

Sophos Endpoint Security and Control Guide de démarrage pour postes autonomes

Sophos Endpoint Security and Control pour Windows, version 10.0
Sophos Anti-Virus pour Mac OS X, version 7

Date du document : décembre 2011



Table des matières

1 Avant de commencer.....	3
2 Protection des ordinateurs Windows.....	4
3 Protection des ordinateurs Mac OS X.....	9
4 Support technique.....	11
5 Mentions légales.....	12

1 Avant de commencer

1.1 Configuration requise

Pour voir la configuration requise, reportez-vous à la page des différentes configurations requises sur le site Web de Sophos (<http://www.sophos.fr/products/all-sysreqs.html>).

Par ailleurs, vous devez disposer d'un accès Internet pour télécharger le logiciel depuis le site Web de Sophos.

1.2 De quelles informations avez-vous besoin ?

Munissez-vous des informations suivantes pour effectuer l'installation et la configuration :

- L'adresse Web et les codes d'accès de téléchargement pour le programme d'installation autonome de Sophos Endpoint Security and Control et/ou pour le programme d'installation autonome de Sophos Anti-Virus pour Mac OS X, selon vos besoins.
- L'adresse de la source des mises à jour, à moins que vous ne procédiez à la mise à jour directement depuis Sophos.
- Les codes d'accès nécessaires pour accéder à la source des mises à jour.
- Les détails du serveur proxy que vous allez utiliser pour accéder à la source de mise à jour (l'adresse et le numéro du port, les codes d'accès utilisateur).

2 Protection des ordinateurs Windows

2.1 Installation de Sophos Endpoint Security and Control

Ouvrez une session en tant qu'administrateur pour installer Sophos Endpoint Security and Control.

Si un logiciel de sécurité tiers est installé :

- Assurez-vous que son interface utilisateur est fermée.
 - Assurez-vous que le pare-feu et le logiciel HIPS tiers sont désactivés ou configurés de manière à autoriser l'exécution du programme d'installation.
1. A l'aide de l'adresse Web et des codes d'accès de téléchargement fournis par Sophos ou par votre administrateur système, rendez-vous sur le site Web de Sophos et téléchargez le programme d'installation autonome de votre version de Windows.
 2. Recherchez le programme d'installation dans le dossier où il a été téléchargé. Cliquez deux fois sur le programme d'installation. Sur la fenêtre du programme d'installation, cliquez sur **Installer** pour lancer l'assistant d'installation.
 3. Sur la première page de l'**Assistant d'installation de Sophos Endpoint Security and Control**, cliquez sur **Suivant**.
 4. Sur la page **Contrat de licence**, cliquez sur **J'accepte les termes de ce contrat de licence** si vous êtes d'accord avec les termes de la licence et souhaitez poursuivre. Cliquez sur **Suivant**.
 5. Sur la page du **Dossier de destination**, si nécessaire, changez le dossier dans lequel Sophos Endpoint Security and Control sera installé. Cliquez sur **Suivant**.
 6. Sur la page **Source de mise à jour**, saisissez l'emplacement à partir duquel l'ordinateur va récupérer les mises à jour. Sophos vous recommande d'effectuer cette opération dès maintenant.
 - a) Dans la boîte **Adresse**, sélectionnez **Sophos** ou, si votre administrateur système vous a remis une adresse, saisissez cette adresse.
 - b) Dans les champs **Nom utilisateur** et **Mot de passe**, saisissez le nom utilisateur et le mot de passe qui vous ont été fournis par Sophos ou par votre administrateur système pour accéder à la source de mise à jour.
 - c) Si vous accédez au réseau et à Internet via un serveur proxy, sélectionnez la case **Accéder à la source de mise à jour via un proxy** et cliquez sur **Suivant** pour saisir les détails du proxy.

Remarque : pour saisir la source de mise à jour ultérieurement, sélectionnez la case **Je saisisrai ces détails ultérieurement**. Dès que l'installation est terminée, ouvrez Sophos Endpoint Security and Control et sélectionnez **Configurer AutoUpdate**.

Par défaut, Sophos Endpoint Security and Control va se mettre à jour toutes les 60 minutes, à condition que les détails de la source de mise à jour soient fournis et que l'ordinateur soit connecté au réseau.

7. Sur la page **Sélection des composants supplémentaires à installer**, sélectionnez la case à cocher **Installer Sophos Client Firewall** si vous souhaitez installer le pare-feu et cliquez sur **Suivant**.
8. Sur la page **Suppression des logiciels de sécurité tiers**, sélectionnez la case **Supprimer les logiciels de sécurité tiers** si un logiciel antivirus ou pare-feu tiers est installé et cliquez sur **Suivant**.
9. Sur la page **Prêt à installer Sophos Endpoint Security and Control**, cliquez sur **Suivant**. Vous devriez voir la progression de l'installation du logiciel sur votre ordinateur.

Important : par défaut, la suppression des logiciels de sécurité désinstalle aussi les outils de mise à jour associés car il se peut que d'autres logiciels de sécurité tiers les utilisent. Toutefois, s'ils ne sont pas utilisés, vous pouvez les supprimer via le Panneau de configuration.

10. Sur la dernière page de l'assistant d'installation, vous pouvez choisir de redémarrer l'ordinateur et cliquez sur **Terminer**.

Redémarrez l'ordinateur :



- Pour activer le pare-feu.
- Pour terminer la suppression des logiciels de sécurité tiers.

L'installation de Sophos Endpoint Security and Control est terminée lorsque l'icône de Sophos Endpoint Security and Control apparaît dans la barre d'état système Windows à droite de la barre des tâches.



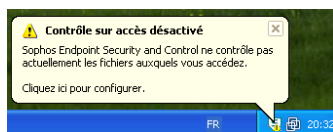
2.1.1 Que signifient les icônes de la zone de notification ?

L'icône Sophos Endpoint Security and Control de la zone de notification change en cas d'alertes en attente ou d'un problème de protection contre les menaces. Le tableau suivant présente les icônes affichées dans la zone de notification et les raisons pour lesquelles elles apparaissent.

Icône	Raison
	<ul style="list-style-type: none"> ■ Le contrôle sur accès ne fonctionne pas sur votre ordinateur. ■ Un message de pare-feu apparaît. ■ Un message d'application contrôlée apparaît. ■ Un message de contrôle des périphériques apparaît. ■ Un message de contrôle des données apparaît. ■ Un site Web est bloqué.
	<ul style="list-style-type: none"> ■ Lorsque Sophos Endpoint Security and Control ne parvient pas à se mettre à jour. ■ Un service Sophos a échoué.

Un message apparaît dans une bulle en même temps qu'une des icônes mentionnées ci-dessus pour en expliquer la cause.

Par exemple, si le contrôle sur accès n'est pas activé sur votre ordinateur, le message **Contrôle sur accès désactivé** apparaît sous forme de bulle dans la zone de notification comme suit :



2.2 Configuration du pare-feu

Vous devez impérativement configurer le pare-feu pour :

- Gérer les messages du pare-feu.
- Autoriser les programmes que vous utilisez à accéder au réseau et à Internet.
- Bloquer les programmes inconnus.

2.2.1 Gestion des messages du pare-feu

Par défaut, le pare-feu est en mode “interactif”, ce qui signifie qu'il affiche un message lorsqu'il détecte une application ou un processus qui n'a pas encore été autorisé. Dans chaque cas, vous pouvez bloquer ou autoriser l'activité.

Pour commencer, bloquez le trafic inconnu uniquement pour cette fois seulement. Par exemple, si le pare-feu affiche un message à propos d'un processus caché, cliquez sur **Bloquer ce processus cette fois-ci seulement** et cliquez sur **OK**.

Si vous ne parvenez pas à bloquer le trafic à cette occasion seulement, c'est que l'application générant le trafic n'a peut-être pas été identifiée. Dans ce cas, choisissez soit d'autoriser, soit de bloquer, la solution la plus appropriée. Vous pouvez la changer ultérieurement en modifiant la configuration du pare-feu. Pour plus d'informations, reportez-vous à l'aide de Sophos Endpoint Security and Control.

Dans certains cas, vous ne devez pas bloquer le trafic. Ceci est valable pour la somme de contrôle et les messages de règles d'application concernant votre navigateur, votre programme de messagerie et tout autre programme auxquels vous souhaitez autoriser l'accès au réseau et à Internet.

2.2.2 Autorisation d'accès au réseau et à Internet pour vos programmes

Vous devez activer le pare-feu pour autoriser les programmes de votre choix à accéder au réseau et à Internet.

1. Ouvrez le programme auquel vous souhaitez autoriser l'accès au réseau ou à Internet, tel qu'un navigateur ou un programme de messagerie.
2. Le pare-feu affiche un message vous informant qu'une nouvelle application ou une application modifiée a demandé l'accès au réseau. Cliquez sur **Ajouter la somme de contrôle à celles existantes pour cette application** et cliquez sur **OK**.
3. Le pare-feu affiche un second message vous informant qu'une application (votre navigateur ou votre programme de messagerie) a demandé l'accès au réseau. Cliquez sur **Créer une règle pour cette application avec celles prédéterminées** et assurez-vous d'avoir coché le bon paramètre pour le programme (tel que **Navigateur**, **Client de messagerie**) dans la case, et cliquez sur **OK**.

Vous pouvez aussi modifier la configuration du pare-feu pour permettre aux programmes d'accéder au réseau et à Internet quel que soit le mode utilisé. Pour plus d'informations, reportez-vous à l'aide de Sophos Endpoint Security and Control.

2.2.3 Autorisation d'accès au réseau et à Internet pour d'autres programmes

Il se peut que vous ayez besoin d'autoriser l'accès au réseau et à Internet pour d'autres programmes, par exemple, Windows Update. Utilisez le mode interactif et suivez la même procédure qu'à la section [Autorisation d'accès au réseau et à Internet pour vos programmes](#) à la page 7.

Pour autoriser le téléchargement FTP, reportez-vous à l'aide de Sophos Endpoint Security and Control.

2.2.4 Blocage des programmes inconnus

Activez maintenant le pare-feu pour traiter le trafic automatiquement et bloquer les programmes inconnus.

1. Dans la zone de notification, cliquez avec le bouton droit de la souris sur l'icône de Sophos Endpoint Security and Control pour afficher un menu. Sélectionnez **Ouvrir Sophos Endpoint Security and Control**.

2. Dans la fenêtre **Sophos Endpoint Security and Control**, dans la section **Pare-feu**, cliquez sur **Configurer le pare-feu**.

La boîte de dialogue **Configuration du pare-feu** apparaît.

3. Dans l'onglet **Général**, sous **Configuration**, cliquez sur **Configurer**.
4. Dans la boîte de dialogue de configuration des emplacements, sous la section **Mode de fonctionnement**, sélectionnez **Bloquer par défaut : tout le trafic sans règle de correspondance est bloqué**.

Désormais, le pare-feu n'affiche aucun message lorsqu'il rencontre du trafic inconnu. A la place, il enregistre le trafic dans son journal. Pour activer les infobulles lorsque le pare-feu détecte du trafic non autorisé, modifiez la configuration du pare-feu. Pour plus d'informations, reportez-vous à l'Aide de Sophos Endpoint Security and Control.

Remarque : vous pourriez avoir besoin de passer en mode interactif, par exemple, pour exécuter Windows Update. Suite à l'exécution du programme de votre choix, Sophos vous recommande de repasser en mode non interactif.

3 Protection des ordinateurs Mac OS X

3.1 Installation de Sophos Anti-Virus

Vous devez impérativement désinstaller tout logiciel antivirus tiers avant de procéder à l'installation de Sophos Anti-Virus.

Commencez par ouvrir une session sous un compte administrateur.

1. En utilisant l'adresse Web et les codes de téléchargement fournis par votre administrateur, allez sur le site Web de Sophos et téléchargez le programme d'installation autonome de Sophos Anti-Virus pour Mac OS X.
2. Recherchez l'image disque du programme d'installation dans le dossier où il a été téléchargé. Ouvrez l'image disque. Recherchez Sophos Anti-Virus.mpkg et cliquez deux fois dessus pour démarrer le programme d'installation.
3. Cliquez sur **Continuer**. Suivez les étapes jusqu'à ce que l'installation soit terminée.

L'installation de Sophos Anti-Virus est terminée lorsque l'icône Sophos Anti-Virus dans la partie droite de la barre de menus est de couleur noire.



Si l'icône est grise, c'est que le contrôle sur accès ne fonctionne pas et que votre Mac ne dispose d'aucune protection sur accès contre les menaces. Pour obtenir de l'aide, veuillez contacter votre administrateur.

3.2 Configuration de la mise à jour de Sophos Anti-Virus

Assurez-vous d'avoir ouvert une session sous un compte administrateur.

1. Cliquez sur l'icône de Sophos Anti-Virus sur le côté droit de la barre de menu et choisissez **Ouvrir les Préférences** dans le menu des raccourcis.
2. Cliquez sur **AutoUpdate**.
3. Si certains paramètres sont grisés, cliquez sur l'icône du cadenas et saisissez un nom et un mot de passe administrateur.
4. Changez les préférences comme suit :
 - Pour permettre à Sophos Anti-Virus de se mettre à jour directement depuis Sophos, choisissez **Sophos** dans le menu contextuel **Mise à jour depuis un emplacement principal**. Dans les champs **Nom utilisateur** et **Mot de passe**, saisissez les codes d'accès de mise à jour qui vous ont été attribués par Sophos.

- Pour permettre à Sophos Anti-Virus de se mettre à jour depuis le serveur Web de votre entreprise, choisissez **Serveur Web de l'entreprise** dans le menu contextuel **Mise à jour depuis un emplacement principal**. Dans le champ **Adresse**, saisissez l'adresse Web de l'emplacement depuis lequel les mises à jour seront téléchargées. Dans les champs **Nom utilisateur** et **Mot de passe**, saisissez les codes d'accès de mise à jour nécessaires pour accéder au serveur.
- Pour permettre à Sophos Anti-Virus de se mettre à jour depuis un volume réseau, choisissez **Volume réseau** dans le menu contextuel **Mise à jour depuis un emplacement principal**. Dans le champ **Adresse**, saisissez l'adresse réseau de l'emplacement depuis lequel les mises à jour seront téléchargées. Dans les champs **Nom utilisateur** et **Mot de passe**, saisissez les codes d'accès de mise à jour nécessaires pour accéder au volume.

Retrouvez ci-dessous des exemples d'adresse. Remplacez le texte entre crochets par les noms appropriés :

http://<serveur>/<partage Web>/Sophos Anti-Virus/ESCOSX

smb://<serveur>/<partage Samba>/Sophos Anti-Virus/ESCOSX

afp://<serveur>/<partage AppleShare>/Sophos Anti-Virus/ESCOSX

Vous pouvez utiliser une adresse IP ou un nom NetBIOS plutôt qu'un nom de domaine ou d'hôte pour faire référence au serveur. L'utilisation d'une adresse IP est préférable si vous avez des problèmes DNS.

5. Pour permettre à Sophos Anti-Virus de se mettre à jour via le proxy qui a été configuré dans les Préférences système, choisissez **Utiliser les paramètres proxy du système** depuis le menu contextuel en bas de la section de l'**Emplacement principal**.
6. Pour permettre à Sophos Anti-Virus de se mettre à jour via un proxy dont vous allez spécifier les paramètres :
 - a) Choisissez **Utiliser les paramètres proxy personnalisés** depuis le menu contextuel en bas de la section de l'**Emplacement principal**.
 - b) Dans la boîte de dialogue qui apparaît, saisissez l'adresse et le numéro de port du proxy dans les champs **Adresse**. Dans les champs **Nom utilisateur** et **Mot de passe**, saisissez les codes d'accès nécessaires pour accéder au proxy.
7. Sélectionnez **Vérifier la présence de mises à jour à la connexion au réseau ou à Internet**.

Sophos Anti-Virus se mettra à jour automatiquement depuis la source de mise à jour que vous avez spécifiée. Par défaut, il le fera toutes les 60 minutes à condition que l'ordinateur soit connecté au réseau. Si une croix blanche apparaît sur l'icône Sophos Anti-Virus dans la partie droite de la barre de menu, cela signifie que Sophos Anti-Virus n'a pas réussi à se mettre à jour. Pour obtenir de l'aide, veuillez contacter votre administrateur.

4 Support technique

Le support technique pour les produits Sophos est disponible de l'une des manières suivantes :

- Rendez-vous sur le forum de la communauté SophosTalk en anglais sur <http://community.sophos.com/> et recherchez d'autres utilisateurs rencontrant le même problème que le vôtre.
- Rendez-vous sur la base de connaissances du support de Sophos sur <http://www.sophos.fr/support/>.
- Téléchargez la documentation des produits sur <http://www.sophos.fr/support/docs/>.
- Envoyez un courriel à support@sophos.fr, y compris le ou les numéros de version du logiciel Sophos, le ou les systèmes d'exploitation et le ou les niveaux de correctif ainsi que le texte du ou des messages d'erreur.

5 Mentions légales

Copyright © 2011 Sophos Limited. Tous droits réservés. Aucune partie de cette publication ne peut être reproduite, stockée dans un système de recherche documentaire ou transmise, sous quelque forme ou par quelque moyen que ce soit, électronique, mécanique, photocopie, enregistrement ou autre sauf si vous possédez une licence valide, auquel cas vous pouvez reproduire la documentation conformément aux termes de cette licence ou si vous avez le consentement préalable écrit du propriétaire du copyright.

Sophos et Sophos Anti-Virus sont des marques déposées de Sophos Limited. Tous les autres noms de produits et de sociétés mentionnés sont des marques ou des marques déposées appartenant à leurs propriétaires respectifs.

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 chacun de ces logiciels couverts par la licence CPL, le code source est disponible sur commande par courrier postal envoyé à Sophos, par courrier électronique envoyé à support@sophos.fr ou par Internet sur <http://www.sophos.fr/support/queries/enterprise.html>. Une copie du contrat de licence pour chacun des logiciels inclus est disponible sur <http://opensource.org/licenses/cpl1.0.php>

ConvertUTF

Copyright 2001–2004 Unicode, Inc.

This source code is provided as is by Unicode, Inc. No claims are made as to fitness for any particular purpose. No warranties of any kind are expressed or implied. The recipient agrees to determine applicability of information provided. If this file has been purchased on magnetic or optical media from Unicode, Inc., the sole remedy for any claim will be exchange of defective media within 90 days of receipt.

Unicode, Inc. hereby grants the right to freely use the information supplied in this file in the creation of products supporting the Unicode Standard, and to make copies of this file in any form for internal or external distribution as long as this notice remains attached.

iMatix SFL

This product uses parts of the iMatix SFL, Copyright © 1991-2000 iMatix Corporation
<http://www.imatix.com>.