

SOPHOS

Sophos Helpdesk Console manuel utilisateur

Date du document : février 2008



Table des matières

1	Présentation de Helpdesk Console.....	4
2	Comment protéger les ordinateurs ?.....	9
3	Comment m'assurer que mon réseau est protégé ?.....	15
4	Comment mettre à jour les ordinateurs ?.....	22
5	Comment m'assurer que les ordinateurs sont en conformité avec les stratégies ?.....	22
6	Comment effectuer le contrôle des ordinateurs ?.....	23
7	Comment gérer les alertes ?.....	24
8	Comment nettoyer les ordinateurs ?.....	29
9	Comment générer des rapports ?.....	31
10	Résolution des problèmes.....	40
11	Glossaire.....	45

1 Présentation de Helpdesk Console

Sophos Helpdesk Console permet au personnel du service d'assistance informatique de surveiller et de gérer les logiciels Sophos.

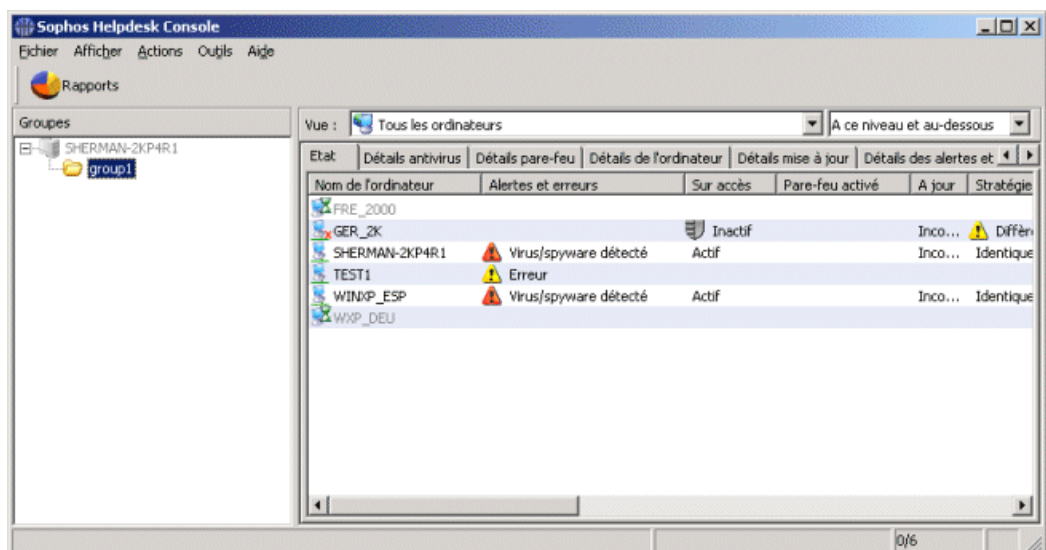
Grâce à Helpdesk Console, vous pouvez administrer des groupes d'ordinateurs auxquels votre administrateur réseau vous a donné accès. Vous pouvez protéger des ordinateurs, vous assurer qu'ils sont à jour, voir toutes les menaces, menaces potentielles ou applications indésirables détectées et les nettoyer.

Cette section vous donne un aperçu de l'interface et des fonctions principales de Helpdesk Console.

- [A propos de l'interface](#)
- [Qu'est-ce qu'un groupe ?](#)
- [Qu'est-ce qu'une stratégie ?](#)
- [Que signifient les icônes ?](#)

A propos de l'interface

Les fonctionnalités principales de l'interface de Helpdesk Console sont décrites ci-dessous.



Le volet Groupes

Dans le volet **Groupes** figurent les groupes d'ordinateurs que vous pouvez administrer. Sélectionnez un groupe pour afficher une liste des ordinateurs.



Votre administrateur a décidé quels groupes d'ordinateurs vous pouvez voir depuis Helpdesk Console. Si vous pensez que vous avez besoin d'accéder à différents groupes, contactez l'administrateur.

La liste des ordinateurs

La liste des ordinateurs (volet de droite) affiche les ordinateurs appartenant au groupe sélectionné.



Si vous avez des ordinateurs Linux administrés depuis la console, assurez-vous qu'un nom d'hôte unique est configuré pour chaque ordinateur. Autrement, chaque ordinateur apparaîtra dans la console avec le nom par défaut "localhost."


L'onglet **Etat** indique si les ordinateurs sont protégés par le contrôle sur accès, si le pare-feu est activé et si le logiciel est mis à jour. Cette page indique aussi la présence d'alertes. Les autres onglets fournissent des informations plus détaillées sur chacun de ces sujets.

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

La barre d'outils

Rapports vous permet de générer des rapports concernant les alertes sur vos réseaux.

Qu'est-ce qu'un groupe ?

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

Votre administrateur décide quels groupes d'ordinateurs vous pouvez administrer depuis Helpdesk Console. Si vous pensez que vous avez besoin d'accéder à différents groupes, contactez l'administrateur.

Chaque groupe dispose de paramètres pour la mise à jour, la protection antivirale et HIPS, la protection pare-feu et le contrôle des

applications. Tous les ordinateurs d'un groupe doivent généralement utiliser ces paramètres aussi appelés une "stratégie".

Un groupe peut contenir des sous-groupes.

Qu'est-ce qu'une stratégie ?

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

L'administrateur réseau crée les stratégies. En tant qu'utilisateur de Helpdesk Console, vous ne pouvez ni créer, ni modifier de stratégies, en revanche, vous pouvez vous assurer que les ordinateurs sont en conformité avec les stratégies créées par l'administrateur.

Les stratégies sont comme suit.

- La stratégie de **Mise à jour** définit la manière dont les ordinateurs sont mis à jour avec les nouveaux logiciels.
- La stratégie **Antivirus et HIPS** définit la manière dont Sophos Anti-Virus effectue des contrôles à la recherche de virus, de chevaux de Troie, de vers, de spywares, d'adwares et d'autres applications potentiellement indésirables connus et inconnus et détecte des comportements et des fichiers suspects. Elle permet de définir aussi comment Sophos Anti-Virus nettoie les ordinateurs.
- La stratégie de **Contrôle des applications** définit la manière dont Sophos Anti-Virus gère les applications que vous voulez contrôler.
- La stratégie de **Pare-feu** définit la manière dont Sophos Client Firewall assure la protection des ordinateurs.



Que signifient les icônes ?

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

- les alertes
- une protection désactivée ou obsolète
- l'état de chaque ordinateur, par exemple, si le logiciel est en cours

d'installation ou non.

Alertes

Symbole	Explication
	L'apparition d'un signal d'avertissement rouge dans la colonne Alertes et erreurs signifie qu'un virus, un ver, un cheval de Troie, un spyware ou un comportement suspect a été détecté.
	L'apparition d'un signal d'avertissement jaune dans la colonne Alertes et erreurs indique l'un des problèmes suivants : <ul style="list-style-type: none"> • Un fichier suspect a été détecté. • Un adware ou toute autre application potentiellement indésirable a été détecté. • Une application contrôlée a été détectée. • Le pare-feu a bloqué une application. • Une erreur a eu lieu. <p>L'apparition d'un signal d'avertissement jaune dans les colonnes Stratégie antivirus et HIPS, Stratégie de pare-feu, Stratégie de mise à jour ou Stratégie de contrôle des applications signifie que l'ordinateur n'utilise pas les mêmes stratégies que les autres ordinateurs de son groupe.</p>




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

Priorité des alertes







1. Alertes de virus/spyware
2. Alertes de comportement suspect
3. Alertes de fichiers suspects
4. Alertes de pare-feu

5. Alertes d'adwares/PUA
6. Alertes des applications contrôlées
7. Erreurs de Sophos Anti-Virus, de mise à jour et de Sophos Client Firewall

Protection désactivée ou non à jour

Symbole	Explication
	Un bouclier gris signifie que le contrôle sur accès est inactif.
	L'icône pare-feu gris signifie que le pare-feu est désactivé.
	L'icône horloge signifie que le logiciel n'est pas à jour.

Etat de l'ordinateur

Symbole	Explication
	Un symbole affichant un ordinateur bleu signifie que l'ordinateur est géré par Helpdesk Console.
	Un symbole avec un ordinateur et une flèche jaune signifie que l'installation des logiciels antivirus et pare-feu est en attente.
	Un symbole avec un ordinateur et une flèche verte signifie que l'installation est en progrès.
	Un symbole avec un ordinateur et un sablier signifie que le composant de mise à jour automatique de Sophos Anti-Virus a été installé et qu'il est désormais en train de télécharger la plus récente version du produit.
	Un symbole affichant un ordinateur gris signifie que l'ordinateur est géré par Helpdesk Console.
	Un symbole affichant un ordinateur avec une croix rouge signifie que l'ordinateur est déconnecté.

2 Comment protéger les ordinateurs ?

Cette section décrit comment installer Sophos Anti-Virus et Sophos Client Firewall sur les ordinateurs en réseau.

- [Protection des ordinateurs](#)
- [Protection des ordinateurs nécessitant une installation manuelle](#)
- [Protection des ordinateurs avec un script de connexion](#)
- [Ajout du pare-feu aux ordinateurs protégés](#)

Protection des ordinateurs

Protégez les ordinateurs Windows automatiquement de la manière suivante.



L'installation automatique n'est pas possible sur les ordinateurs Windows 95/98/Me. Utilisez plutôt l'[installation manuelle](#).

1. Sélectionnez le ou les ordinateurs. Cliquez avec le bouton droit de la souris et sélectionnez **Protéger les ordinateurs**. L'Assistant de protection des ordinateurs se lance.
2. Sur la page de **Bienvenue** de l'assistant, cliquez sur **Suivant**.
3. Sur la page **Sélection des logiciels de sécurité**, sélectionnez le logiciel que vous désirez.

Sophos Client Firewall est uniquement disponible s'il est inclus dans votre licence, et seulement pour Windows 2000 ou supérieur. Vous ne pouvez pas installer le pare-feu sur des ordinateurs fonctionnant sous des systèmes d'exploitation de type serveur.

Cliquez sur **Suivant**.

4. Sur la page **Récapitulatif de la protection**, tout problème rencontré avec l'installation figure dans la colonne **Problèmes de protection**. Reportez-vous à la section [Résolution des problèmes](#) ou procédez à une [installation manuelle](#) de ces ordinateurs. Cliquez sur **Suivant**.
5. Sur la page **Codes d'accès**, saisissez les détails d'un compte qui

peut être utilisé pour installer le logiciel. Généralement, ce compte est un compte d'administrateur de domaine. Il doit impérativement :

- § posséder les droits administrateur sur les ordinateurs que vous souhaitez protéger
- § pouvoir se connecter à l'ordinateur sur lequel vous avez installé le serveur d'administration
- § avoir un accès en lecture à l'emplacement Serveur principal spécifié dans la stratégie de **Mise à jour**.



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

Protection des ordinateurs nécessitant une installation manuelle

Si Helpdesk Console n'arrive pas à effectuer l'installation automatique du logiciel antivirus ou du pare-feu sur certains ordinateurs, effectuez l'installation manuellement.

Ainsi, si les ordinateurs sont dans un groupe ou des groupes, Helpdesk Console administrera et mettra à jour ces installations.



Autrement, vous pouvez effectuer l'installation automatiquement à l'aide d'un script. Reportez-vous à la section Protection des ordinateurs avec un script de connexion.



Si vous avez une version antérieure de Sophos Anti-Virus sur Windows 95, 98 ou Me, vous devez impérativement la désinstaller avant de procéder à l'installation de la dernière version.

Pour une installation manuelle, procédez comme suit.

1. Dans Helpdesk Console, sélectionnez le ou les ordinateurs sur lequel ou lesquels vous désirez effectuer une installation manuelle. Cliquez sur l'onglet **Détails mise à jour** et observez la colonne **Serveur principal**. Le répertoire à partir duquel chaque ordinateur se mettra à jour est affiché.

Si vous utilisez les répertoires par défaut, les dossiers à partir desquels chaque produit est installé et mis à jour sont les suivants :

Sophos Endpoint Security and Control pour Windows 2000/XP/2003/Vista	\\Nomserveur\InterChk\SAVSCFXP
Sophos Anti-Virus pour Windows 2000/XP/2003/Vista	\\Nomserveur\InterChk\ESXP
Sophos Anti-Virus pour Windows NT	\\Nomserveur\InterChk\ESNT
Sophos Anti-Virus pour Windows 95/98/Me	\\Nomserveur\InterChk\ES9x
Sophos Anti-Virus pour Mac OS X	\\Nomserveur\InterChk\ESOSX
Sophos Anti-Virus pour Linux	\\Nomserveur\InterChk\savlinux



Le répertoire de "Sophos Endpoint Security and Control" contient le programme d'installation de Sophos Anti-Virus et de Sophos Client Firewall.

2. Rendez-vous sur l'ordinateur et naviguez jusqu'au répertoire depuis lequel il se mettra à jour.

Sur un ordinateur **Windows**, cliquez deux fois sur setup.exe.

Pour protéger les ordinateurs Windows 2000 ou supérieur avec le pare-feu et le logiciel antivirus, ouvrez une invite de commande et exécutez setup.exe avec le bon qualificatif :
 setup.exe -sav installe uniquement l'antivirus
 setup.exe -scf installe l'antivirus et le pare-feu

Sur un ordinateur **Mac OS X**, cliquez deux fois sur Sophos Anti-Virus.mpkg.

Sur un ordinateur **Linux**, installez Sophos Anti-Virus à l'aide du package de distribution comme décrit dans le *Guide de démarrage réseau Sophos Endpoint Security and Control*.



Si vous avez des ordinateurs Linux administrés depuis la console, assurez-vous qu'un nom d'hôte unique est configuré pour chaque ordinateur. Autrement, chaque ordinateur apparaîtra dans la console avec le nom par défaut "localhost."

Protection des ordinateurs avec un script de connexion

Vous pouvez protéger les ordinateurs avec le logiciel antivirus (et avec le pare-feu s'il est inclus dans votre licence) en exécutant le programme d'installation avec un script ou un programme comme Microsoft SMS.



Ainsi, si les ordinateurs sont dans un groupe ou des groupes, Helpdesk Console administrera et mettra à jour ces installations.

Cette page décrit :

- La recherche du programme d'installation requis
- La protection des ordinateurs Windows 2000 ou supérieur
- La protection des ordinateurs Windows 95/98/Me
- La protection des ordinateurs Mac OS X
- La protection des ordinateurs Linux

La recherche du programme d'installation requis

Le programme d'installation se trouve dans le répertoire qui contient les mises à jour Sophos. Pour vérifier de quel répertoire il s'agit, parcourez la liste des ordinateurs et recherchez le ou les ordinateurs que vous désirez protéger. Cliquez sur l'onglet **Détails mise à jour** et observez la colonne **Serveur principal**.

Si vous utilisez les répertoires par défaut, les dossiers à partir desquels chaque produit est installé et mis à jour sont les suivants :

Sophos Endpoint Security and Control pour Windows 2000/XP/2003/Vista	\\Nomserveur\InterChk\SAVSCFXP
Sophos Anti-Virus pour Windows 2000/XP/2003/Vista	\\Nomserveur\InterChk\ESXP
Sophos Anti-Virus pour Windows NT	\\Nomserveur\InterChk\ESNT
Sophos Anti-Virus pour Windows 95/98/Me	\\Nomserveur\InterChk\ES9x
Sophos Anti-Virus pour Mac OS X	\\Nomserveur\InterChk\ESOSX
Sophos Anti-Virus pour Linux	\\Nomserveur\InterChk\savlinux



Le répertoire de "Sophos Endpoint Security and Control" contient le programme d'installation de Sophos Anti-Virus et de Sophos Client Firewall.

La protection des ordinateurs Windows 2000 ou supérieur

Si vous désirez protéger les ordinateurs Windows 2000 ou version supérieure avec le pare-feu ainsi qu'avec le logiciel antivirus, vous devez procéder comme suit :

- Assurez-vous que vous utilisez le bon programme d'installation. Il s'agit du programme d'installation de Sophos Endpoint Security and Control qui se trouve dans le répertoire nommé SAVSCFXP.
- Exécutez le programme d'installation à l'aide du qualificatif -scf.

La protection des ordinateurs Windows 95/98/Me

Pour protéger les ordinateurs Windows 95/98/Me avec un script de connexion, procédez comme suit.

1. Si vous ne savez pas déjà où il se trouve, recherchez l'emplacement du répertoire qui contient le programme d'installation.
2. Ajoutez au script de connexion la ligne suivante :

```
[Chemin]\setup.exe -user [domaine\nom] -pwd [mot de passe] -login -s
```

où [Chemin] est l'emplacement du répertoire contenant le programme d'installation (par exemple, \\Nomserveur\InterChk\ES9x), et les nom utilisateur et mot de passe sont pour un compte capable de se connecter à vos ordinateurs Windows 95/98/Me, avec un accès en lecture au partage du CID (dans cet exemple, \\Nomserveur\InterChk).



Si vous avez des ordinateurs Windows 95, vous devez exécuter un utilitaire sur ceux-ci avant d'effectuer l'installation. A partir du CD-ROM Sophos Endpoint Security and Control Network Install CD, copiez le fichier Tools/Utils/w95ws2setup.exe sur votre serveur. Puis, insérez une ligne au script de connexion, avant la ligne affichée ci-dessus, pour exécuter cet utilitaire.

Le compte utilisateur que vous spécifiez doit impérativement

- § pouvoir se connecter aux ordinateurs que vous désirez protéger
- § posséder les droits administrateur sur les ordinateurs que vous souhaitez protéger
- § avoir un accès en lecture à l'emplacement Serveur principal

spécifié dans la stratégie de Mise à jour.



Si vous ne désirez pas administrer les ordinateurs avec Helpdesk Console, ajoutez le paramètre -mng no

À la prochaine connexion de vos utilisateurs, leurs ordinateurs installeront le logiciel antivirus.

La protection des ordinateurs Mac OS X

Pour les ordinateurs Mac OS X, utilisez Apple Remote Desktop. Allez dans le répertoire d'installation centralisée et copiez le programme d'installation sur l'ordinateur exécutant Apple Remote Desktop avant de l'utiliser.

La protection des ordinateurs Linux

Pour de plus amples informations sur l'installation de Sophos Anti-Virus sur des ordinateurs Linux, reportez-vous au *Guide de démarrage de Sophos Anti-Virus pour Linux*.



Si vous avez des ordinateurs Linux administrés depuis la console, assurez-vous qu'un nom d'hôte unique est configuré pour chaque ordinateur. Autrement, chaque ordinateur apparaîtra dans la console avec le nom par défaut "localhost."

Ajout du pare-feu aux ordinateurs protégés

Si vous avez déjà protégé vos ordinateurs avec Sophos Anti-Virus, vous pouvez installer Sophos Client Firewall sur ceux-ci à condition que le pare-feu soit inclus dans votre licence.



Le pare-feu peut uniquement être installé sur les ordinateurs exécutant Windows 2000 ou supérieur.



Vous ne pouvez pas installer le pare-feu sur des ordinateurs fonctionnant sous des systèmes d'exploitation de type serveur.

1. Sélectionnez le ou les ordinateurs sur lesquels vous souhaitez installer le pare-feu. Cliquez avec le bouton droit de la souris et sélectionnez **Protéger les ordinateurs**. Un assistant se lance.

2. Sur la page de **Bienvenue** de l'assistant, cliquez sur **Suivant**.
3. Sur la page **Sélection des logiciels de sécurité**, sélectionnez **Installer Sophos Client Firewall**.
4. Sur la page **Récapitulatif de la protection**, tout problème rencontré avec l'installation figure dans la colonne **Problèmes de protection**. Reportez-vous à la section Résolution des problèmes ou procédez à une installation manuelle de ces ordinateurs. Cliquez sur **Suivant**.
5. Sur la page **Codes d'accès**, saisissez les détails d'un compte qui peut être utilisé pour installer le logiciel. Généralement, ce compte est un compte d'administrateur de domaine.

3 Comment m'assurer que mon réseau est protégé ?

Cette section vous explique comment vous assurer que les ordinateurs sont correctement protégés. Elle vous indique aussi comment identifier les ordinateurs ayant un problème à l'aide des filtres de la liste des ordinateurs et quelle action à entreprendre pour résoudre le problème.

- Quels ordinateurs sont protégés ?
- Quels ordinateurs sont à jour ?
- Recherche des ordinateurs non protégés
- Recherche des ordinateurs sans pare-feu
- Recherche des ordinateurs dont les alertes nécessitent d'être vigilant
- Recherche des ordinateurs non mis à jour
- Recherche des ordinateurs non administrés par la console
- Recherche des ordinateurs non connectés au réseau

Vous pouvez aussi vérifier si tous les ordinateurs du groupe sont en conformité avec les paramètres antivirus et HIPS, de mise à jour, de pare-feu et de contrôle des applications du groupe comme le décrit la

rubrique Vérification de la conformité des ordinateurs aux stratégies.

Quels ordinateurs sont protégés ?

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



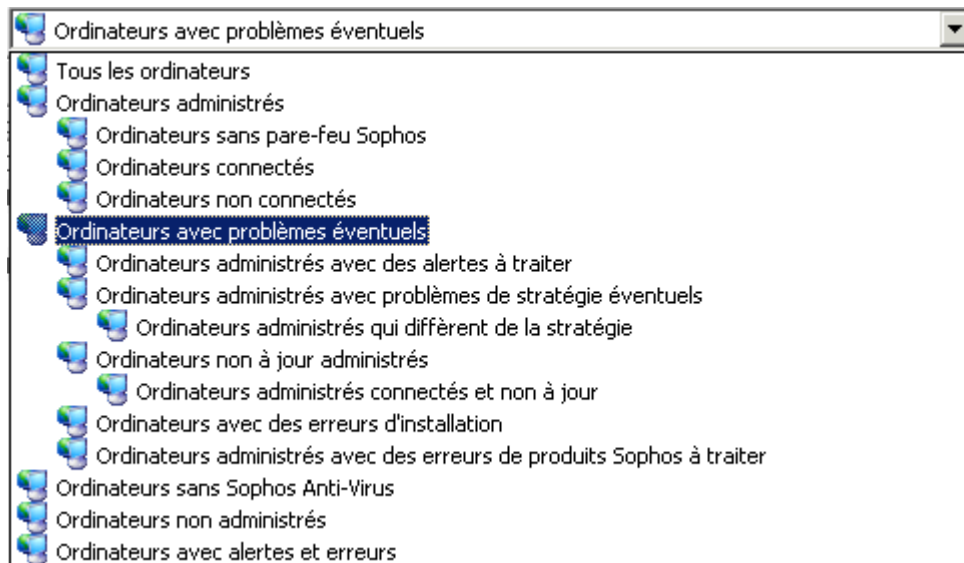
Il se peut que l'administrateur ait délibérément désactivé le contrôle sur accès sur certains types d'ordinateur (par exemple, les serveurs de fichiers).

Pour vérifier que les ordinateurs sont protégés :

1. Sélectionnez le groupe d'ordinateurs que vous désirez vérifier.
2. Si vous désirez vérifier les ordinateurs dans les sous-groupes du groupe, sélectionnez **A ce niveau et au-dessous** dans la liste déroulante.
3. Dans la liste des ordinateurs, observez la colonne **Sur accès**. Si vous voyez "Actif", l'ordinateur exécute le contrôle sur accès. Si vous voyez un bouclier gris, il ne l'exécute pas.
4. Si vous avez installé le pare-feu, observez la colonne **Pare-feu activé**. Si "Oui" apparaît, l'ordinateur dispose de la protection pare-feu.
5. Observez ensuite la colonne **A jour**. Si vous voyez "Oui", l'ordinateur est à jour. Si vous voyez une horloge et une date, il ne l'est pas.



Vous pouvez afficher une liste des ordinateurs qui ne sont pas correctement protégés ou qui ont d'autres problèmes liés à la protection. Dans la liste déroulante **Vue**, sélectionnez **Ordinateurs avec problèmes éventuels**. Vous pouvez aussi sélectionner une sous-entrée de cette entrée pour afficher les ordinateurs affectés par un problème spécifique (par exemple, les ordinateurs qui diffèrent de la stratégie de groupe ou lorsqu'une erreur sur un produit Sophos a lieu).




Quels ordinateurs sont à jour ?

Si votre administrateur a défini les logiciels de sécurité Sophos comme cela était conseillé, les ordinateurs devront recevoir les mises à jour automatiquement.

1. Sélectionnez le groupe d'ordinateurs que vous désirez vérifier.
2. Si vous désirez vérifier les ordinateurs dans un des sous-groupes, sélectionnez **A ce niveau et au-dessous** dans la liste déroulante.
3. Observez ensuite la colonne **A jour**.

Si vous voyez "Oui", l'ordinateur est à jour.

Si une horloge apparaît, l'ordinateur n'est pas à jour. Le texte indique depuis quand l'ordinateur n'est plus à jour.

 Pour mettre immédiatement à jour les ordinateurs, sélectionnez les ordinateurs. Cliquez avec le bouton droit de la souris et sélectionnez **Mettre les ordinateurs à jour maintenant**.

Recherche des ordinateurs non protégés

Un ordinateur n'est pas correctement protégé s'il n'exécute pas un contrôle sur accès ou si le pare-feu (lorsqu'il est installé) est désactivé.



Il se peut que l'administrateur ait délibérément désactivé le contrôle sur accès sur certains types d'ordinateur (par exemple, les serveurs de fichiers).

Si un ordinateur n'exécute pas le contrôle sur accès, un bouclier gris ainsi que le terme "Inactif" apparaissent dans la colonne **Sur accès** de la page d'Etat.

Si le pare-feu est désactivé, un icône (un mur de briques) pare-feu gris apparaît dans la colonne **Pare-feu activé**.

Pour afficher tous les ordinateurs qui ne sont pas correctement protégés, procédez comme suit :

1. Sélectionnez le groupe dans lequel vous souhaitez rechercher les ordinateurs.
2. Sur la barre d'outils, dans la liste déroulante **Vue**, sélectionnez **Ordinateurs avec problèmes éventuels**. Vous pouvez aussi sélectionner une sous-entrée de cette entrée pour afficher les ordinateurs affectés par un problème spécifique (par exemple, les ordinateurs qui diffèrent de la stratégie de groupe ou lorsqu'une erreur sur un produit Sophos a lieu).
3. Si le groupe contient des sous-groupes, sélectionnez également si vous souhaitez rechercher les ordinateurs **A ce niveau seulement** ou **A ce niveau et au-dessous**.
4. Tout ordinateur ayant des problèmes de protection sera répertorié.

Recherche des ordinateurs sans pare-feu

Si le pare-feu n'est pas installé sur un ordinateur, une icône (mur de briques) pare-feu gris apparaît dans la colonne **Pare-feu activé** de la page d'Etat.

Pour afficher tous les ordinateurs dans ce cas et corriger le problème, procédez comme suit :

1. Sélectionnez le groupe dans lequel vous souhaitez rechercher les ordinateurs avec des alertes.
2. Sur la barre d'outils, dans la liste déroulante **Vue**, sélectionnez **Ordinateurs sans pare-feu Sophos**.

3. Si le groupe contient des sous-groupes, sélectionnez également si vous souhaitez rechercher les ordinateurs **A ce niveau seulement** ou **A ce niveau et au-dessous**.
4. Si vous désirez installer le pare-feu sur des ordinateurs, sélectionnez-les, cliquez dessus avec le bouton droit de la souris et sélectionnez **Protéger les ordinateurs**. Lorsqu'invité à choisir le logiciel, sélectionnez **Installer Sophos Client Firewall**.

Recherche des ordinateurs dont les alertes nécessitent d'être vigilant

Si un ordinateur possède une alerte qui nécessite votre vigilance, une icône d'alerte s'affiche dans la colonne **Alertes et erreurs** de la page d'Etat.

Un signal d'alerte rouge indique un virus ou un spyware. Un signal jaune indique un comportement ou un fichier suspect, un adware ou toute autre application potentiellement indésirable, une application bloquée par le pare-feu, une application contrôlée ou une erreur.

Pour afficher les ordinateurs dont les alertes nécessitent toujours une attention particulière, procédez comme suit :

1. Sélectionnez le groupe dans lequel vous souhaitez rechercher les ordinateurs avec des alertes.
2. Sur la barre d'outils, dans la liste déroulante **Vue**, sélectionnez **Ordinateurs administrés avec des alertes à traiter**.
3. Si le groupe contient des sous-groupes, sélectionnez également si vous souhaitez rechercher les ordinateurs **A ce niveau seulement** ou **A ce niveau et au-dessous**.
4. En cas de présence d'un virus ou d'une application indésirable sur vos ordinateurs, reportez-vous à la rubrique [Nettoyage immédiat des ordinateurs](#).

En cas de présence **souhaitée** d'un adware ou de toute autre application potentiellement indésirable sur vos ordinateurs, veuillez contacter votre administrateur pour qu'il l'autorise.

Si le pare-feu a bloqué une application que vous **souhaitez** exécuter, veuillez contacter votre administrateur pour qu'il l'autorise.

Si des ordinateurs sont non mis à jour, reportez-vous à la section Recherche des ordinateurs non mis à jour pour obtenir de l'aide sur le diagnostic et la correction du problème.



Si l'affichage de l'alerte n'est plus nécessaire, vous pouvez l'effacer. Sélectionnez le ou les ordinateurs affichant des alertes et sélectionnez **Effacer les alertes et les erreurs**.

Recherche des ordinateurs non mis à jour

Si le logiciel d'un ordinateur n'est pas à jour, une horloge s'affiche dans la colonne **A jour** de la page d'**Etat**. Le texte indique depuis quand l'ordinateur n'est plus à jour.

Un ordinateur peut être non mis à jour pour l'une des deux raisons suivantes :

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

Cette section vous indique comment établir un diagnostic du problème et mettre à jour les ordinateurs.

1. Sélectionnez le groupe dans lequel vous souhaitez rechercher les ordinateurs non mis à jour.
2. Sur la page à onglets **Etat**, cliquez sur la colonne **A jour** pour trier les ordinateurs et voir lesquels sont mis à jour.
3. Cliquez sur l'onglet **Détails mise à jour** et observez la colonne **Serveur principal**. Le répertoire à partir duquel chaque ordinateur se met à jour est affiché.
4. A présent, observez les ordinateurs qui se mettent à jour à partir d'un répertoire particulier.

Si certains ne sont pas à jour alors que d'autres le sont, le problème provient des ordinateurs individuels. Sélectionnez-les, cliquez dessus avec le bouton droit de la souris et sélectionnez **Mettre les ordinateurs à jour maintenant**.

Si tous ne sont pas à jour, le problème pourrait provenir du répertoire. Demandez à votre administrateur réseau de veiller à

ce que le répertoire contienne les logiciels Sophos les plus récents.

Recherche des ordinateurs non administrés par la console

Les ordinateurs Windows Mac et Linux doivent être administrés par Helpdesk Console afin de pouvoir être mis à jour et sous surveillance.

Si un ordinateur n'est pas administré, les détails le concernant sur la page d'Etat sont grisés.

Pour rechercher et corriger les ordinateurs non administrés, procédez comme suit.

1. Sur la barre d'outils, dans la liste déroulante **Vue**, sélectionnez **Ordinateurs non administrés**.
2. Sélectionnez tous les ordinateurs qui sont répertoriés. Cliquez avec le bouton droit de la souris et sélectionnez **Protéger les ordinateurs** pour installer une version administrée de Sophos Anti-Virus.
3. Si Helpdesk Console échoue dans sa tentative d'installer Sophos Anti-Virus automatiquement sur certains ordinateurs, procédez à une installation manuelle.

Recherche des ordinateurs non connectés au réseau

Si un ordinateur est non connecté au réseau, une croix rouge apparaît sur l'icône présente à côté de son nom dans la page d'Etat.

Pour afficher une liste d'ordinateurs non connectés, procédez comme suit :

1. Sélectionnez le groupe dans lequel vous souhaitez rechercher les ordinateurs non connectés.
2. Sur la barre d'outils, dans la liste déroulante **Vue**, sélectionnez **Ordinateurs non connectés**.
3. Si le groupe contient des sous-groupes, sélectionnez également si vous souhaitez rechercher les ordinateurs **A ce niveau seulement** ou **A ce niveau et au-dessous**.



"Ordinateurs non connectés" signifie que les ordinateurs qui sont habituellement gérés par Helpdesk Console sont ici non connectés. Les ordinateurs non connectés et non gérés ne sont pas affichés.

4 Comment mettre à jour les ordinateurs ?

Les ordinateurs sont généralement configurés pour se mettre à jour automatiquement avec les plus récents logiciels Sophos. Mais vous pouvez aussi à n'importe quel moment mettre à jour les ordinateurs manuellement, comme le décrit cette section.

- Mise à jour immédiate des ordinateurs

Mise à jour immédiate des ordinateurs

Vous pouvez mettre à jour un ou plusieurs ordinateurs immédiatement sans attendre la prochaine mise à jour automatique.

Sélectionnez le ou les ordinateurs que vous souhaitez mettre à jour. Cliquez avec le bouton droit de la souris et sélectionnez **Mettre les ordinateurs à jour maintenant**.

5 Comment m'assurer que les ordinateurs sont en conformité avec les stratégies ?

Cette section vous explique aussi comment vous assurer que tous les ordinateurs d'un groupe utilisent les mêmes paramètres antivirus et HIPS, de mise à jour, de pare-feu et de contrôle des applications.

- Vérification de la conformité des ordinateurs aux stratégies
- Mise en conformité des ordinateurs avec les stratégies

Vérification de la conformité des ordinateurs aux stratégies

Vous pouvez vérifier si tous les ordinateurs d'un groupe sont conformes aux paramètres antivirus et HIPS, de mise à jour, de pare-feu et de contrôle des applications de ce groupe.

1. Sélectionnez le groupe que vous désirez vérifier.
2. Sur la page **Etat**, consultez les colonnes **Stratégie antivirus et HIPS**, **Stratégie de mise à jour**, **Stratégie de pare-feu** et **Stratégie de contrôle des applications**. Si l'ordinateur n'utilise pas les mêmes paramètres que le reste du groupe, un signal d'avertissement apparaît accompagné des mots "Diffère de la stratégie".

Si vous souhaitez que vos ordinateurs soient en conformité avec leurs stratégies de groupe, reportez-vous à la rubrique [Mise des ordinateurs en conformité avec les stratégies](#).

Mise en conformité des ordinateurs avec les stratégies

Si vous découvrez qu'un ou plusieurs ordinateurs ne sont pas conformes aux paramètres antivirus et HIPS, de mise à jour, de pare-feu ou de contrôle d'application de leur groupe, vous pouvez appliquer les paramètres de groupe à ce ou ces ordinateurs.

1. Sélectionnez le ou les ordinateurs qui n'appliquent pas les paramètres de groupe.
2. Cliquez avec le bouton droit de la souris et sélectionnez **Appliquer**. Puis, sélectionnez **Stratégie antivirus et HIPS du groupe**, **Stratégie de mise à jour du groupe**, **Stratégie de pare-feu du groupe**, **Stratégie de contrôle des applications du groupe** ou **Toutes les stratégies du groupe** de manière appropriée.

6 Comment effectuer le contrôle des ordinateurs ?

Par défaut, Sophos Anti-Virus détecte automatiquement les virus, les chevaux de Troie, les vers et les spywares connus et inconnus présents dans les fichiers dès qu'un utilisateur tente d'y accéder. Sophos Anti-Virus 7 et supérieur pour Windows 2000 et supérieur analyse aussi le comportement des programmes s'exécutant sur le système.

Vous pouvez également effectuer immédiatement un contrôle intégral du système des ordinateurs sélectionnés.

Contrôle immédiat des ordinateurs

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



Seuls les ordinateurs Windows exécutant Sophos Anti-Virus 7 ou supérieur peuvent effectuer immédiatement un contrôle intégral du système demandé depuis la console.

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

Autrement, dans le menu **Actions**, sélectionnez **Contrôle intégral du système**.

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

7 Comment gérer les alertes ?

Cette section décrit comment gérer les alertes.


Elle inclut :

- Que signifient les icônes d'alertes ?
- Gestion des alertes virales et de spywares
- Gestion des alertes de comportement suspect
- Gestion des alertes de fichier suspect
- Gestion des alertes de pare-feu
- Gestion des alertes d'adwares/PUA
- Gestion des alertes d'application contrôlée
- Suppression des alertes de la console



Que signifient les icônes d'alertes ?

Si un virus ou un spyware, un élément suspect, un adware ou toute autre application potentiellement indésirable est détecté, des icônes d'alertes apparaissent sur la page **Etat** de Helpdesk Console.

Les icônes d'alertes sont représentées ci-dessous. Les autres pages de cette section vous fournissent des conseils sur la manière de gérer les alertes.

 Des avertissements apparaissent aussi sur la console si le logiciel est désactivé ou non à jour. Pour plus d'informations, reportez-vous à la rubrique [Comment m'assurer que mon réseau est protégé ?](#)

Icônes d'alertes


Symbole	Explication
	L'apparition d'un signal d'avertissement rouge dans la colonne Alertes et erreurs signifie qu'un virus, un ver, un cheval de Troie, un spyware ou un comportement suspect a été détecté.
	L'apparition d'un signal d'avertissement jaune dans la colonne Alertes et erreurs indique l'un des problèmes suivants : <ul style="list-style-type: none"> • Un fichier suspect a été détecté. • Un adware ou toute autre application potentiellement indésirable a été détecté. • Une application contrôlée a été détectée. • Le pare-feu a bloqué une application. • Une erreur a eu lieu. <p>L'apparition d'un signal d'avertissement jaune dans les colonnes Stratégie antivirus et HIPS, Stratégie de pare-feu, Stratégie de mise à jour ou Stratégie de contrôle des applications signifie que l'ordinateur n'utilise pas les mêmes stratégies que les autres ordinateurs de son groupe.</p>

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

Priorité des alertes


1. Alertes de virus/spyware
2. Alertes de comportement suspect
3. Alertes de fichiers suspects
4. Alertes de pare-feu
5. Alertes d'adwares/PUA
6. Alertes des applications contrôlées
7. Erreurs de Sophos Anti-Virus, de mise à jour et de Sophos Client Firewall

Gestion des alertes virales et de spywares

Si un virus ou un spyware est détecté, un triangle rouge d'avertissement apparaît  ainsi que les mots "Virus/spyware détecté" sur la page Etat.


Pour plus de détails, cliquez sur l'onglet **Détails des alertes et des erreurs**. Pour gérer les virus ou les spywares, suivez les instructions de la rubrique [Nettoyage immédiat des ordinateurs](#).

Gestion des alertes de comportement suspect

Si un comportement suspect ou un dépassement de la mémoire tampon est détecté lors d'une analyse comportementale runtime, un triangle rouge d'avertissement  apparaît accompagné des mots "Comportement suspect détecté" sur la page Etat.

Pour plus de détails, cliquez sur l'onglet **Détails des alertes et des erreurs**. Pour supprimer l'élément suspect, suivez les instructions de la rubrique [Nettoyage immédiat des ordinateurs](#). Si vous souhaitez l'autoriser, veuillez contacter votre administrateur.


Gestion des alertes de fichier suspect

Si un fichier suspect est détecté, un triangle jaune d'avertissement apparaît  ainsi que les mots "Fichier suspect détecté" sur la page Etat.

Pour plus de détails, cliquez sur l'onglet **Détails des alertes et des erreurs**. Le nom du fichier apparaît dans la colonne **Élément détecté**.

Pour supprimer le fichier, reportez-vous à la rubrique Nettoyage immédiat des ordinateurs. Pour autoriser le fichier, veuillez contacter votre administrateur.

Gestion des alertes de pare-feu

Si le pare-feu bloque une application, un triangle jaune d'avertissement  apparaît ainsi que les mots "Alerte pare-feu" sur la page Etat.




Cette icône indique aussi une alerte adware/PUA depuis Sophos Anti-Virus. Le texte "Adware/PUA détecté" apparaît ensuite à côté de l'icône.

Pour plus de détails, cliquez sur l'onglet **Détails des alertes et des erreurs**. Le nom de l'application bloquée par le pare-feu apparaît dans la colonne **Élément détecté**.

Si vous souhaitez autoriser l'application, ou créer une nouvelle règle pour celle-ci, veuillez contacter votre administrateur.

Gestion des alertes d'adwares/PUA

En cas de détection d'un adware ou de toute autre application potentiellement indésirable (PUA), un triangle jaune d'avertissement  apparaît ainsi que les mots "Adware/PUA détecté" sur la page Etat.




Cette icône peut aussi indiquer une alerte de pare-feu. Le texte "Alerte pare-feu" apparaît à côté de l'icône.

Pour plus de détails, cliquez sur l'onglet **Détails des alertes et des erreurs**. Le nom de l'application apparaît dans la colonne **Élément détecté**.

Pour supprimer l'application, reportez-vous à la rubrique Nettoyage immédiat des ordinateurs. Pour autoriser l'application, veuillez contacter votre administrateur.

Gestion des alertes d'application contrôlée

Si une application contrôlée est détectée, un triangle jaune d'avertissement apparaît  ainsi que les mots "Application contrôlée détectée" sur la page **Etat**.

Pour plus de détails, cliquez sur l'onglet **Détails des alertes et des erreurs**. Le nom de l'application apparaît dans la colonne **Élément détecté**.

Pour supprimer l'application, rendez-vous sur chaque ordinateur et exécutez le programme de désinstallation de ce produit.



Il se peut que les logiciels de sécurité Sophos perturbent la désinstallation, en effet, le contrôle sur accès des applications contrôlées bloque les programmes utilisés pour installer et désinstaller les applications. Veuillez contacter votre administrateur.

Suppression des alertes de la console

Si vous prenez des mesures pour gérer les alertes ou si vous êtes certain que l'ordinateur est sain, vous pouvez effacer les signaux d'alertes affichés sur la console.



Vous ne pouvez pas effacer les alertes concernant les erreurs d'installation. Celles-ci sont effacées uniquement lorsque l'installation de Sophos Anti-Virus sur l'ordinateur s'effectue avec succès.

1. Sélectionnez le ou les ordinateurs sur lesquels vous souhaitez effacer des alertes. Cliquez avec le bouton droit de la souris et sélectionnez **Effacer les alertes et les erreurs**.
2. La boîte de dialogue **Effacement des alertes et des erreurs** apparaît.

Pour effacer les alertes depuis la console, dans la boîte de

dialogue **Effacement des alertes et des erreurs**, sur l'onglet **Alertes**, sélectionnez les alertes que vous souhaitez effacer et cliquez sur **OK**. Les alertes effacées (supprimées) n'apparaissent plus dans la console.

Pour supprimer les erreurs de produits Sophos depuis la console, dans la boîte de dialogue **Effacement des alertes et des erreurs**, rendez-vous sur l'onglet **Erreurs Sophos Anti-Virus** ou sur l'onglet **Erreurs de pare-feu**, sélectionnez les erreurs que vous souhaitez effacer de la console et cliquez sur **OK**.

8 Comment nettoyer les ordinateurs ?


Cette section décrit la procédure de nettoyage des ordinateurs infectés par un virus ou sur lesquels une application indésirable est installée.

Vous pouvez :

- Nettoyer immédiatement les ordinateurs
- Gérer les éléments détectés en cas d'échec du nettoyage

Nettoyage immédiat des ordinateurs

Depuis Helpdesk Console, vous pouvez procéder à un nettoyage immédiat des ordinateurs infectés par un virus ou ayant des applications indésirables.

 Cette option s'applique uniquement aux ordinateurs Windows 2000 ou supérieur exécutant Sophos Anti-Virus 6 ou supérieur.

Pour nettoyer les ordinateurs Windows 95/98/Me et NT4, Mac ou Linux, vous pouvez soit demander à votre administrateur de configurer un nettoyage automatique, soit nettoyer les ordinateurs individuellement comme décrit à la rubrique Gestion des éléments détectés en cas d'échec du nettoyage.



Sophos Anti-Virus peut signaler qu'un élément (par exemple, un cheval de Troie ou une application potentiellement indésirable) est "partiellement détecté". Ceci signifie qu'il n'a pas trouvé tous les composants de cette application. Avant de nettoyer l'article, vous aurez besoin de trouver ses autres composants en exécutant un contrôle intégral du système du ou des ordinateur(s) affectés. Pour plus d'informations, reportez-vous à la rubrique Élément partiellement détecté.

1. Dans la liste des ordinateurs, cliquez avec le bouton droit de la souris sur le ou les ordinateurs que vous souhaitez nettoyer. Sélectionnez **Nettoyer les éléments détectés**.
2. Dans la boîte de dialogue **Nettoyage des éléments détectés**, sélectionnez la case de chaque élément que vous souhaitez nettoyer ou cliquez sur **Sélectionner tout**.
3. Cliquez sur **OK** pour nettoyer le ou les ordinateur(s).
4. Si le nettoyage réussit, la ou les alerte(s) apparaissant dans la liste des ordinateurs ne s'affiche(nt) plus.

Si une quelconque alerte demeure répertoriée, procédez à un nettoyage manuel des ordinateurs. Voir la rubrique Gestion des éléments détectés en cas d'échec du nettoyage.

Gestion des éléments détectés en cas d'échec du nettoyage

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

1. Dans la liste des ordinateurs, cliquez sur l'onglet **Détails des alertes et des erreurs**. Dans la colonne **Élément détecté**, recherchez le nom de l'élément.
2. Dans le menu **Aide**, cliquez sur **Voir des informations sur l'élément**. Cette opération vous connecte au site Web de Sophos sur lequel vous pouvez rechercher l'élément et trouver des conseils sur la façon de nettoyer votre ordinateur.
3. Rendez-vous sur chaque ordinateur et effectuez le nettoyage manuellement.



Le site Web de Sophos offre au téléchargement des outils de désinfection spéciaux pour certains virus et vers.

9 Comment générer des rapports ?

Vous pouvez générer des rapports à propos des alertes sur votre réseau.

Pour cela, cliquez sur l'icône **Rapports** de la barre d'outils puis utilisez les options d'**Edition de rapports** comme décrit dans cette section.

Vous pouvez :

- Générer un rapport
- Visualiser un rapport sous forme de tableau
- Visualiser un rapport sous forme de diagramme
- Afficher le nombre d'alertes par nom d'élément
- Afficher le nombre d'alertes par emplacement
- Afficher le pourcentage d'alertes
- Afficher l'historique des alertes
- Imprimer un rapport
- Exporter un rapport dans un fichier
- Modifier la mise en page du rapport

Génération d'un rapport

Pour créer un rapport, procédez comme suit.

1. Cliquez sur l'icône **Rapports** dans la barre d'outils.
2. Dans le menu déroulant de la boîte de dialogue **Edition de rapports**, sélectionnez le type de rapport désiré.
 - § **Alertes par nom d'élément** affiche le nombre d'alertes pour chaque élément (un virus ou une application indésirable) détectée sur votre réseau.
 - § **Alertes par emplacement** affiche le nombre d'alertes pour chaque ordinateur ou groupe d'ordinateurs.
 - § **Alertes par heure** affiche le pourcentage d'alertes détectées

pendant une durée déterminée.

- § **Historique des alertes** affiche l'intégralité des détails concernant chaque alerte.


Sur l'onglet **Configuration**, vous pouvez personnaliser le rapport.

Puis cliquez sur l'onglet **Tableau** ou **Diagramme** pour voir le rapport.

Visualisation d'un rapport sous forme de tableau

1. Cliquez sur l'icône **Rapports** dans la barre d'outils.
2. Dans la boîte de dialogue **Edition de rapports**, sélectionnez le type de rapport que vous souhaitez créer à partir du menu déroulant. Dans l'onglet **Configuration**, configurez le rapport. Puis cliquez sur l'onglet **Tableau**.
3. Le tableau apparaît. La **Description du rapport** résume les critères (par exemple la période de temps couverte) utilisés pour créer le rapport.

Visualisation d'un rapport sous forme de diagramme

 Il n'y a pas de vue du diagramme disponible pour les rapports 'Historique des alertes'.

1. Cliquez sur l'icône **Rapports** dans la barre d'outils.
2. Dans la boîte de dialogue **Edition de rapports**, sélectionnez le type de rapport que vous souhaitez créer à partir du menu déroulant. Dans l'onglet **Configuration**, configurez le rapport. Puis cliquez sur l'onglet **Diagramme**.
3. Le diagramme s'affiche. La **Description du rapport** résume les critères (par exemple la période de temps couverte) utilisés pour créer le rapport.

Affichage du nombre d'alertes par nom d'élément

1. Cliquez sur l'icône **Rapports** dans la barre d'outils.

2. Dans la boîte de dialogue **Edition de rapports**, à partir du menu déroulant, sélectionnez **Alertes par nom d'élément**.
3. Sur l'onglet **Configuration**, vous pouvez sélectionner les options énumérées ci-dessous. Une fois que vous avez terminé, vous pouvez visualiser le rapport sous forme de diagramme ou de tableau en cliquant sur les onglets respectifs.

Période du rapport

Dans la zone de texte **Période**, cliquez sur le bouton de déroulement et sélectionnez une période de temps. Vous pouvez soit sélectionner une période de temps définie comme par exemple, **Le mois dernier**, ou sélectionnez l'option **Personnalisé** et définir votre propre période de temps dans les cases **Début** et **Fin**.

Emplacement

Cliquez sur **Groupe d'ordinateurs** ou sur **Ordinateur individuel**. Puis cliquez sur le bouton de déroulement pour définir un nom de groupe ou d'ordinateur.

Filtre

Par défaut, le rapport affiche toutes les alertes ainsi que le nombre d'occurrences pour chacune d'entre elles. Vous pouvez modifier les types d'alertes affichés sur l'un des suivants :

- § Toutes (sauf les applications contrôlées)
- § Virus/spywares seulement
- § Comportement suspect seulement
- § Fichiers suspects seulement
- § Pare-feu seulement
- § Adwares/PUA seulement
- § Applications contrôlées seulement

Vous pouvez aussi configurer le rapport pour qu'il indique uniquement :

- § les *n* premières alertes (où *n* est un nombre que vous définissez), ou

§ les alertes avec m occurrences ou plus (où m est un nombre que vous définissez).

Tri par

Par défaut, le rapport répertorie les alertes dans l'ordre décroissant du nombre d'occurrences. Sélectionnez la case **Nom d'alerte** si vous souhaitez que leurs noms soient classés par ordre alphabétique.

Affichage du nombre d'alertes par emplacement

1. Cliquez sur l'icône **Rapports** dans la barre d'outils.
2. Dans la boîte de dialogue **Edition de rapports**, à partir du menu déroulant, sélectionnez **Alertes par emplacement**.
3. Sur l'onglet **Configuration**, vous pouvez sélectionner les options énumérées ci-dessous. Une fois que vous avez terminé, vous pouvez visualiser le rapport sous forme de diagramme ou de tableau en cliquant sur les onglets respectifs.

Période du rapport

Dans la zone de texte **Période**, cliquez sur le bouton de déroulement et sélectionnez une période de temps. Vous pouvez soit sélectionner une période de temps définie comme par exemple, **Le mois dernier**, ou sélectionnez l'option **Personnalisé** et définir votre propre période de temps dans les cases **Début** et **Fin**.

Emplacement

Cliquez sur **Ordinateurs** pour afficher les alertes par ordinateur ou sur **Groupe** pour afficher les alertes pour chaque groupe d'ordinateurs.

Filtre

Par défaut, le rapport affiche toutes les alertes ainsi que le nombre d'occurrences pour chacune d'entre elles. Vous pouvez modifier les types d'alertes affichés sur l'un des suivants :

- § Toutes (sauf les applications contrôlées)
- § Virus/spywares seulement
- § Comportement suspect seulement
- § Fichiers suspects seulement
- § Pare-feu seulement
- § Adwares/PUA seulement
- § Applications contrôlées seulement

Autrement, vous pouvez configurer le rapport pour qu'il affiche uniquement les emplacements ayant signalé une alerte particulière. Pour définir une seule alerte, cliquez sur la flèche du menu déroulant et sur un nom d'alerte dans la liste. Pour définir plusieurs alertes, saisissez un nom dans la zone de texte en utilisant des caractères joker. Utilisez ? pour la substitution d'un seul caractère du nom et * pour la substitution d'une chaîne de caractères. Par exemple, W32/* définit tous les virus dont le nom commence par W32/.

Par défaut, le rapport affiche tous les ordinateurs ou tous les groupes (selon la sélection effectuée pour **Emplacement**). Toutefois, vous pouvez le configurer pour qu'il affiche uniquement

- § les n premiers emplacements qui ont enregistré le plus d'alertes (ou n est un nombre que vous définissez), ou
- § les emplacements avec m alertes ou plus (où m est un nombre que vous définissez).

Tri par

Par défaut, le rapport répertorie les emplacements dans l'ordre décroissant du nombre d'alertes par virus. Cochez **Emplacement** si vous souhaitez que leurs noms soient classés par ordre alphabétique.

Affichage du pourcentage d'alertes

1. Cliquez sur l'icône **Rapports** dans la barre d'outils.

2. Dans la boîte de dialogue **Edition de rapports**, à partir du menu déroulant, sélectionnez **Alertes par heure**.
3. Sur l'onglet **Configuration**, vous pouvez sélectionner les options énumérées ci-dessous. Une fois que vous avez terminé, vous pouvez visualiser le rapport sous forme de diagramme ou de tableau en cliquant sur les onglets respectifs.

Période du rapport

Dans la zone de texte **Période**, cliquez sur le bouton de déroulement et sélectionnez une période de temps. Vous pouvez soit sélectionner une période de temps définie comme par exemple, **Le mois dernier**, ou sélectionnez l'option **Personnalisé** et définir votre propre période de temps dans les cases **Début** et **Fin**.

Emplacement

Cliquez sur **Groupe d'ordinateurs** ou sur **Ordinateur individuel**. Puis cliquez sur le bouton de déroulement pour définir un nom de groupe ou d'ordinateur.

Filtre

Par défaut, le rapport affiche toutes les alertes ainsi que le nombre d'occurrences pour chacune d'entre elles. Vous pouvez modifier les types d'alertes affichés sur l'un des suivants :

- § Toutes (sauf les applications contrôlées)
- § Virus/spywares seulement
- § Comportement suspect seulement
- § Fichiers suspects seulement
- § Pare-feu seulement
- § Adwares/PUA seulement
- § Applications contrôlées seulement

Si vous souhaitez que le rapport affiche uniquement les statistiques d'une alerte particulière ou d'un groupe d'alertes, utilisez la zone de texte **Afficher seulement les alertes comme**. Pour définir une seule alerte, cliquez sur la flèche du menu

déroulant et sur un nom d'alerte dans la liste. Pour définir plusieurs alertes, saisissez un nom dans la zone de texte en utilisant des caractères joker. Utilisez ? pour la substitution d'un seul caractère du nom et * pour la substitution d'une chaîne de caractères. Par exemple, W32/* définit tous les virus dont le nom commence par W32/.

Intervalle de mesure

Pour définir les intervalles de temps auxquels le pourcentage d'alertes doit être calculé, par exemple toutes les heures ou tous les jours, cliquez sur la flèche du menu déroulant et sélectionnez un intervalle.

Affichage de l'historique des alertes

1. Cliquez sur l'icône **Rapports** dans la barre d'outils.
2. Dans la boîte de dialogue **Edition de rapports**, à partir du menu déroulant, sélectionnez **Historique des alertes**.
3. Sur l'onglet **Configuration**, vous pouvez sélectionner les options énumérées ci-dessous. Lorsque vous avez terminé, cliquez sur l'onglet **Tableau** pour afficher le rapport.

Période du rapport

Dans la zone de texte **Période**, cliquez sur le bouton de déroulement et sélectionnez une période de temps. Vous pouvez soit sélectionner une période de temps définie comme par exemple, **Le mois dernier**, ou sélectionnez l'option **Personnalisé** et définir votre propre période de temps dans les cases **Début** et **Fin**.

Emplacement

Sélectionnez **Groupe d'ordinateurs** ou sur **Ordinateur individuel**. Puis cliquez sur le bouton de déroulement pour définir un nom de groupe ou d'ordinateur.

Filtre

Par défaut, le rapport affiche toutes les alertes ainsi que le

nombre d'occurrences pour chacune d'entre elles. Vous pouvez modifier les types d'alertes affichés sur l'un des suivants :

- § Toutes (sauf les applications contrôlées)
- § Virus/spywares seulement
- § Comportement suspect seulement
- § Fichiers suspects seulement
- § Pare-feu seulement
- § Adwares/PUA seulement
- § Applications contrôlées seulement

Si vous souhaitez que le rapport affiche uniquement les statistiques d'une alerte particulière ou d'un groupe d'alertes, utilisez la zone de texte **Afficher seulement les alertes comme**. Pour définir une seule alerte, cliquez sur la flèche du menu déroulant et sur un nom d'alerte dans la liste. Pour définir plusieurs alertes, saisissez un nom dans la zone de texte en utilisant des caractères joker. Utilisez ? pour la substitution d'un seul caractère du nom et * pour la substitution d'une chaîne de caractères. Par exemple, W32/* définit tous les virus dont le nom commence par W32/.

Tri par

Par défaut, les détails de l'alerte sont triés en fonction du **Nom d'alerte**. Toutefois, les rapports peuvent aussi être triés en fonction du **Nom d'ordinateur**, du **Nom de groupe de l'ordinateur**, ou de la **Date et heure**.

Impression d'un rapport

Pour imprimer un rapport, cliquez sur l'icône **Imprimer** de la barre d'outils en haut du rapport.



Exportation d'un rapport dans un fichier

Pour exporter un rapport dans un fichier :

1. Cliquez sur l'icône **Exporter** de la barre d'outils en haut du rapport.



2. Dans la boîte de dialogue **Exportation du rapport**, sélectionnez le type de document ou de feuille de calcul vers lequel vous souhaitez exporter le rapport. les options sont :

- § PDF (Acrobat)
- § HTML
- § Microsoft Excel
- § Microsoft Word
- § Rich Text Format (RTF)
- § Valeurs séparées par des virgules (CSV)
- § XML

3. Cliquez sur le bouton de navigation **Nom du fichier** pour sélectionner un emplacement. Puis saisissez un nom. Cliquez sur **OK**.

Modification de la mise en page du rapport

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

1. Cliquez sur l'icône de mise en page de la barre d'outils en haut du rapport.



2. Dans la boîte de dialogue **Mise en page**, définissez la taille, l'orientation et les marges de la page. Cliquez sur **OK**. Le rapport s'affichera ensuite avec ces paramètres de mise en page.

Ces paramètres de mise en page seront aussi utilisés lorsque vous

imprimerez ou exporterez le rapport.

10 Résolution des problèmes

Cette section décrit comment traiter les problèmes qui pourraient survenir lors de l'utilisation de Helpdesk Console.

- Impossible de démarrer Helpdesk Console
- Groupes non affichés
- L'installation de Sophos Anti-Virus a échoué
- Les ordinateurs ne sont pas à jour
- Élément partiellement détecté
- Echec du nettoyage
- Guérison des effets secondaires des virus
- Guérison des effets secondaires des applications

Impossible de démarrer Helpdesk Console

Lorsque vous essayez de démarrer Helpdesk Console, le message d'erreur "Impossible de démarrer Helpdesk Console" peut être affiché. Ceci se produit pour l'une des raisons suivantes.

- Ceci se produit si l'administrateur n'est pas membre du groupe Sophos Console Administrators sur le serveur exécutant l'Enterprise Console. Demandez à l'administrateur de s'assurer qu'il vous ajoute à ce groupe et au groupe Sophos DB Users.
- Helpdesk Console Configuration Utility n'a pas été utilisé pour configurer l'ordinateur Helpdesk Console. Veuillez contacter votre administrateur pour effectuer cette opération.

Groupes non affichés

Si vous ne pouvez pas voir les groupes que vous souhaitez ou si ne voyez pas de groupes du tout, il y a deux raisons possibles :

- Votre administrateur n'a pas configuré la Helpdesk Console pour afficher les groupes.
- Votre administrateur a renommé les groupes depuis la configuration de la Helpdesk Console.

Demandez à votre administrateur de reconfigurer la Helpdesk Console de manière à ce que vous puissiez administrer les groupes.

L'installation de Sophos Anti-Virus a échoué

Si l'Assistant de protection des ordinateurs ne parvient pas à installer Sophos Anti-Virus sur les ordinateurs, c'est probablement parce que :

- Helpdesk Console ne reconnaît pas le système d'exploitation exécuté par les ordinateurs. Ceci se produit probablement parce que l'administrateur n'a pas correctement saisi son nom utilisateur lorsqu'il a utilisé la Sophos Enterprise Console pour rechercher des ordinateurs. Veuillez demander à l'administrateur de recommencer la procédure en saisissant son nom utilisateur au format domaine\utilisateur.
- Les ordinateurs exécutent un pare-feu (généralement, il s'agit d'ordinateurs Windows XP SP2 et Windows Vista).
- Le "Partage de fichiers simple" n'a pas été activé ou désactivé sur les ordinateurs Windows XP.

Une liste complète des configurations requises pour les logiciels antivirus et de pare-feu figure sur le site Web de Sophos à l'adresse : www.sophos.fr/products/all-sysreqs.html

Les ordinateurs ne sont pas à jour

Si le logiciel d'un ordinateur n'est pas à jour, une horloge s'affiche dans la colonne **A jour** de la page d'Etat. Le texte indique depuis quand l'ordinateur n'est plus à jour.

Un ordinateur peut être non mis à jour pour l'une des deux raisons suivantes :

- l'ordinateur ne parvient pas à récupérer une mise à jour depuis le

serveur.

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

Cette section vous indique comment établir un diagnostic du problème et mettre à jour les ordinateurs.

1. Sélectionnez le groupe dans lequel vous souhaitez rechercher les ordinateurs non mis à jour.
2. Sur la page à onglet **Etat**, cliquez sur la colonne **A jour** pour trier les ordinateurs par date de mise à jour.
3. Cliquez sur l'onglet **Détails mise à jour** et observez la colonne **Serveur principal**. Le répertoire à partir duquel chaque ordinateur se met à jour est affiché.
4. A présent, observez les ordinateurs qui se mettent à jour à partir d'un répertoire particulier.

Si certains ne sont pas à jour alors que d'autres le sont, le problème provient des ordinateurs individuels. Sélectionnez-les, cliquez dessus avec le bouton droit de la souris et sélectionnez **Mettre les ordinateurs à jour maintenant**.

Si tous ne sont pas à jour, le problème pourrait provenir du répertoire. Demandez à votre administrateur réseau de veiller à ce que le répertoire contienne les logiciels Sophos les plus récents.

Élément partiellement détecté

Sophos Anti-Virus peut signaler qu'un élément (par exemple, un cheval de Troie ou une application potentiellement indésirable) est "partiellement détectée". Ceci signifie qu'il n'a pas trouvé tous les composants de cette application.

Pour trouver d'autres composants, il est nécessaire que vous lanciez un contrôle intégral du système du ou des ordinateurs affectés. Sur des ordinateurs utilisant Sophos Anti-Virus 7 pour Windows 2000/XP/2003/Vista, vous pouvez effectuer cette opération en sélectionnant le ou les ordinateurs, en cliquant avec le bouton droit de la souris et en sélectionnant **Contrôle intégral du système**.

Si l'application n'a toujours pas été intégralement détectée, il se peut

que ce soit parce que :

- vous ne disposez pas de droits suffisants
- certains lecteurs ou dossiers de l'ordinateur, contenant les composants de l'application, sont exclus du contrôle.

Dans le dernier cas, veuillez contacter votre administrateur pour qu'il vérifie la liste des éléments exclus du contrôle et supprime tous les éléments de la liste. Puis, effectuez un nouveau contrôle de l'ordinateur.

Il se peut que Sophos Anti-Virus ne soit pas en mesure de détecter intégralement ou de supprimer les adwares et les applications potentiellement indésirables dont les composants sont installés sur des lecteurs réseau.

Pour plus de conseils, veuillez contacter votre administrateur.

Echec du nettoyage

Si Helpdesk Console ne parvient pas à nettoyer les éléments ("Echec du nettoyage"), c'est probablement parce que :

- Il n'a pas trouvé tous les composants d'un élément à plusieurs composants. Exécutez un contrôle intégral du système du ou des ordinateurs pour trouver les autres composants.
- Certains lecteurs ou dossiers contenant les composants de l'élément sont exclus du contrôle. Veuillez contacter votre administrateur pour qu'il vérifie la liste des éléments exclus du contrôle et supprime tous les éléments de la liste.
- Vous ne disposez pas de droits suffisants.
- Il ne parvient pas à nettoyer ce type d'élément.
- Un fragment de virus a été découvert plutôt qu'une correspondance virale exacte.
- L'élément se trouve sur une disquette ou un CD-ROM protégé en écriture.
- L'élément se trouve sur un volume NTFS (Windows 2000 ou supérieur) protégé en écriture.

Guérison des effets secondaires des virus

Le nettoyage peut supprimer un virus des ordinateurs mais ne peut pas toujours neutraliser les effets secondaires.

Certains virus ne laissent aucun effet secondaire. D'autres peuvent apporter des modifications ou corrompre des données de telle manière qu'il est très difficile de les détecter. Pour gérer ce problème, procédez comme suit :

- Dans le menu **Aide**, cliquez sur **Voir des informations sur l'élément**. Cette opération vous connecte au site Web de Sophos sur lequel vous pouvez consulter l'analyse du virus.
- Utilisez des sauvegardes ou des copies originales des programmes pour remplacer les programmes infectés. Si vous n'aviez pas de copies de sauvegarde avant l'infection, créez les en cas de futures infections.

Parfois, vous pouvez récupérer des données sur les disques endommagés par un virus. Sophos peut fournir des utilitaires pour réparer les dommages occasionnés par certains virus. Pour obtenir des conseils, contactez votre administrateur réseau.

Guérison des effets secondaires des applications

Le nettoyage supprime les applications indésirables mais ne peut pas toujours neutraliser les effets secondaires.

Certaines applications modifient le système d'exploitation, par exemple, en changeant vos paramètres de connexion Internet. Sophos Anti-Virus ne peut pas toujours restaurer tous les paramètres. Par exemple, si une application a modifié la page d'accueil de l'explorateur, Sophos Anti-Virus ne peut pas savoir quelle page d'accueil était utilisée auparavant.

Certaines applications installent des utilitaires, tels que des fichiers .dll ou .ocx sur votre ordinateur. Si un utilitaire est inoffensif (c'est à dire qu'il ne possède pas les "qualités" d'une application potentiellement indésirable), par exemple, une bibliothèque de langue, et qu'il ne fait pas partie intégrante de l'application, il se peut que Sophos Anti-Virus ne le détecte pas en tant que partie de l'application. Dans ce cas, le nettoyage n'entraînera pas la suppression

du fichier de votre ordinateur.

Parfois une application, telle qu'un adware (logiciel publicitaire), fait partie d'un programme que vous avez installé de manière intentionnelle, et sa présence est requise pour pouvoir exécuter le programme. Si vous supprimez cette application, l'exécution de ce programme peut s'interrompre sur l'ordinateur.

Vous devez :

- Cliquer sur **Voir des informations sur l'élément** dans le menu **Aide**. Cette opération vous connecte au site Web de Sophos sur lequel vous pouvez consulter l'analyse de l'application.
- Utiliser des sauvegardes pour restaurer les paramètres de votre système ou les programmes que vous désirez utiliser. Si vous n'aviez pas de copies de sauvegarde avant l'incident, créez les en cas de futurs incidents.

Pour plus d'informations ou de conseils sur la guérison des effets secondaires d'un adware/PUA, contactez votre administrateur réseau.

11 Glossaire

A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z

-A-

adware

Programme qui affiche des fenêtres publicitaires intempestives pour un impact négatif sur la productivité de l'utilisateur et sur l'efficacité du système.

Application Control

Fonctionnalité de Sophos Anti-Virus permettant de bloquer ou d'autoriser l'exécution d'applications légitimes, conformément à la politique de sécurité de l'entreprise.

application contrôlée

Application légitime ne constituant pas une menace à la sécurité, mais que vous avez décidé de considérer l'utilisation comme inappropriée dans l'environnement de votre entreprise. Les applications contrôlées peuvent inclure des jeux, des clients de messagerie instantanée (IM), des clients de voix sur IP (VoIP), des logiciels d'imagerie numérique, des lecteurs multimédia, des plug-ins de navigateur et bien d'autres encore.

application potentiellement indésirable (PUA)

Programme non malveillant en soi mais dont la présence est généralement considérée comme inappropriée par la majorité des réseaux professionnels. Les applications potentiellement indésirables peuvent afficher de la publicité, suivre à la trace les visites sur les sites Web ou modifier la configuration d'un ordinateur. Elles incluent les adwares, les composeurs, les outils d'administration à distance et les outils de piratage.

^ [Haut de page](#)

-C-

comportement suspect

Comportement normalement attribué à un logiciel malveillant manifesté par une application qui n'a pas été identifiée comme malveillante avant son exécution.

CSV (valeurs séparées par des virgules)

Autre nom pour le format délimité par des virgules. Il s'agit d'un format de données dans lequel chaque groupe de données est séparé par une virgule. Ce format est couramment utilisé pour transférer des données d'une application vers une autre, car la plupart des systèmes de base de données peuvent importer et exporter des données délimitées par des virgules. Par exemple, un fichier .csv peut être importé dans Microsoft Excel pour une analyse plus approfondie.

^ [Haut de page](#)

-F-

fichier suspect

Fichier contenant certaines caractéristiques communes aux logiciels malveillants mais pas suffisantes pour que le fichier soit identifié en tant que nouvelle pièce d'un logiciel malveillant (par exemple, un fichier contenant du code de décompression dynamique habituellement utilisé par les logiciels malveillants).

^ [Haut de page](#)

-H-

HIPS (système de prévention des intrusions sur l'hôte)

Technologie de sécurité pour assurer la protection contre les fichiers suspects, les virus non identifiés et tout comportement suspect.

^ [Haut de page](#)

-N-

NAC (contrôle d'accès réseau)

Un système permettant de réduire les menaces à la sécurité posées par des ordinateurs non autorisés, non conformes ou infectés en leur interdisant l'accès aux ressources réseau.

^ [Haut de page](#)

-P-

PUA ou application potentiellement indésirable

Programme non malveillant en soi mais dont la présence est

généralement considérée comme inappropriée par la majorité des réseaux professionnels. Les applications potentiellement indésirables peuvent afficher de la publicité, suivre à la trace les visites sur les sites Web ou modifier la configuration d'un ordinateur. Elles incluent les adwares, les composeurs, les outils d'administration à distance et les outils de piratage.

^ [Haut de page](#)

-S-

spyware

Programme qui s'installe furtivement, par subterfuge ou par ingénierie sociale sur un ordinateur et qui envoie depuis ce dernier des informations à un tiers sans l'autorisation ou à l'insu de son utilisateur. Parmi les spywares, on trouve les enregistreurs de touches, les chevaux de Troie de porte dérobée, les voleurs de mots de passe et les vers Botnet qui volent des données professionnelles et occasionnent des pertes financières et détériorent le réseau.

^ [Haut de page](#)

-T-

tableau de bord

Visualisation en un clin d'œil de l'état de la sécurité du réseau.

^ [Haut de page](#)

-V-

virus

Programme qui se propage sur les ordinateurs et les réseaux en se joignant à un autre programme et en créant des copies de lui-

même.

virus non identifié

Virus sans identité attribuée ou virus inconnu.

^ [Haut de page](#)