations depuis cet ordinateur vers l'extérieur.

Stratégie de pare-feu

Paramètres émis par la console d'administration et que le pare-feu utilise pour surveiller la connexion de l'ordinateur à Internet et à tout autre réseau.

Système de prévention des intrusions sur l'hôte (HIPS)

Terme général désignant une analyse du comportement avant exécution et une analyse du comportement runtime.

Trafic inconnu

Accès au réseau par une application ou un service pour lequel le pare-feu n'a pas de règle.

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.

Virus non identifié

Virus pour lequel il n'existe pas d'identité spécifique.

Visionneuse de journaux

Formulaire où l'utilisateur peut voir les informations provenant d'une base de données d'événements, comme des connexions ayant été

autorisées ou bloquées, le journal système et toutes les alertes qui ont été signalées.

Voix sur IP
Catégorie d'applications contrôlées incluant des applications clientes de voix sur IP.

Vue des données
Vue qui affiche différentes données en fonction de l'élément sélectionné dans l'arborescence.

Support technique

Le support technique des produits Sophos est disponible de l'une des manières suivantes :

- Rendez-vous sur le forum de la communauté SophosTalk en anglais sur *community.sophos.com/* et recherchez d'autres utilisateurs rencontrant le même problème que le vôtre.
- Rendez-vous dans la base de connaissances du support Sophos à l'adresse *www.sophos.com/fr-fr/support.aspx*.
- Téléchargez la documentation des produits à l'adresse *www.sophos.com/fr-fr/support/documentation/*.
- Envoyez un courriel à *support@sophos.fr*, y compris le(s) numéro(s) de version du logiciel Sophos, le(s) système(s) d'exploitation et le(s) niveau(x) de correctif ainsi que le texte de tous les messages d'erreur.

Mentions légales

Apache

Les logiciels Sophos mentionnés dans le présent document peuvent inclure des programmes logiciels concédés en licence (ou en sous licence) à l'utilisateur selon les termes de la licence Apache. Une copie du contrat de licence pour chacun des logiciels inclus est disponible sur *http://www.apache.org/licenses/LICENSE-2.0*.

Common Public License

Les logiciels Sophos auxquels le présent document fait référence incluent ou peuvent inclure des programmes logiciels concédés en licence (ou en sous licence) à l'utilisateur selon les termes de la licence Common Public License (CPL), qui, entre autres droits, permettent à l'utilisateur d'avoir accès au code source. La licence CPL exige que pour tout logiciel concédé en licence sous les termes de la licence CPL, qui est distribuée sous un format de code objet, le code source soit aussi mis à disposition de ces utilisateurs sous un format de code objet. Pour chaque logiciel couvert par la licence CPL, le code source est disponible sur commande par courrier postal envoyé à Sophos, par courrier électronique envoyé à *support@sophos.fr* ou par Internet sur *http://www.sophos.com/fr-fr/support/contact-support/contact-information.aspx*. Une copie du contrat de licence pour chacun des logiciels inclus est disponible sur *http://opensource.org/licenses/cpl1.0.php*

ConvertUTF

dtoa.c

The author of this software is David M. Gay.

ICU

ICU version 1.8.1 or later

COPYRIGHT AND PERMISSION NOTICE

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, provided that the above copyright notice(s) and this permission notice appear in all copies of the Software and that both the above copyright notice(s) and this permission notice appear in supporting documentation.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR HOLDERS INCLUDED IN THIS NOTICE BE LIABLE FOR ANY CLAIM, OR ANY SPECIAL INDIRECT OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

IEEE Software Taggant Library

This software was developed by The Institute of Electrical and Electronics Engineers, Incorporated (IEEE), through the Industry Connections Security Group (ICSG) of its Standards Association. Portions of it include software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/), and those portions are governed by the OpenSSL Toolkit License.

IEEE License

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

   "This product includes software developed by the IEEE Industry Connections Security Group (ICSG)".
4. The name "IEEE" must not be used to endorse or promote products derived from this software without prior written permission from the IEEE Standards Association (stds.ipr@ieee.org).
5. Products derived from this software may not contain "IEEE" in their names without prior written permission from the IEEE Standards Association (stds.ipr@ieee.org).
6. Redistributions of any form whatsoever must retain the

following acknowledgment:

"This product includes software developed by the IEEE Industry Connections Security Group (ICSG)".

THIS SOFTWARE IS PROVIDED "AS IS" AND "WITH ALL FAULTS." IEEE AND ITS CONTRIBUTORS EXPRESSLY DISCLAIM ALL WARRANTIES AND REPRESENTATIONS, EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION: (A) THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE; (B) ANY WARRANTY OF NON-INFRINGEMENT; AND (C) ANY WARRANTY WITH RESPECT TO THE QUALITY, ACCURACY, EFFECTIVENESS, CURRENCY OR COMPLETENESS OF THE SOFTWARE.

IN NO EVENT SHALL IEEE OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES, (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

THIS SOFTWARE USES STRONG CRYPTOGRAPHY, WHICH MAY BE SUBJECT TO LAWS AND REGULATIONS GOVERNING ITS USE, EXPORTATION OR IMPORTATION. YOU ARE SOLELY RESPONSIBLE FOR COMPLYING WITH ALL APPLICABLE LAWS AND REGULATIONS, INCLUDING, BUT NOT LIMITED TO, ANY THAT GOVERN YOUR USE, EXPORTATION OR IMPORTATION OF THIS SOFTWARE. IEEE AND ITS CONTRIBUTORS DISCLAIM ALL LIABILITY ARISING FROM YOUR USE OF THE SOFTWARE IN VIOLATION OF ANY APPLICABLE LAWS OR REGULATIONS.

Info-ZIP

For the purposes of this copyright and license, ?Info-ZIP? is defined as the following set of individuals:

Mark Adler, John Bush, Karl Davis, Harald Denker, Jean-Michel Dubois, Jean-loup Gailly, Hunter Goatley, Ed Gordon, Ian Gorman, Chris Herborth, Dirk Haase, Greg Hartwig, Robert Heath, Jonathan Hudson, Paul Kienitz, David Kirschbaum, Johnny Lee, Onno van der Linden, Igor Mandrichenko, Steve P. Miller, Sergio Monesi, Keith Owens, George Petrov, Greg Roelofs, Kai Uwe Rommel, Steve Salisbury, Dave Smith, Steven M. Schweda, Christian Spieler, Cosmin Truta, Antoine Verheijen, Paul von Behren, Rich Wales, Mike White

This software is provided ?as is,? without warranty of any kind, express or implied. In no event shall Info-ZIP or its contributors be held liable for any direct, indirect, incidental, special or consequential damages arising out of the use of or inability to use this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. Redistributions of source code must retain the above copyright notice, definition, disclaimer, and this list of conditions.
2. Redistributions in binary form (compiled executables) must reproduce the above copyright notice, definition, disclaimer, and this list of conditions in documentation and/or other materials provided with the distribution. The sole exception to this condition is redistribution of a standard UnZipSFX binary (including SFXWiz) as part of a self-extracting archive; that is permitted without inclusion of this license, as long as the normal SFX banner has not been removed from the binary or disabled.
3. Altered versions?including, but not limited to, ports to new

operating systems, existing ports with new graphical interfaces, and dynamic, shared, or static library versions? must be plainly marked as such and must not be misrepresented as being the original source. Such altered versions also must not be misrepresented as being Info-ZIP releases?including, but not limited to, labeling of the altered versions with the names ?Info- ZIP? (or any variation thereof, including, but not limited to, different capitalizations), ?Pocket UnZip,? ?WiZ? or ?MacZip? without the explicit permission of Info-ZIP. Such altered versions are further prohibited from misrepresentative use of the Zip-Bugs or Info-ZIP e-mail addresses or of the Info-ZIP URL(s).

4. Info-ZIP retains the right to use the names ?Info-ZIP,? ?Zip,? ?UnZip,? ?UnZipSFX,? ?WiZ,? ?Pocket UnZip,? ?Pocket Zip,? and ?MacZip? for its own source and binary releases.

Lua

Les logiciels Sophos mentionnés dans le présent document peuvent inclure des programmes logiciels concédés en licence (ou en sous licence) à l'utilisateur selon les termes de la licence Lua. Une copie du contrat de licence pour chaque logiciel inclus est disponible sur *http://www.lua.org/copyright.html*

Logiciels Microsoft

Ce produit Sophos peut inclure certains logiciels Microsoft que Sophos a sous licence pour intégration et utilisation dans ce produit.

mt19937ar.c

OpenSSL cryptographic toolkit

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL license

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

   ?This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)?
4. The names ?OpenSSL Toolkit? and ?OpenSSL Project? must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called ? OpenSSL? nor may ?OpenSSL? appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the

following acknowledgment:

?This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit.

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ?AS IS? AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay license

Copyright © 1995?1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscape?s SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young?s, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   ?This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)?

   The word ?cryptographic? can be left out if the routines from the library being used are not cryptographic related :-).
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

   ?This product includes software written by Tim Hudson (tjh@cryptsoft.com)?

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ?AS IS? AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS

OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License.]

Simple ECMAScript Engine

SQLCipher

strcasestr.c

This code is derived from software contributed to Berkeley by Chris Torek.

Unicode

UNICODE, INC. LICENSE AGREEMENT ? DATA FILES AND SOFTWARE

Unicode Data Files include all data files under the directories http://www.unicode.org/Public/, http://www.unicode.org/reports/, and http://www.unicode.org/cldr/data/. Unicode Software includes any source code published in the Unicode Standard or under the directories http://www.unicode.org/Public/, http://www.unicode.org/reports/, and http://www.unicode.org/cldr/data/.

NOTICE TO USER: Carefully read the following legal agreement. BY DOWNLOADING, INSTALLING, COPYING OR OTHERWISE USING UNICODE INC.'S DATA FILES ("DATA FILES"), AND/OR SOFTWARE ("SOFTWARE"), YOU UNEQUIVOCALLY ACCEPT, AND AGREE TO BE BOUND BY, ALL OF THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE, DO NOT DOWNLOAD, INSTALL, COPY, DISTRIBUTE OR USE THE DATA FILES OR SOFTWARE.

COPYRIGHT AND PERMISSION NOTICE

Permission is hereby granted, free of charge, to any person obtaining a copy of the Unicode data files and any associated documentation (the "Data Files") or Unicode software and any associated documentation (the "Software") to deal in the Data Files or Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, and/or sell copies of the Data Files or Software, and to permit persons to whom the Data Files or Software are furnished to do so, provided that (a) the above copyright notice(s) and this permission notice appear with all copies of the Data Files or Software, (b) both the above copyright notice(s) and this permission notice appear in associated documentation, and (c) there is clear notice in each modified Data File or in the Software as well as in the documentation associated with the Data File(s) or Software that the data or software has been modified.

UnRAR

The source code of UnRAR utility is freeware. This means:

1. All copyrights to RAR and the utility UnRAR are exclusively owned by the author - Alexander Roshal.
2. The UnRAR sources may be used in any software to handle RAR archives without limitations free of charge, but cannot be used to re-create the RAR compression algorithm, which is proprietary. Distribution of modified UnRAR sources in separate form or as a part of other software is permitted, provided that it is clearly stated in the documentation and source comments that the code may not be used to develop a RAR (WinRAR) compatible archiver.
3. The UnRAR utility may be freely distributed. It is allowed to distribute UnRAR inside of other software packages.
4. THE RAR ARCHIVER AND THE UnRAR UTILITY ARE DISTRIBUTED ?AS IS?. NO WARRANTY OF ANY KIND IS EXPRESSED OR IMPLIED. YOU USE AT YOUR OWN RISK. THE AUTHOR WILL NOT BE LIABLE FOR DATA LOSS, DAMAGES, LOSS OF PROFITS OR ANY OTHER KIND OF LOSS WHILE USING OR MISUSING THIS SOFTWARE.
5. Installing and using the UnRAR utility signifies acceptance of these terms and conditions of the license.
6. If you don?t agree with terms of the license you must remove UnRAR files from your storage devices and cease to use the utility.

Thank you for your interest in RAR and UnRAR.

Alexander L. Roshal