

# SOPHOS

## Sophos Update Manager pour Mac OS X Aide

Version du produit : 2.5

Date du document : mai 2009



## Table des matières

1 A propos de Sophos Update Manager.....	3
2 Mise à jour immédiate de l'installation centralisée depuis Sophos.....	4
3 Configuration de l'installation centralisée pour la mise à jour depuis Sophos.....	5
4 Consultation du journal de mise à jour de l'installation centralisée.....	7
5 Configuration centralisée des Macs.....	8
6 Résolution des problèmes.....	18
7 Support technique.....	19
8 Copyright.....	20

## **1 A propos de Sophos Update Manager**

Sophos Update Manager est un logiciel qui vous permet de :

- mettre à jour l'installation centralisée de Sophos Anti-Virus sur votre serveur Mac avec les mises à jour récupérées depuis Sophos
- configurer tous les Macs de votre réseau pour procéder à la mise à jour depuis l'installation centralisée et aussi, si nécessaire, directement depuis Sophos
- procéder à la configuration centralisée de Sophos Anti-Virus pour tous vos Macs

## **2 Mise à jour immédiate de l'installation centralisée depuis Sophos**

Par défaut, Update Manager procède à la mise à jour de l'installation centralisée depuis Sophos toutes les 10 minutes.

Pour une mise à jour immédiate de l'installation centralisée depuis Sophos :

1. Dans la fenêtre **Sophos Update Manager**, cliquez sur l'icône de la barre d'outils **Mise à jour du logiciel**.
2. Dans le volet **Général**, cliquez sur **Mettre à jour maintenant**.

Update Manager recherche les nouveaux logiciels de Sophos et, si nécessaire, procède à la mise à jour de l'installation centralisée.

## 3 Configuration de l'installation centralisée pour la mise à jour depuis Sophos

### 3.1 Spécification des codes d'accès pour la mise à jour depuis Sophos

Pour permettre à l'installation centralisée de se mettre à jour depuis Sophos, vous devez spécifier des codes d'accès de connexion à Sophos.

Pour spécifier des codes d'accès pour la mise à jour depuis Sophos :

1. Dans la fenêtre **Sophos Update Manager**, cliquez sur l'icône de la barre d'outils **Mise à jour du logiciel**.
2. Dans le volet **Général**, dans les champs **Nom utilisateur** et **Mot de passe**, saisissez les codes d'accès qui vous ont été fournis par Sophos pour que vous puissiez vous connecter au site Web de Sophos.
3. Cliquez sur **Appliquer**.

### 3.2 Modification de l'emplacement de l'installation centralisée

1. Dans la fenêtre **Sophos Update Manager**, cliquez sur l'icône de la barre d'outils **Mise à jour du logiciel**.
2. Dans le volet **Général**, le champ intitulé “**Télécharger les mises à jour dans**” doit contenir l'emplacement que vous avez spécifié lors de l'installation. Cliquez sur **Choisir** et saisissez le nouvel emplacement dans la boîte de dialogue.
3. Cliquez sur **Appliquer**.

### 3.3 Activation ou désactivation de la mise à jour de l'installation centralisée via un proxy

1. Dans la fenêtre **Sophos Update Manager**, cliquez sur l'icône de la barre d'outils **Mise à jour du logiciel**.
2. Dans le volet **Proxy**, spécifiez les préférences comme suit :
  - Pour permettre à Update Manager d'utiliser les paramètres du proxy qui ont été définis dans les Préférences système, choisissez **Utiliser les paramètres du proxy système** dans le menu contextuel.
  - Pour permettre à Update Manager d'utiliser les paramètres proxy que vous avez saisis dans ce volet, choisissez **Utiliser les paramètres proxy personnalisés** dans le menu contextuel. Dans le champ **Adresse**, saisissez l'adresse du proxy. Dans les champs **Nom utilisateur** et **Mot de passe**, saisissez les codes d'accès nécessaires pour accéder au proxy.
  - Pour désactiver la mise à jour via un proxy, choisissez **Ne pas utiliser de proxy** dans le menu contextuel.
3. Cliquez sur **Appliquer**.

## 3.4 Planification de la mise à jour de l'installation centralisée

Par défaut, Update Manager procède à la mise à jour de l'installation centralisée toutes les 10 minutes.

Pour changer la fréquence des mises à jour ou pour désactiver les mises à jour planifiées :

1. Dans la fenêtre **Sophos Update Manager**, cliquez sur l'icône de la barre d'outils **Mise à jour du logiciel**.
2. Dans le volet **Général**, spécifiez les préférences comme suit :
  - Pour changer la fréquence des mises à jour, modifiez la valeur dans le champ intitulé **“Rechercher les mises à jour depuis Sophos toutes les”**, ou sélectionnez une unité de temps différente dans le menu.
  - Pour désactiver les mises à jour planifiées, dessélectionnez la case intitulée **“Rechercher les mises à jour depuis Sophos toutes les”**.
3. Cliquez sur **Appliquer**.

## 3.5 Configuration de la journalisation de la mise à jour de l'installation centralisée

Par défaut, toute activité liée à la mise à jour de l'installation centralisée est journalisée dans le journal Update Manager.

Pour configurer la journalisation de la mise à jour de l'installation centralisée :

1. Dans la fenêtre **Sophos Update Manager**, cliquez sur l'icône de la barre d'outils **Mise à jour du logiciel**.
2. Dans le volet **Journalisation**, spécifiez les préférences comme suit :
  - Pour consigner l'intégralité de l'activité de mise à jour dans le journal système, sélectionnez la case à cocher intitulée **“Se connecter au journal système”**.
  - Pour changer le nom de fichier ou l'emplacement du journal Update Manager, cliquez sur **Choisir** et entrez le nouveau nom de fichier ou d'emplacement dans la boîte de dialogue.
  - Pour désactiver la journalisation dans le journal Update Manager, dessélectionnez la case à cocher intitulée **“Se connecter au fichier”**.
3. Cliquez sur **Appliquer**.

## **4 Consultation du journal de mise à jour de l'installation centralisée**

1. Dans la fenêtre **Sophos Update Manager**, cliquez sur l'icône de la barre d'outils **Mise à jour du logiciel**.
2. Dans le volet **Journalisation**, cliquez sur **Voir le journal**.

Le journal apparaît dans TextEdit.

## 5 Configuration centralisée des Macs

### 5.1 Configuration de la mise à jour

#### 5.1.1 Spécification de la source de mise à jour principale pour les Macs

La source de mise à jour principale est la source habituelle depuis laquelle les Macs de votre réseau vont récupérer les mises à jour de Sophos Anti-Virus.

Pour spécifier la source de mise à jour principale pour les Macs :

1. Dans la fenêtre **Sophos Update Manager**, cliquez sur l'icône de la barre d'outils **Préférences SAV**.
2. En haut du volet **AutoUpdate**, sélectionnez **Paramètres réseau** dans le menu contextuel.
3. Dans le volet **Paramètres réseau**, cliquez sur **Serveur principal**.
4. Dans le volet **Serveur principal**, 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**. 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 **Mettre à jour depuis**. Dans le champ **Adresse**, saisissez l'adresse web de l'installation centralisée. 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 **Mettre à jour depuis**. Dans le champ **Adresse**, saisissez l'adresse du réseau de l'installation centralisée. 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 les parenthèses avec 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 pour faire référence au serveur. L'utilisation d'une adresse IP est préférable si vous avez des problèmes DNS.

5. Cliquez sur **Appliquer**.

Si Sophos Anti-Virus doit accéder à la source de mise à jour via un proxy, reportez-vous à la section [Activation ou désactivation de la mise à jour des Macs via un proxy](#) à la page 9.

## 5.1.2 Spécification de la source de mise à jour secondaire pour les Macs

Si les Macs de votre réseau ne peuvent pas contacter la source de mise à jour principale pour récupérer les mises à jour de Sophos Anti-Virus, ils peuvent essayer de contacter une source secondaire.

Pour spécifier la source de mise à jour secondaire pour les Macs :

1. Dans la fenêtre **Sophos Update Manager**, cliquez sur l'icône de la barre d'outils **Préférences SAV**.
2. En haut du volet **AutoUpdate**, dans le menu contextuel, choisissez **Paramètres réseau**.
3. Dans le volet **Paramètres réseau**, cliquez sur **Serveur secondaire**.
4. Dans le volet **Serveur secondaire**, assurez-vous que la case à cocher intitulée **“Utiliser le serveur secondaire”** est sélectionnée. Puis 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**. 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 **Mettre à jour depuis**. Dans le champ **Adresse**, saisissez l'adresse web de l'installation centralisée. 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 **Mettre à jour depuis**. Dans le champ **Adresse**, saisissez l'adresse du réseau de l'installation centralisée. 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 les parenthèses avec 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 pour faire référence au serveur. L'utilisation d'une adresse IP est préférable si vous avez des problèmes DNS.

5. Cliquez sur **Appliquer**.

Si Sophos Anti-Virus doit accéder à la source de mise à jour via un proxy, reportez-vous à la section [Activation ou désactivation de la mise à jour des Macs via un proxy](#) à la page 9.

## 5.1.3 Activation ou désactivation de la mise à jour des Macs via un proxy

1. Dans la fenêtre **Sophos Update Manager**, cliquez sur l'icône de la barre d'outils **Préférences SAV**.
2. En haut du volet **AutoUpdate**, sélectionnez **Paramètres réseau** dans le menu contextuel.

3. Dans le volet **Paramètres réseau**, cliquez sur **Proxy principal** ou **Proxy secondaire** selon le cas.
4. Dans le volet **Proxy principal** ou dans le volet **Proxy secondaire**, changez les préférences comme suit :
  - Pour que Sophos Anti-Virus puisse utiliser les paramètres du proxy qui ont été définis dans les Préférences système, choisissez **Utiliser les paramètres du proxy système** dans le menu contextuel.
  - Pour permettre à Sophos Anti-Virus d'utiliser les paramètres proxy que vous avez saisis dans ce volet, choisissez **Utiliser les paramètres proxy personnalisés** dans le menu contextuel. Dans le champ **Adresse**, saisissez l'adresse du proxy. Dans les champs **Nom utilisateur** et **Mot de passe**, saisissez les codes d'accès nécessaires pour accéder au proxy.
  - Pour désactiver la mise à jour via un proxy, choisissez **Ne pas utiliser de proxy** dans le menu contextuel.
5. Cliquez sur **Appliquer**.

#### 5.1.4 Planification de la mise à jour des Macs

Par défaut, les installations de Sophos Anti-Virus sur vos Macs se mettent à jour toutes les heures.

Pour changer le moment et la fréquence de mise à jour de Sophos Anti-Virus :

1. Dans la fenêtre **Sophos Update Manager**, cliquez sur l'icône de la barre d'outils **Préférences SAV**.
2. En haut du volet **AutoUpdate**, sélectionnez **Planification et journalisation** dans le menu contextuel.
3. Dans la zone de groupe intitulée "**Rechercher les mises à jour**", changez les préférences comme suit :
  - Pour permettre à Sophos Anti-Virus de se mettre à jour à intervalles réguliers, sélectionnez la case à cocher **Toutes les** et saisissez la durée.
  - Pour permettre à Sophos Anti-Virus de se mettre à jour à chaque fois qu'une connexion réseau est établie, sélectionnez la case à cocher intitulée "**Lors de la connexion au réseau ou à Internet**".
4. Cliquez sur **Appliquer**.

#### 5.1.5 Configuration de la journalisation de la mise à jour des Macs

Par défaut, toute activité liée à la mise à jour d'un Mac particulier est journalisée dans le journal AutoUpdate sur ce Mac.

Pour configurer la journalisation des Macs :

1. Dans la fenêtre **Sophos Update Manager**, cliquez sur l'icône de la barre d'outils **Préférences SAV**.
2. En haut du volet **AutoUpdate**, sélectionnez **Planification et journalisation** dans le menu contextuel.

3. Dans la zone de groupe **Journalisation**, changez les préférences comme suit :
  - Pour consigner l'intégralité de l'activité de mise à jour dans le journal système, sélectionnez la case à cocher intitulée "**Se connecter au journal système**".
  - Pour changer le nom de fichier ou l'emplacement du journal AutoUpdate, cliquez sur **Choisir** et entrez le nouveau nom de fichier ou emplacement dans la boîte de dialogue.
  - Pour désactiver la journalisation dans le journal AutoUpdate, dessélectionnez la case à cocher intitulée "**Se connecter au fichier**".
4. Cliquez sur **Appliquer**.

## 5.2 Activation ou désactivation du contrôle sur accès

Par défaut, le contrôle sur accès est activé automatiquement lorsque vous démarrez vos Macs.  
Pour activer ou désactiver le contrôle sur accès :

1. Dans la fenêtre **Sophos Update Manager**, cliquez sur l'icône de la barre d'outils **Préférences SAV**.
2. Dans la partie supérieure du volet **Contrôle**, choisissez **Général** dans le menu contextuel.
3. Dans le volet **Général**, changez le paramètre comme suit :
  - Pour *activer* le contrôle sur accès, sélectionnez la case à cocher intitulée "**Activer le contrôle sur accès**" et cliquez sur **Appliquer**.
  - Pour *désactiver* le contrôle sur accès, dessélectionnez la case à cocher intitulée "**Activer le contrôle sur accès**" et cliquez sur **Appliquer**.

**Important :** si vous désactivez le contrôle sur accès, Sophos Anti-Virus ne contrôle pas la présence de menaces dans les fichiers auxquels vous accédez. Ceci met vos Macs en danger.

## 5.3 Configuration du contrôle sur accès

### 5.3.1 Ajout d'une exclusion sur accès

Vous pouvez exclure des fichiers, des dossiers et des volumes du contrôle sur accès.

Pour ajouter une exclusion sur accès :

1. Dans la fenêtre **Sophos Update Manager**, cliquez sur l'icône de la barre d'outils **Préférences SAV**.
2. Dans la partie supérieure du volet **Contrôle**, choisissez **Exclusions** dans le menu contextuel.
3. Procédez de l'une des manières suivantes :
  - Faites glisser le ou les élément(s) à exclure dans la liste des éléments exclus.
  - Cliquez sur **Ajouter (+)** et choisissez le ou les élément(s) à exclure de la boîte de dialogue.
4. Cliquez sur **Appliquer**.

### 5.3.2 Modification d'une exclusion sur accès

Vous pouvez exclure des fichiers, des dossiers et des volumes du contrôle sur accès.

Pour modifier une exclusion sur accès :

1. Dans la fenêtre **Sophos Update Manager**, cliquez sur l'icône de la barre d'outils **Préférences SAV**.
2. Dans la partie supérieure du volet **Contrôle**, choisissez **Exclusions** dans le menu contextuel.
3. Dans la liste des éléments exclus, cliquez deux fois sur un élément et modifiez-le.  
Pour plus d'informations sur la détermination des éléments à exclure, reportez-vous à la section [Règles d'exclusion](#) à la page 12.
4. Cliquez sur **Appliquer**.

### 5.3.3 Règles d'exclusion

Lorsque vous ajoutez ou modifiez une exclusion, vous pouvez taper n'importe quel chemin POSIX, qu'il s'agisse d'un volume, d'un dossier ou d'un fichier. Pour spécifier les éléments à exclure, utilisez les règles suivantes :

Élément(s) à exclure	Syntaxe à utiliser
Un dossier et les sous-dossiers de manière récursive	Suffixez l'exclusion avec une barre oblique avant
Un dossier mais sans sous-dossiers	Suffixez l'exclusion avec une double barre oblique avant
Un fichier	Ne suffixez <i>pas</i> l'exclusion avec une barre oblique simple ou double
Un dossier ou un fichier à un emplacement spécifique	Préfixez l'exclusion avec une barre oblique avant
Un dossier ou un fichier n'importe où en local ou sur le réseau	Ne préfixez <i>pas</i> l'exclusion avec une barre oblique avant
Un fichier dont le nom porte une extension spécifique	Remplacez la racine du nom du fichier par un astérisque (*)

#### Exemples

Chemin d'exclusion	Élément(s) à exclure
/MonDossier/MonApplication	Le fichier MonApplication à un emplacement spécifique

Chemin d'exclusion	Élément(s) à exclure
/MonDossier/	Tous les fichiers du dossier MonDossier à un emplacement spécifique et les sous-dossiers de manière récursive
/MonDossier//	Tous les fichiers du dossier MonDossier à un emplacement spécifique mais pas les sous-dossiers
MonDossier/MonApplication	Le fichier MonApplication dans un dossier quelconque appelé MonDossier, localement ou sur le réseau
MonDossier/	Tous les fichiers dans un dossier quelconque appelé MonDossier, localement ou sur le réseau, et les sous-dossiers de manière récursive
MonDossier//	Tous les fichiers dans un dossier quelconque appelé MonDossier, localement ou sur le réseau, mais pas les sous-dossiers
MonApplication	Le fichier MonApplication n'importe où localement ou sur le réseau
*.mov	Tous les fichiers dont l'extension est .mov n'importe où localement ou sur le réseau
/MonDossier/*.mov	Tous les fichiers dont l'extension est .mov à un emplacement spécifique

### 5.3.4 Suppression d'une exclusion sur accès

Vous pouvez exclure des fichiers, des dossiers et des volumes du contrôle sur accès.

Pour supprimer une exclusion sur accès :

1. Dans la fenêtre **Sophos Update Manager**, cliquez sur l'icône de la barre d'outils **Préférences SAV**.
2. Dans la partie supérieure du volet **Contrôle**, choisissez **Exclusions** dans le menu contextuel.
3. Dans la liste des éléments exclus, sélectionnez l'exclusion que vous voulez supprimer et cliquez sur **Supprimer (-)**.
4. Cliquez sur **Appliquer**.

### 5.3.5 Activation du contrôle sur accès dans les archives et les fichiers compressés

Par défaut, le contrôle à l'intérieur des archives et des fichiers compressés est désactivé parce que cela ralentit le contrôle de manière significative et n'est généralement pas nécessaire. Même

si vous n'activez pas l'option, les fichiers qui sont compressés avec des utilitaires de compression dynamique (PKLite, LZEXE et Diet) font l'objet d'un contrôle et lorsque vous tentez d'accéder à un fichier extrait d'une archive, le fichier extrait est contrôlé.

Vous pouvez, par contre, activer l'option afin que le contenu d'une archive ou d'un fichier compressé soit contrôlé avant qu'il ne soit téléchargé ou envoyé par courriel depuis vos Macs.

Pour activer le contrôle sur accès dans les archives et les fichiers compressés :

1. Dans la fenêtre **Sophos Update Manager**, cliquez sur l'icône de la barre d'outils **Préférences SAV**.
2. Dans la partie supérieure du volet **Contrôle**, choisissez **Général** dans le menu contextuel.
3. Dans le volet **Général**, sélectionnez la case à cocher intitulée "**Contrôler dans les archives et les fichiers**".
4. Cliquez sur **Appliquer**.

### 5.3.6 Désactivation du contrôle sur accès des volumes réseau

Par défaut, le contrôle des fichiers auxquels vous accédez sur les volumes réseau est activé.

Pour désactiver le contrôle sur accès des volumes réseau :

1. Dans la fenêtre **Sophos Update Manager**, cliquez sur l'icône de la barre d'outils **Préférences SAV**.
2. Dans la partie supérieure du volet **Contrôle**, choisissez **Général** dans le menu contextuel.
3. Dans le volet **Général**, dessélectionnez la case à cocher intitulée "**Contrôler les volumes**".
4. Cliquez sur **Appliquer**.

### 5.3.7 Désactivation des alertes de bureau

Par défaut, Sophos Anti-Virus affiche une alerte de bureau s'il détecte une menace lors d'un contrôle sur accès.

Pour désactiver les alertes de bureau :

1. Dans la fenêtre **Sophos Update Manager**, cliquez sur l'icône de la barre d'outils **Préférences SAV**.
2. Dans la partie supérieure du volet **Contrôle**, choisissez **Alertes de bureau** dans le menu contextuel.
3. Dans le volet **Alertes de bureau**, dessélectionnez la case à cocher intitulée "**Activer les alertes de bureau**".
4. Cliquez sur **Appliquer**.

### 5.3.8 Configuration de la journalisation du contrôle sur accès

Par défaut, toute l'activité de contrôle sur accès, y compris les virus/spywares trouvés, est journalisée dans le journal Sophos Anti-Virus.

Pour configurer la journalisation du contrôle sur accès :

1. Dans la fenêtre **Sophos Update Manager**, cliquez sur l'icône de la barre d'outils **Préférences SAV**.
2. Dans la partie supérieure du volet **Contrôle**, choisissez **Journalisation** dans le menu contextuel.
3. Dans le volet **Journalisation**, changez les préférences comme suit :
  - Pour journaliser l'activité de contrôle sur accès dans le journal système, sélectionnez la case à cocher intitulée "**Se connecter au journal système**".
  - Pour changer le nom de fichier ou l'emplacement du journal Sophos Anti-Virus, cliquez sur **Choisir** et entrez le nouveau nom de fichier ou emplacement dans la boîte de dialogue.
  - Pour désactiver la journalisation dans le journal Sophos Anti-Virus, désélectionnez la case à cocher intitulée "**Se connecter au fichier**".
4. Cliquez sur **Appliquer**.

## 5.4 Nettoyage

### 5.4.1 A propos du nettoyage

Le nettoyage élimine les menaces sur vos Macs soit en supprimant les virus des fichiers soit en déplaçant ou en supprimant les fichiers infectés. Par contre, il n'annule aucune des opérations déjà exécutées par la menace.

### 5.4.2 Obtention d'informations sur le nettoyage

Lorsqu'une menace est trouvée sur vos Macs, il est très important que vous vérifiez l'analyse lui correspondant sur le site Web de Sophos pour avoir plus d'informations sur la menace ainsi que des conseils sur le nettoyage de vos Macs.

- ❖ Pour voir l'analyse de la menace, allez dans <http://www.sophos.fr/security/analyses/viruses-and-spyware/> et recherchez le nom de cette menace qui apparaît dans le journal de Sophos Anti-Virus, l'alerte de bureau ou la notification par courriel.

### 5.4.3 Configuration du nettoyage pour le contrôle sur accès

Lorsque le contrôle sur accès est activé, Sophos Anti-Virus peut automatiquement désinfecter de nombreux éléments infectés ou assainir des éléments infectés autrement que par la désinfection.

Pour configurer le nettoyage pour le contrôle sur accès :

1. Dans la fenêtre **Sophos Update Manager**, cliquez sur l'icône de la barre d'outils **Préférences SAV**.
2. Dans la partie supérieure du volet **Contrôle**, choisissez **Nettoyage** dans le menu contextuel.

3. Dans le volet **Nettoyage**, changez les préférences comme suit :
  - Pour activer la désinfection automatique des fichiers infectés, sélectionnez la case à cocher intitulée “**Nettoyer automatiquement les éléments contenant des virus ou des spywares**”.
  - Pour déplacer les fichiers infectés à un autre emplacement afin d'empêcher leur exécution, sélectionnez la case à cocher intitulée “**et déplacer dans le dossier**”. Par défaut, les fichiers sont déplacés dans /Users/Shared/Infected/. Pour choisir un emplacement différent, cliquez sur **Choisir** et entrez l'emplacement dans la boîte de dialogue.
  - Pour supprimer les fichiers infectés, sélectionnez le bouton appelé “**supprimer les fichiers infectés**”.
4. Cliquez sur **Appliquer**.

Toutes les actions entreprises par Sophos Anti-Virus contre les éléments infectés sont consignées dans le journal Sophos Anti-Virus.

## 5.5 Configuration de la notification par courriel

Sophos Anti-Virus peut envoyer un courriel s'il détecte une menace ou si une erreur se produit. Par défaut, la notification par courriel est désactivée.

Pour configurer la notification par courriel :

1. Dans la fenêtre **Sophos Update Manager**, cliquez sur l'icône de la barre d'outils **Préférences SAV**.
2. Dans le volet **Notification**, assurez-vous que la case à cocher intitulée “**Activer la notification par courriel**” est sélectionnée.
3. Changez les préférences comme suit :
  - Pour permettre à Sophos Anti-Virus d'envoyer une notification par courriel seulement s'il trouve une menace, sélectionnez **Signaler les menaces**.
  - Pour permettre à Sophos Anti-Virus d'envoyer une notification par courriel s'il trouve une menace ou s'il y a une erreur, sélectionnez **Signaler les menaces et les erreurs**.
  - Pour spécifier l'adresse électronique à laquelle les notifications par courriel doivent être envoyées, entrez l'adresse dans le champ **Destinataire**.
  - Pour spécifier l'adresse électronique avec laquelle les notifications par courriel doivent être envoyées, entrez l'adresse dans le champ **Expéditeur**.
  - Pour spécifier l'adresse du serveur de messagerie à partir duquel les notifications par courriel doivent être envoyées, entrez l'adresse dans le champ **Serveur de messagerie sortante**.
4. Cliquez sur **Appliquer**.

## 5.6 Restauration des préférences par défaut

- ❖ Pour restaurer les préférences par défaut du contrôle sur accès, du nettoyage et des alertes par courriel, dans la fenêtre **Sophos Update Manager**, cliquez sur **Restaurer**.

**Remarque :** le bouton apparaît uniquement lorsque le volet **Contrôle** ou le volet **Notification** est sélectionné.

## 6 Résolution des problèmes

### 6.1 L'installation centralisée n'est pas mise à jour

#### Symptômes

Update Manager ne tente pas de se mettre à jour ou n'est pas en mesure de le faire.

#### Causes

Pour en savoir plus, consultez le journal de la mise à jour. Pour plus d'informations, reportez-vous à la section [Consultation du journal de mise à jour de l'installation centralisée](#) à la page 7.

#### Résolution du problème

- Si Update Manager fournit les mauvais codes d'accès pour effectuer la mise à jour depuis Sophos, reportez-vous à la section [Spécification des codes d'accès pour la mise à jour depuis Sophos](#) à la page 5. Vérifiez que les paramètres sont corrects.
- Si Update Manager procède à la mise à jour d'une installation centralisée différente de celle que attendiez, reportez-vous à la section [Modification de l'emplacement de l'installation centralisée](#) à la page 5. Assurez-vous que la stratégie est correcte.
- Si Update Manager ne peut pas utiliser votre serveur proxy, reportez-vous à la section [Activation ou désactivation de la mise à jour de l'installation centralisée via un proxy](#) à la page 5. Vérifiez que les paramètres sont corrects.
- Si Update Manager ne tente pas de se mettre à jour au moment où vous vous y attendez, reportez-vous à la section [Planification de la mise à jour de l'installation centralisée](#) à la page 6. Vérifiez que les paramètres sont corrects.

### 6.2 Le bouton Mettre à jour maintenant est grisé

#### Symptômes

Le bouton **Mettre à jour maintenant** est grisé dans le volet **Général**.

#### Causes

L'installation centralisée n'est pas configurée pour être mise à jour depuis Sophos

#### Résolution du problème

Reportez-vous à la section [Configuration de l'installation centralisée pour la mise à jour depuis Sophos](#) à la page 5.

## **7 Support technique**

Pour obtenir du support technique, visitez <http://www.sophos.fr/support>.

Si vous contactez le support technique, fournissez autant d'informations que possible, notamment :

- Le ou les numéro(s) de version des logiciels Sophos
- Le(s) système(s) d'exploitation et le(s) niveau(x) de correctif
- Le texte exact de tous les messages d'erreur

## **8 Copyright**

Copyright © 2009 Sophos Group. Tous droits réservés. Aucune partie de cette publication ne peut être reproduite, stockée dans un système de recherche documentaire ou transmise, sous quelque forme ou par quelque moyen que ce soit, électronique, mécanique, photocopie, enregistrement ou autre sauf si vous possédez une licence valide, auquel cas vous pouvez reproduire la documentation conformément aux termes de cette licence ou si vous avez le consentement préalable écrit du propriétaire du copyright.

Sophos et Sophos Anti-Virus sont des marques déposées de Sophos Plc et de Sophos Group. Sophos Group. Tous les autres noms de produits et d'entreprises cités dans ce document sont des marques ou des marques déposées de leurs propriétaires respectifs.