

**SOPHOS**

simple + secure

# Sophos Enterprise Manager Guide de démarrage

Version du produit : 4.7

Date du document : août 2011



# Table des matières

1 À propos de ce guide.....	3
2 Quelles sont les étapes essentielles ?.....	3
3 Vérification de la configuration système requise.....	4
4 Préparation de l'installation.....	5
5 Téléchargement du programme d'installation.....	5
6 Installation d'Enterprise Manager .....	5
7 Téléchargement des logiciels de sécurité.....	6
8 Création de groupes d'ordinateurs.....	6
9 Configuration des stratégies de sécurité.....	7
10 Recherche d'ordinateurs.....	8
11 Protection des ordinateurs Windows.....	9
12 Protection des ordinateurs Mac OS X.....	13
13 Protéger les ordinateurs Linux.....	14
14 Vérification du bon fonctionnement de votre réseau.....	16
15 Résolution des problèmes.....	16
16 Aide sur les tâches les plus courantes.....	16
17 Annexe : passage à l'Enterprise Manager à partir de l'Enterprise Console.....	17
18 Support technique.....	20
19 Mentions légales.....	21

## 1 À propos de ce guide

Ce guide vous indique comment installer la version 4.7 de Sophos Enterprise Manager et protéger votre réseau avec les logiciels de sécurité Sophos.

Sophos Enterprise Manager est une console automatisée qui gère et met à jour les logiciels de sécurité Sophos sur les ordinateurs Windows, Mac et Linux. Enterprise Manager vous permet de :

- Protéger votre réseau contre les virus, chevaux de Troie, vers, spywares, sites Web malveillants et autres menaces inconnues, et contre les adwares et autres applications potentiellement indésirables.
- Administrer la protection du pare-feu client sur les ordinateurs d'extrémité.
- Empêcher l'utilisation de périphériques de stockage externes non autorisés et de technologies de connexion sans fil sur des ordinateurs d'extrémité.
- Empêcher l'utilisateur de reconfigurer, désactiver ou désinstaller les logiciels de sécurité Sophos.

Pour voir une liste des fonctions de l'Enterprise Manager et obtenir des informations sur ce qui fait la différence entre l'Enterprise Manager et ses licences et les autres produits Sophos et leurs licences, consultez l'article 113711 de la base de connaissances du support de Sophos (<http://www.sophos.fr/support/knowledgebase/article/113711.html>).

### Changement à partir de l'Enterprise Console

Ce guide vous indique également les étapes supplémentaires à exécuter si vous voulez désinstaller l'Enterprise Console et installer Enterprise Manager.

**Important :** la mise à niveau inférieure depuis l'Enterprise Console vers Enterprise Manager n'est pas prise en charge. Vous devez désinstaller l'Enterprise Console, puis installer Enterprise Manager comme le décrit ce guide et le paramétrer.

Vous allez perdre tous vos paramètres Enterprise Console.

Avant de désinstaller l'Enterprise Console, prenez note de vos paramètres existants et sauvegardez la base de données Enterprise Console comme le décrit la section [Annexe : passage à l'Enterprise Manager à partir de l'Enterprise Console](#) à la page 17.

## 2 Quelles sont les étapes essentielles ?

Exécutez les étapes essentielles suivantes :

- Vérification de la configuration système requise.
- Préparation de l'installation.
- Téléchargement du programme d'installation.
- Installation d'Enterprise Manager.
- Téléchargement des logiciels de sécurité.

- Création de groupes d'ordinateurs.
- Configuration des stratégies de sécurité.
- Recherche d'ordinateurs.
- Protection des ordinateurs.
- Vérification du bon fonctionnement de votre réseau.

## 3 Vérification de la configuration système requise

Avant de commencer l'installation, vérifiez la configuration requise pour le matériel, le système d'exploitation et le logiciel système.

### 3.1 Matériel et système d'exploitation

Pour plus d'informations sur la configuration requise, consultez la page Configuration requise sur le site Web de Sophos (<http://www.sophos.fr/products/all-sysreqs.html>).

### 3.2 Logiciels système Microsoft

Enterprise Manager requiert certains logiciels système Microsoft (par exemple, des logiciels de base de données).

Si ce logiciel système n'est pas déjà disponible sur votre serveur, le programme d'installation d'Enterprise Manager tente de l'installer. Par contre, dans certains cas, le logiciel est incompatible avec votre serveur ou doit être installé manuellement.

#### Installation de SQL Server

Le programme d'installation tente d'installer SQL Server 2008 Express, sauf si vous êtes déjà équipé de SQL Server 2005 Express ou supérieur. Sachez que :

- Nous vous conseillons de ne pas installer SQL Server sur un contrôleur de domaine.
- SQL Server 2008 Express n'est pas compatible avec Windows Server 2003 SP1 ou Windows XP 64 bits ou Windows Essential Business Server 2008.
- Sous Windows Server 2008 R2 Datacenter, vous devez élever le niveau fonctionnel du domaine à Windows Server 2003, comme cela est expliqué dans <http://support.microsoft.com/kb/322692>.

#### Installation de .NET Framework

Le programme d'installation tente d'installer .NET Framework 3.5 sauf s'il est déjà installé. Sachez que :

- Le programme d'installation ne peut pas installer .NET Framework 3.5 sur un ordinateur utilisant Windows Server 2008 R2. Vous devez l'ajouter depuis la section Fonctions du Gestionnaire de serveur.

**Remarque :** après avoir installé les logiciels système requis, redémarrez vos ordinateurs. Pour plus d'informations, consultez les articles 65190 et 111220 de la base de connaissances du

support Sophos (<http://www.sophos.fr/support/knowledgebase/article/65190.html> et <http://www.sophos.fr/support/knowledgebase/article/111220.html>).

## 4 Préparation de l'installation

Sélectionnez un serveur satisfaisant à la configuration système requise et procédez de la manière suivante :

- Assurez-vous d'être connecté à Internet.
- Assurez-vous d'avoir le CD-ROM du système d'exploitation de Windows et les CD-ROM des Service Packs. Il se peut que vous soyez invité à les utiliser lors de l'installation.
- Si le serveur exécute Windows Server 2008 ou supérieur, désactivez le Contrôle de compte d'utilisateur et redémarrez le serveur.

**Remarque :** vous pouvez réactiver le Contrôle de compte d'utilisateur après avoir terminé l'installation et téléchargé vos logiciels de sécurité.

## 5 Téléchargement du programme d'installation

Téléchargez le programme d'installation Sophos et placez-le sur le serveur sur lequel vous souhaitez installer la console d'administration :

1. Rendez-vous sur <http://www.sophos.fr/support/updates/>.
2. Saisissez votre nom utilisateur et mot de passe MySophos.
3. Sur la page Web **Téléchargements et mises à jour**, téléchargez le programme d'installation d'Enterprise Manager.
4. Si nécessaire, copiez le programme d'installation téléchargé sur le serveur sur lequel vous désirez effectuer l'installation.

## 6 Installation d'Enterprise Manager

Pour installer Enterprise Manager :

1. Sur l'ordinateur sur lequel vous souhaitez installer Enterprise Manager, ouvrez une session avec les droits administrateur.
  - Si l'ordinateur est dans un domaine, ouvrez une session en tant qu'administrateur de domaine.
  - Si l'ordinateur est dans un groupe de travail, connectez-vous en tant qu'administrateur local.
2. Recherchez le programme d'installation d'Enterprise Manager que vous avez téléchargé auparavant.
3. Cliquez deux fois sur le programme d'installation.

4. Dans la boîte de dialogue du programme d'installation réseau, cliquez sur **Installer**.  
Les fichiers d'installation sont copiés sur l'ordinateur et l'assistant d'installation démarre.
5. Sur la page de Bienvenue de l'assistant d'installation de Sophos Enterprise Manager, cliquez sur **Suivant**.
6. Un assistant vous guide tout au long de l'installation. Acceptez les valeurs par défaut partout où c'est possible.
7. Une fois l'installation terminée, il se peut que vous soyez invité à redémarrer. Cliquez sur **Oui** ou sur **Terminer**.

## 7 Téléchargement des logiciels de sécurité

Lorsque vous rouvrez une session (ou redémarrez) pour la première fois après l'installation, Enterprise Manager s'ouvre automatiquement et un assistant se lance.

**Remarque :** si vous avez utilisé le Bureau à distance pour l'installation, la console ne s'ouvre pas automatiquement. Ouvrez-la depuis le menu Démarrer.

L'assistant vous guide tout au long des opérations de sélection et de téléchargement des logiciels de sécurité. Procédez ainsi :

1. Sur la page **Détails du compte de téléchargement Sophos**, saisissez le nom utilisateur et le mot de passe imprimés sur votre annexe de licence. Si vous accédez à Internet via un serveur proxy, sélectionnez la case à cocher **Accéder à Sophos via un serveur proxy**.
2. Sur la page **Sélection des plates-formes**, sélectionnez les plates-formes que vous souhaitez protéger.

Lorsque vous cliquez sur **Suivant**, Enterprise Manager commence à télécharger vos logiciels.

3. Sur la page **Téléchargement des logiciels**, vous pouvez voir la progression du téléchargement. Cliquez sur **Suivant** à n'importe quel moment.
4. Sur la page **Importation des ordinateurs depuis Active Directory**, sélectionnez la case **Définir des groupes pour vos ordinateurs** si vous voulez qu'Enterprise Manager utilise vos groupes d'ordinateurs Active Directory existants.

**Remarque :** si un ordinateur est ajouté à plus d'un conteneur Active Directory, cela va entraîner un problème d'échange continu de messages entre l'ordinateur et Enterprise Manager.

Les logiciels que vous avez sélectionnés sont téléchargés dans le partage \\nom serveur\SophosUpdate, où *nom serveur* est le nom du serveur sur lequel Enterprise Manager est installé.

Si vous avez désactivé le Contrôle de compte d'utilisateur avant l'installation, vous pouvez le réactiver.

## 8 Création de groupes d'ordinateurs

Avant de pouvoir protéger et administrer les ordinateurs, vous devez leur créer des groupes.

Grâce aux groupes, vous pouvez :

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

Si vous avez déjà configuré vos groupes d'ordinateurs basés sur les groupes Active Directory à l'aide de l'**Assistant de téléchargement des logiciels de sécurité**, vous pouvez passer cette section. Rendez-vous sur [Configuration des stratégies de sécurité](#) à la page 7.

1. Si l'Enterprise Manager n'est pas déjà ouvert, ouvrez-le.
2. Dans le volet **Groupes** (sur le côté gauche de la console), assurez-vous que le nom du serveur qui apparaît en haut est sélectionné.
3. Dans la barre d'outils, cliquez sur l'icône **Créer un groupe**.  
Un "Nouveau groupe" est ajouté à la liste et son nom est mis en surbrillance.
4. Saisissez un nouveau nom pour le groupe.

Pour créer d'autres groupes, allez dans le volet de gauche. Sélectionnez le premier serveur affiché si vous désirez créer un autre groupe principal. Sélectionnez un groupe si vous voulez créer un sous-groupe dans le groupe principal. Puis créez et nommez le groupe comme précédemment.

## 9 Configuration des stratégies de sécurité

### Stratégies par défaut

L'Enterprise Manager applique les stratégies de sécurité "par défaut" à vos groupes d'ordinateurs. Sauf si vous le souhaitez, il n'est pas nécessaire de changer ces stratégies, avec les exceptions suivantes :

- Vous devez configurer une stratégie de pare-feu. Reportez-vous à la section [Configuration d'une stratégie de pare-feu](#) à la page 8.
- Vous devez modifier les stratégies de contrôle des périphériques et de protection antialtération si vous voulez utiliser ces fonctions. Vous pouvez effectuer cette opération à tout moment.

Pour plus d'informations sur l'activation et la configuration des stratégies de contrôle des périphériques et de protection antialtération, reportez-vous aux sections *Configuration de la stratégie de contrôle des périphériques* et *Configuration de la stratégie de protection antialtération* de l'Aide de l'Enterprise Manager.

### Création de nouvelles stratégies

Dans l'Enterprise Manager, vous pouvez créer jusqu'à quatre nouvelles stratégies de chaque type. Une fois que vous avez atteint cette limite, les options **Créer une stratégie** et **Dupliquer une stratégie** sont désactivées.

Pour créer une nouvelle stratégie :

1. Dans la vue **Ordinateurs d'extrémité**, dans le volet **Stratégies**, cliquez avec le bouton droit de la souris sur le type de stratégie que vous désirez créer, par exemple "Mise à jour" et sélectionnez **Créer une stratégie**.

Une "Nouvelle stratégie" est ajoutée à la liste et son nom est mis en surbrillance.

2. Saisissez un nouveau nom pour cette stratégie.
3. Cliquez deux fois sur la nouvelle stratégie. Saisissez les paramètres de votre choix.

Pour obtenir des instructions sur la manière de choisir les paramètres, reportez-vous à la section sur la configuration de la stratégie appropriée.

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

### **Affectation de stratégies aux groupes**

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

## **9.1 Configuration d'une stratégie de pare-feu**

Par défaut, le pare-feu est activé et bloque tout le trafic non indispensable. Par conséquent, vous devez le configurer pour qu'il autorise les applications que vous souhaitez utiliser puis le tester avant de procéder à son installation sur tous les ordinateurs. Consultez le *guide de configuration des stratégies de Sophos Enterprise Manager* pour plus de conseils.

Vous pouvez paramétrer les options de configuration principales pour le pare-feu dans l'**Assistant de stratégie de pare-feu**.

1. Dans le volet **Stratégie**, cliquez deux fois sur **Pare-feu**.
2. Cliquez deux fois sur la stratégie **Par défaut** pour la modifier. Un assistant se lance.
3. Dans l'**Assistant de stratégie de pare-feu**, nous vous conseillons d'effectuer les sélections suivantes.
  - a) Sur la page **Configuration du pare-feu**, sélectionnez **Emplacement unique** sauf si vous voulez que le pare-feu utilise des paramètres différents en fonction de l'endroit où vous l'utilisez.
  - b) Sur la page **Mode de fonctionnement**, sélectionnez **Bloquer le trafic entrant et autoriser le trafic sortant**.
  - c) Sur la page **Partage de fichiers et d'imprimante**, sélectionnez **Autoriser le partage de fichiers et d'imprimante**.

## **10 Recherche d'ordinateurs**

Recherchez les ordinateurs sur le réseau avant qu'Enterprise Manager ne puisse les protéger et les administrer.

Si vous avez déjà configuré vos groupes d'ordinateurs basés sur les groupes Active Directory à l'aide de l'**Assistant de téléchargement des logiciels de sécurité**, vous pouvez passer cette section. Rendez-vous à la section [Protection des ordinateurs Windows](#) à la page 9.

1. Cliquez sur l'icône **Rechercher de nouveaux ordinateurs** dans la barre d'outils.
2. Sélectionnez la méthode que vous voulez utiliser pour rechercher des ordinateurs.
  - Si vous utilisez l'option **Importer depuis Active Directory** et choisissez ensuite d'importer les ordinateurs et les conteneurs, les ordinateurs sont placés dans leurs groupes respectifs.
  - Si vous utilisez une des options de **Recherche**, les ordinateurs sont placés dans le groupe **Non affectés**.
3. Saisissez les détails du compte, si nécessaire, et spécifiez où vous voulez effectuer la recherche.
4. Si vous avez utilisé une des options de **Recherche**, cliquez sur le groupe **Non affectés** pour voir les ordinateurs qui ont été trouvés. Pour commencer à gérer les ordinateurs, sélectionnez-les et faites les glisser dans un groupe.

## 11 Protection des ordinateurs Windows

Cette section vous indique comment protéger vos ordinateurs Windows automatiquement ou manuellement si les ordinateurs ne peuvent pas être protégés automatiquement.

### 11.1 Préparation de la protection automatique des ordinateurs

Avant de protéger les ordinateurs, préparez-les de la manière suivante :

- Préparez la suppression automatique des logiciels de sécurité tiers.
- Vérifiez que votre compte peut être utilisé pour l'installation du logiciel
- Préparez l'installation du logiciel antivirus

#### 11.1.1 Préparation à la suppression automatique des logiciels de sécurité tiers

Si vous voulez que le programme d'installation Sophos supprime tout logiciel de sécurité précédemment installé, procédez ainsi :

- Si les ordinateurs utilisent le logiciel antivirus d'un autre éditeur, veillez à ce que son interface utilisateur soit fermée.
- Si les ordinateurs utilisent le pare-feu ou le produit HIPS d'un autre éditeur, veillez à ce qu'il soit désactivé ou configuré pour permettre au programme d'installation Sophos de s'exécuter.

Si les ordinateurs utilisent l'outil de mise à jour d'un autre éditeur, vous pouvez le supprimer si vous le désirez. Reportez-vous à la section *Suppression des logiciels de sécurité tiers* de la section *Protection des ordinateurs* de l'*Aide de l'Enterprise Manager* .

### 11.1.2 Vérification que votre compte peut être utilisé pour l'installation du logiciel

Lorsque vous procédez à la protection automatique, dans l'**Assistant de protection des ordinateurs**, vous êtes invité à saisir les détails d'un compte qui peut être utilisé pour installer le logiciel de sécurité. Généralement, il s'agit d'un compte d'administrateur de domaine. Il doit impérativement :

- Posséder les droits d'administrateur local sur les ordinateurs que vous souhaitez protéger.
- Pouvoir se connecter à l'ordinateur sur lequel vous avez installé l'Enterprise Manager.
- Avoir un accès en lecture à l'emplacement depuis lequel les ordinateurs se mettront à jour.

Par défaut, les ordinateurs se mettent à jour à partir d'une seule source principale de mise à jour dans un partage UNC, \\<NomOrdinateur>\SophosUpdate, où <NomOrdinateur> correspond au nom de l'ordinateur sur lequel l'Enterprise Manager est installée. Pour vérifier cet emplacement, dans le volet **Stratégies**, cliquez deux fois sur **Mise à jour** puis cliquez deux fois sur la stratégie que vous souhaitez mettre à jour.

### 11.1.3 Préparation de l'installation du logiciel antivirus

Préparez les ordinateurs à l'installation du logiciel antivirus. Les étapes de préparation diffèrent selon le système d'exploitation.

**Remarque :** si aucun système d'exploitation n'apparaît ici, il est inutile de préparer les ordinateurs à exécuter ce système.

#### 11.1.3.1 Préparation des ordinateurs Windows 7

Préparez les ordinateurs Windows 7 à l'installation du logiciel antivirus en suivant les étapes ci-dessous.

Si vous utilisez Active Directory, vous pouvez également choisir de préparer vos ordinateurs Windows 7 en utilisant un Objet de stratégie de groupe dans Windows 2008 et dans Windows 2008 R2. Consultez l'article 62730 de la base de connaissances du support de Sophos (<http://www.sophos.fr/support/knowledgebase/article/111180.html>).

1. Dans le Panneau de configuration, ouvrez le Centre Réseau et partage. Pour l'emplacement **Réseau professionnel**, assurez-vous que les options sont configurées ci-dessous :
  - Recherche du réseau : activé
  - Partage de fichiers et d'imprimantes : activé
  - Connexions de partage de fichiers : activer le partage de fichiers pour les périphériques qui utilisent le chiffrement 40 ou 56 bits
  - Partage protégé par mot de passe : désactivé
2. Assurez-vous que le service Registre à distance est lancé et que son type de démarrage est défini sur Automatique.
3. Définissez le Contrôle de compte d'utilisateur sur **Ne jamais notifier**. Une fois l'installation terminée, rétablissez cette option sur **Par défaut**.

4. Désactivez l'Assistant Partage.
5. Ouvrez le Pare-feu Windows avec fonctions avancées de sécurité en allant dans le Panneau de configuration et en cliquant sur **Outils d'administration**.
  - a) Assurez-vous que les **Connexions entrantes** sont autorisées.
  - b) Changez les **Règles de trafic entrant** pour activer les processus ci-dessous. Une fois l'installation terminée, désactivez de nouveau ces processus.
    - Administration à distance (NP-Entrée) Domaine
    - Administration à distance (NP-Entrée) Privé
    - Administration à distance (RPC) Domaine
    - Administration à distance (RPC) Privé
    - Administration à distance (RPC-EPMAP) Domaine
    - Administration à distance (RPC-EPMAP) Privé

### 11.1.3.2 Préparation des ordinateurs Windows Vista

1. Dans le Panneau de configuration, ouvrez le Centre Réseau et partage. Assurez-vous que les options sont configurées comme ci-dessous :
  - Recherche du réseau : activé
  - Partage de fichiers : activé
  - Partage d'imprimantes : activé
  - Partage protégé par mot de passe : désactivé
2. Assurez-vous que le service Registre à distance est lancé et que son type de démarrage est défini sur Automatique.
3. Désactivez le Contrôle des comptes d'utilisateurs. Une fois l'installation terminée, activez de nouveau cette option.
4. Désactivez l'Assistant Partage.
5. Ouvrez le Pare-feu Windows avec fonctions avancées de sécurité en allant dans le Panneau de configuration et en cliquant sur **Outils d'administration**.
  - a) Assurez-vous que les **Connexions entrantes** sont autorisées.
  - b) Changez les **Règles de trafic entrant** pour activer les processus ci-dessous. Une fois l'installation terminée, désactivez de nouveau ces processus.
    - Administration à distance (NP-Entrée) Domaine
    - Administration à distance (NP-Entrée) Privé
    - Administration à distance (RPC) Domaine
    - Administration à distance (RPC) Privé
    - Administration à distance (RPC-EPMAP) Domaine
    - Administration à distance (RPC-EPMAP) Privé

### 11.1.3.3 Préparation des ordinateurs Windows 2003/XP Pro/2000

1. Assurez-vous que les services Registre à distance, Serveur, Explorateur d'ordinateur et Planificateur de tâches sont démarrés.
2. Assurez-vous que le partage admin C\$ est activé.
3. Assurez-vous que le Partage de fichiers simple est désactivé (XP Pro uniquement).

### 11.1.3.4 Préparation des ordinateurs Windows XP (SP2 ou supérieur)

**Remarque :** pour les ordinateurs Windows XP Pro, reportez-vous à la section [Préparation des ordinateurs Windows 2003/XP Pro/2000](#) à la page 12.

1. Assurez-vous que les services Registre à distance, Serveur, Explorateur d'ordinateur et Planificateur de tâches sont démarrés.
2. Assurez-vous que le partage admin C\$ est activé.
3. Assurez-vous que Partage de fichiers simple est désactivé.
4. Activez le Partage de fichiers et d'imprimantes pour les réseaux Microsoft.
5. Assurez-vous que les ports TCP 8192, 8193 et 8194 sont ouverts.
6. Redémarrez l'ordinateur pour appliquer les changements.

## 11.2 Protection automatique des ordinateurs Windows

Pour protéger les ordinateurs, procédez ainsi :

1. Sélectionnez les ordinateurs que vous voulez protéger.
2. Cliquez avec le bouton droit de la souris et sélectionnez **Protéger les ordinateurs**.

**Remarque :** si des ordinateurs sont dans le dossier **Non affectés**, faites-les simplement glisser dans les groupes de votre choix.

3. Un assistant vous guide tout au long de l'installation du logiciel de sécurité Sophos. Procédez ainsi :

- a) Sur la page **Sélection des fonctions**, sélectionnez toutes les fonctions optionnelles que vous désirez.

La fonction antivirus est toujours installée.

Sophos Client Firewall n'est pas pris en charge sur les systèmes d'exploitation serveur.

**Important :** assurez-vous de bien avoir configuré le pare-feu pour qu'il autorise le trafic, les applications et les processus que vous souhaitez utiliser avant de l'installer et de l'exécuter sur tous les ordinateurs. Reportez-vous à la section [Configuration d'une stratégie de pare-feu](#) à la page 8.

- b) Sur la page **Récapitulatif de la protection**, recherchez tous les problèmes relatifs à l'installation. Pour plus d'aide, reportez-vous à la section [Résolution des problèmes](#) à la page 16.
- c) Sur la page **Codes d'accès**, saisissez les détails d'un compte qui peut être utilisé pour installer le logiciel sur les ordinateurs.

L'installation s'effectue par étapes, ainsi l'opération peut prendre un certain temps avant de se terminer sur tous les ordinateurs.

**Remarque :** au cours de l'installation du pare-feu, les cartes réseau sont déconnectées temporairement. Cette interruption peut entraîner la déconnexion des applications en réseau telle que le Bureau à distance.

Pour vérifier l'état de protection des ordinateurs, sélectionnez soit le groupe dans lequel vous avez placé les ordinateurs soit le serveur apparaissant en haut de la liste pour voir tous les ordinateurs. Lorsque l'installation est terminée, dans la liste des ordinateurs, dans la colonne **Sur accès**, le mot **Actif** indique que le contrôle antivirus sur accès fonctionne sur cet ordinateur.

### 11.3 Protection manuelle des ordinateurs Windows

Si vous avez des ordinateurs que vous ne pouvez pas protéger automatiquement, protégez-les en exécutant un programme d'installation depuis un dossier partagé dans lequel le logiciel de sécurité a été téléchargé. Ce dossier est plus connu sous le nom d'emplacement du fichier d'amorce.

1. Pour savoir dans quel répertoire le programme figure, ouvrez Enterprise Manager. Dans le menu **Affichage**, cliquez sur **Emplacements des fichiers d'amorce**.

Dans la boîte de dialogue **Emplacements des fichiers d'amorce**, la colonne **Emplacement** affiche le chemin de l'emplacement du fichier d'amorce pour chaque plate-forme.

2. Allez sur chaque ordinateur et connectez-vous avec les droits d'administrateur local.
3. Recherchez le programme de configuration dans l'emplacement du fichier d'amorce et cliquez deux fois dessus.

Pour Windows, le programme est appelé setup.exe.

4. Un assistant vous guide tout au long de l'installation.

## 12 Protection des ordinateurs Mac OS X

L'installation automatique n'est pas possible sur les ordinateurs Mac. Protégez-les en exécutant un programme d'installation depuis un dossier partagé dans lequel le logiciel de sécurité pour ordinateurs d'extrémité a été téléchargé. Ce dossier est plus connu sous le nom d'emplacement du fichier d'amorce.

1. Pour savoir dans quel répertoire le programme figure, ouvrez Enterprise Manager. Dans le menu **Affichage**, cliquez sur **Emplacements des fichiers d'amorce**.

Dans la boîte de dialogue **Emplacements des fichiers d'amorce**, la colonne **Emplacement** affiche le chemin de l'emplacement du fichier d'amorce pour chaque plate-forme.

2. Allez sur chaque ordinateur et connectez-vous avec les droits d'administrateur local.
3. Recherchez le programme de configuration dans l'emplacement du fichier d'amorce et cliquez deux fois dessus.

Pour Mac OS X, le programme est appelé Sophos Anti-Virus.mpkg.

4. Un assistant vous guide tout au long de l'installation.

## 13 Protéger les ordinateurs Linux

Pour protéger les ordinateurs Linux, vous devez :

- Créer un package de déploiement.
- Installer Sophos Anti-Virus sur les ordinateurs Linux.

### 13.1 Création d'un package de déploiement

Dans cette section, on suppose que vous avez téléchargé Sophos Anti-Virus pour Linux, comme l'explique la section [Téléchargement des logiciels de sécurité](#) à la page 6.

Vous pouvez utiliser le script **mkinstpkg** pour créer un package de déploiement pour vos utilisateurs. Ce script vous invite à donner des informations sur la manière dont Sophos Anti-Virus va être installé sur vos ordinateurs Linux. Les réponses collectées sont ensuite insérées dans le package de déploiement. Lorsque l'utilisateur final installe depuis ce package de déploiement, ce dernier ne demande aucune information et configure correctement à la fois l'emplacement et les codes d'accès de mise à jour. Vous pouvez créer un package au format tar ou RPM.

**Remarque :** le script **mkinstpkg** est uniquement réservé à une utilisation au sein de votre entreprise. Veuillez lire le contrat de licence et la notice légale affichés par le script **mkinstpkg**.

Pour créer un package de déploiement :

1. Pour connaître le chemin du dossier partagé (connu sous le nom d'emplacement des fichiers d'amorce) dans lequel Sophos Anti-Virus a été téléchargé :

- a) Dans Enterprise Manager, dans le menu **Affichage**, cliquez sur **Emplacements des fichiers d'amorce**.

Dans la boîte de dialogue **Emplacements des fichiers d'amorce**, la colonne **Emplacement** affiche le chemin de l'emplacement du fichier d'amorce pour chaque plate-forme.

- b) Notez le nom du chemin.

2. Ouvrez une session sur votre serveur Linux en tant que root.

3. Montez l'emplacement du fichier d'amorce.

Pour autoriser le montage automatique de ce dossier au redémarrage du système, utilisez les outils de distribution spécifiques à cette tâche ou éditez fstab.

4. Changez l'emplacement du fichier d'amorce.

5. Pour créer un package de déploiement au format tar, appelé savinstpkg.tgz, saisissez :  
**./mkinstpkg.sh**

Pour créer un package de déploiement au format RPM, appelé savinstpkg-0.0-1.i586.rpm, saisissez :

**./mkinstpkg.sh -r**

**Remarque :** le nom de fichier peut varier selon la configuration RPM.

6. Lorsqu'on vous le demande, choisissez d'activer l'administration à distance.
7. Lorsqu'on vous demande l'emplacement, saisissez l'emplacement du fichier d'amorce (comme abordé au sujet des ordinateurs Linux).

Vous êtes maintenant prêt à installer Sophos Anti-Virus à l'aide de ce package de déploiement.

## 13.2 Installation de Sophos Anti-Virus pour Linux à l'aide du package de déploiement

Utilisez le package d'installation de Sophos Anti-Virus de deux manières différentes :

- Manuellement sur chaque ordinateur. Cette approche est possible uniquement avec un package au format RPM ou tar.
- Automatiquement sur l'ensemble du réseau. Cette approche est possible uniquement avec un package au format RPM.

**Remarque :** sous la version 6 en 64 bits de Red Hat Enterprise Linux, les packages suivants doivent être installés pour que l'installation de Sophos Anti-Virus réussisse :

- glibc-2.11.1-1.i686
- nss-softokn-freebl i686 3.12.4-10.fc12

### 13.2.1 Installation manuelle de Sophos Anti-Virus pour Linux

1. Utilisez vos propres outils pour copier le package de distribution sur les ordinateurs sur lesquels vous voulez installer Sophos Anti-Virus.
2. Rendez-vous sur chaque ordinateur et ouvrez une session en tant que root.
3. Placez le package de déploiement dans un répertoire temporaire et passez dans ce répertoire.
4. Pour installer depuis le package tar, saisissez :  
**tar -zxvf savinstpkg.tgz**  
**./sophos-av/install.sh**

Pour installer depuis le package RPM, saisissez :

**rpm -i RPM package**

Les fichiers nécessaires sont copiés depuis le serveur et Sophos Anti-Virus est installé. Désormais, Sophos Anti-Virus sera mis à jour automatiquement à chaque mise à jour de l'emplacement du fichier d'amorce.

### 13.2.2 Installation automatique de Sophos Anti-Virus pour Linux

- ❖ Pour installer Sophos Anti-Virus automatiquement depuis le package de déploiement, utilisez l'un des outils d'administration de systèmes d'exploitation prenant en charge le déploiement à distance.

Pour plus d'informations, reportez-vous à la documentation concernant cet outil.

Dès que Sophos Anti-Virus est installé, il démarre et il est automatiquement mis à jour à chaque mise à jour de l'emplacement du fichier d'amorce.

## 14 Vérification du bon fonctionnement de votre réseau

Pour vérifier le bon fonctionnement de votre réseau à partir d'Enterprise Manager, dans la barre de menus, cliquez sur l'icône du **Tableau de bord** (si le Tableau de bord n'est pas déjà affiché).

Le Tableau de bord vous montre combien d'ordinateurs :

- Ont détecté des menaces.
- Ne sont pas à jour.
- Ne sont pas conformes aux stratégies.

## 15 Résolution des problèmes

Lorsque vous exécutez l'assistant de protection des ordinateurs, l'installation des logiciels de sécurité peut échouer pour un certain nombre de raisons :

- L'installation automatique avec Enterprise Manager n'est pas possible sur les ordinateurs Mac et Linux. Pour plus d'informations sur la manière de protéger ces systèmes d'exploitation, reportez-vous aux sections [Protection des ordinateurs Mac OS X](#) à la page 13 et [Protéger les ordinateurs Linux](#) à la page 14.
- Le système d'exploitation n'a pas pu être déterminé. Vous n'avez peut-être pas saisi votre nom utilisateur au format domaine\nomutilisateur lors de la recherche des ordinateurs.
- Les ordinateurs exécutent un pare-feu.

## 16 Aide sur les tâches les plus courantes

Pour plus d'informations sur la manière d'effectuer les tâches communes; reportez-vous aux sections de l'*Aide de l'Enterprise Manager* :

- *Configuration des stratégies*
  - *Configuration de la stratégie antivirus et HIPS*
  - *Configuration de la stratégie de pare-feu*
  - *Configuration de la stratégie de contrôle des périphériques*
  - *Configuration de la stratégie de protection antialtération*
- *Protection des ordinateurs*
  - *Traitement des alertes et des erreurs*
  - *Nettoyage des ordinateurs*

### ■ Génération de rapports

Pour obtenir des instructions sur le paramétrage des stratégies, reportez-vous également au *Guide de configuration des stratégies de Sophos Enterprise Manager*.

## 17 Annexe : passage à l'Enterprise Manager à partir de l'Enterprise Console

Lorsque vous désinstallerez l'Enterprise Console, puis installerez l'Enterprise Manager, tous vos paramètres Enterprise Console seront perdus. Les ordinateurs seront déplacés dans le groupe **Non affectés** et les stratégies rétablies à leurs valeurs par défaut.

Prenez note de votre configuration existante. Cela facilitera la nouvelle création des groupes d'ordinateurs et la configuration des stratégies dans Enterprise Manager.

Vous pouvez exporter les paramètres de configuration de la stratégie de pare-feu depuis Enterprise Console version 4.5 ou 4.7 et les importer dans Enterprise Manager. Pour de plus amples instructions sur la manière de procéder, consultez la section qui suit.

Si vous utilisez actuellement Sophos NAC (contrôle d'accès réseau), supprimez-le de votre réseau. Si vous utilisez les fonctions de contrôle des données et de contrôle des applications, il est par ailleurs conseillé de les désactiver avant de désinstaller l'Enterprise Console.

**Important :** avant de désinstaller l'Enterprise Console, sauvegardez la base de données Enterprise Console comme le décrit la section [Sauvegarde de la base de données Enterprise Console](#) à la page 19.

### 17.1 Exportation et importation des paramètres de configuration du pare-feu

Pour exporter les paramètres de configuration des stratégies de pare-feu depuis l'Enterprise Console et les importer dans Enterprise Manager :

1. Dans l'Enterprise Console, dans le volet **Stratégies**, cliquez deux fois sur **Pare-feu**, puis cliquez deux fois sur la stratégie que vous voulez exporter.
2. Sur la page de **Bienvenue** de l'assistant **Stratégie de pare-feu**, cliquez sur **Stratégie de pare-feu avancée**.
3. Dans la boîte de dialogue **Stratégie du pare-feu**, dans l'onglet **Général**, sous **Gestion de la configuration**, cliquez sur **Exporter** pour exporter les paramètres du pare-feu sous la forme d'un fichier de configuration (\*.conf).
4. Répétez les étapes 1-3 pour chaque stratégie de pare-feu de l'Enterprise Console avec un maximum de 5 (Enterprise Manager prend en charge un maximum de 5 stratégies).
5. Pour importer les paramètres dans Enterprise Manager, dans Enterprise Manager, dans le volet **Stratégies**, cliquez deux fois sur **Pare-feu**, puis cliquez deux fois sur la stratégie vers laquelle vous voulez importer les paramètres.
6. Sur la page de **Bienvenue** de l'assistant **Stratégie de pare-feu**, cliquez sur **Stratégie de pare-feu avancée**.

7. Dans la boîte de dialogue **Stratégie du pare-feu**, dans l'onglet **Général**, sous **Gestion de la configuration**, cliquez sur **Importer** pour importer les paramètres de configuration du pare-feu.
8. Répétez les étapes 5-7 pour les autres stratégies de pare-feu Enterprise Manager si besoin est.

## 17.2 Suppression de Sophos NAC

Si vous utilisez actuellement Sophos NAC (contrôle d'accès réseau), supprimez-le de votre réseau.

Pour supprimer les composants Sophos NAC, vous devez :

- Supprimer Sophos Compliance Agent des ordinateurs d'extrémité.
- Supprimer NAC Manager du serveur.
- Supprimer les bases de données NAC du serveur.

**Remarque :** si vous ne supprimez pas les composants dans cet ordre, les utilisateurs recevront des messages d'erreur.

### 17.2.1 Suppression de Sophos Compliance Agent

Pour supprimer Sophos Compliance Agent, rendez-vous sur chaque ordinateur d'extrémité et supprimez l'agent manuellement.

**Remarque :** il se peut qu'il vous soit demandé de fermer certaines applications avant de supprimer l'agent.

**Remarque :** redémarrez l'ordinateur après la suppression de l'agent.

1. Rendez-vous sur l'ordinateur d'extrémité.
2. Depuis le menu **Démarrer**, sélectionnez **Panneau de configuration > Ajouter ou supprimer des programmes**.
3. Sélectionnez **Sophos Network Access Control** et cliquez sur **Supprimer**.
4. Cliquez sur **Oui** pour confirmer la suppression.

### 17.2.2 Suppression du NAC Manager

Pour supprimer le NAC Manager :

1. Rendez-vous sur le serveur sur lequel le NAC Manager est installé. Généralement, il s'agit du même serveur que celui sur lequel l'Enterprise Console est installée.
2. Dans le menu **Démarrer**, cliquez sur **Panneau de configuration > Ajouter ou supprimer des programmes**.
3. Sélectionnez **Sophos NAC Application Server** et cliquez sur **Supprimer**.
4. Cliquez sur **Oui** pour confirmer la suppression.

Le NAC Manager est supprimé.

### 17.2.3 Suppression des bases de données NAC

**Remarque :** cette procédure supprime uniquement les fichiers serveur qui ont été utilisés pour créer les bases de données et ne supprime pas les bases de données elles-mêmes.

Sur le serveur sur lequel la base de données NAC est installée :

1. Dans le menu **Démarrer**, cliquez sur **Panneau de configuration > Ajouter ou supprimer des programmes**.
2. Sélectionnez **Sophos NAC Databases** et cliquez sur **Supprimer**.
3. Cliquez sur **Oui** pour confirmer la suppression.

## 17.3 Sauvegarde de la base de données Enterprise Console

Avant de désinstaller l'Enterprise Console, assurez-vous d'avoir une sauvegarde valide complète de votre installation de l'Enterprise Console. Assurez-vous d'être en mesure de restaurer le système depuis la sauvegarde. Si vous décidez ultérieurement de réinstaller l'Enterprise Console, vous pourrez restaurer ses paramètres.

**Remarque :** le dossier d'installation par défaut de la base de données est C:\Program files\Microsoft SQL Server\MSSQL\$SOPHOS.

Pour sauvegarder la base de données Enterprise Console :

1. Allez sur l'ordinateur sur lequel est installé le serveur d'administration Enterprise Console.
2. Arrêtez les services Sophos Message Router et Sophos Management Service. Pour cela :
  - a) Cliquez sur **Démarrer**, puis sur **Exécuter**, saisissez **services.msc** et cliquez sur **OK**.
  - b) Dans la fenêtre **Services**, cliquez avec le bouton droit de la souris et cliquez sur **Arrêter**.
  - c) Fermez la fenêtre **Services**.

Ainsi, vous êtes sûr qu'aucune nouvelle information n'est écrite sur la base de données pendant sa sauvegarde.

3. Créez un dossier pour la sauvegarde de la base de données, par exemple, C:\SophosBackups.
4. Ouvrez une fenêtre de commande dans le répertoire de la base de données d'installation de l'Enterprise Console.

Le répertoire par défaut est C:\Program Files\Sophos\Enterprise Console\DB.

5. Sauvegardez la base de données en saisissant une commande au format suivant :  
**BackupDB C:\SophosBackups\SOPHOS.bak**

Si l'instance de SQL Server n'est pas SOPHOS, ajoutez le nom de l'instance de SQL Server, par exemple :

**BackupDB C:\SophosBackups\SOPHOS.bak MonInstanceServeurSQL**

6. Exportez la clé de registre suivante :

- Pour un système d'exploitation en 32 bits : HKLM\SOFTWARE\Sophos\Certification Manager
- Pour un système d'exploitation en 64 bits :  
HKEY\_LOCAL\_MACHINE\Software\WOW6432Node\Sophos\Certification Manager

Vous êtes maintenant prêt à désinstaller l'Enterprise Console.

Pour plus d'informations sur la restauration de la base de données de l'Enterprise Console, reportez-vous à la section *Résolution des problèmes* ci-dessous.

## 17.4 Résolution des problèmes

### Restauration des données de l'Enterprise Console

Si vous avez besoin de restaurer l'installation de l'Enterprise Console à son état précédent, procédez de la manière suivante :

1. Rétablissez l'instance que vous utilisez de la base de données. L'instance par défaut de SQL Server est SOPHOS.
2. Rétablissez la clé de registre suivante :
  - Pour un système d'exploitation en 32 bits : HKLM\SOFTWARE\Sophos\Certification Manager
  - Pour un système d'exploitation en 64 bits :  
HKEY\_LOCAL\_MACHINE\Software\WOW6432Node\Sophos\Certification Manager

Pour plus d'informations ou d'assistance, veuillez contacter le support technique.

## 18 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](mailto: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.

## 19 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.

### **ACE™, TAO™, CIAO™, and CoSMIC™**

ACE<sup>1</sup>, TAO<sup>2</sup>, CIAO<sup>3</sup>, and CoSMIC<sup>4</sup> (henceforth referred to as “DOC software”) are copyrighted by Douglas C. Schmidt<sup>5</sup> and his research group<sup>6</sup> at Washington University<sup>7</sup>, University of California<sup>8</sup>, Irvine, and Vanderbilt University<sup>9</sup>, Copyright © 1993–2005, all rights reserved.

Since DOC software is open-source, free software, you are free to use, modify, copy, and distribute—perpetually and irrevocably—the DOC software source code and object code produced from the source, as well as copy and distribute modified versions of this software. You must, however, include this copyright statement along with code built using DOC software.

You can use DOC software in commercial and/or binary software releases and are under no obligation to redistribute any of your source code that is built using DOC software. Note, however, that you may not do anything to the DOC software code, such as copyrighting it yourself or claiming authorship of the DOC software code, that will prevent DOC software from being distributed freely using an open-source development model. You needn't inform anyone that you're using DOC software in your software, though we encourage you to let us<sup>10</sup> know so we can promote your project in the DOC software success stories<sup>11</sup>.

DOC software is provided as is with no warranties of any kind, including the warranties of design, merchantability, and fitness for a particular purpose, noninfringement, or arising from a course of dealing, usage or trade practice. Moreover, DOC software is provided with no support and without any obligation on the part of Washington University, UC Irvine, Vanderbilt University, their employees, or students to assist in its use, correction, modification, or enhancement. A number of companies<sup>12</sup> around the world provide commercial support for DOC software, however. DOC software is Y2K-compliant, as long as the underlying OS platform is Y2K-compliant.

Washington University, UC Irvine, Vanderbilt University, their employees, and students shall have no liability with respect to the infringement of copyrights, trade secrets or any patents by DOC software or any part thereof. Moreover, in no event will Washington University, UC Irvine, or Vanderbilt University, their employees, or students be liable for any lost revenue or profits or other special, indirect and consequential damages.

The ACE<sup>13</sup>, TAO<sup>14</sup>, CIAO<sup>15</sup>, and CoSMIC<sup>16</sup> web sites are maintained by the DOC Group<sup>17</sup> at the Institute for Software Integrated Systems (ISIS)<sup>18</sup> and the Center for Distributed Object Computing of Washington University, St. Louis<sup>19</sup> for the development of open-source software as part of the open-source software community<sup>20</sup>. By submitting comments, suggestions, code,

code snippets, techniques (including that of usage), and algorithms, submitters acknowledge that they have the right to do so, that any such submissions are given freely and unreservedly, and that they waive any claims to copyright or ownership. In addition, submitters acknowledge that any such submission might become part of the copyright maintained on the overall body of code, which comprises the DOC software. By making a submission, submitter agree to these terms. Furthermore, submitters acknowledge that the incorporation or modification of such submissions is entirely at the discretion of the moderators of the open-source DOC software projects or their designees.

The names ACE, TAO, CIAO, CoSMIC, Washington University, UC Irvine, and Vanderbilt University, may not be used to endorse or promote products or services derived from this source without express written permission from Washington University, UC Irvine, or Vanderbilt University. Further, products or services derived from this source may not be called ACE, TAO, CIAO, or CoSMIC nor may the name Washington University, UC Irvine, or Vanderbilt University appear in their names, without express written permission from Washington University, UC Irvine, and Vanderbilt University.

If you have any suggestions, additions, comments, or questions, please let me<sup>21</sup> know.

Douglas C. Schmidt<sup>22</sup>

### **References**

1. <http://www.cs.wustl.edu/~schmidt/ACE.html>
2. <http://www.cs.wustl.edu/~schmidt/TAO.html>
3. <http://www.dre.vanderbilt.edu/CIAO/>
4. <http://www.dre.vanderbilt.edu/cosmic/>
5. <http://www.dre.vanderbilt.edu/~schmidt/>
6. <http://www.cs.wustl.edu/~schmidt/ACE-members.html>
7. <http://www.wustl.edu/>
8. <http://www.uci.edu/>
9. <http://www.vanderbilt.edu/>
10. [mailto:doc\\_group@cs.wustl.edu](mailto:doc_group@cs.wustl.edu)
11. <http://www.cs.wustl.edu/~schmidt/ACE-users.html>
12. <http://www.cs.wustl.edu/~schmidt/commercial-support.html>
13. <http://www.cs.wustl.edu/~schmidt/ACE.html>
14. <http://www.cs.wustl.edu/~schmidt/TAO.html>
15. <http://www.dre.vanderbilt.edu/CIAO/>
16. <http://www.dre.vanderbilt.edu/cosmic/>
17. <http://www.dre.vanderbilt.edu/>
18. <http://www.isis.vanderbilt.edu/>
19. <http://www.cs.wustl.edu/~schmidt/doc-center.html>
20. <http://www.opensource.org/>
21. <mailto:d.schmidt@vanderbilt.edu>
22. <http://www.dre.vanderbilt.edu/~schmidt/>

### **Apache**

Les logiciels Sophos mentionnés dans le présent document peuvent inclure des programmes logiciels concédés en licence (ou en sous licence) à l'utilisateur selon les termes de la licence

Apache. Une copie du contrat de licence pour chacun des logiciels inclus est disponible sur <http://www.apache.org/licenses/LICENSE-2.0>.

### **Common Public License**

Les logiciels Sophos auxquels le présent document fait référence incluent ou peuvent inclure des programmes logiciels concédés en licence (ou en sous licence) à l'utilisateur selon les termes de la licence Common Public License (CPL), qui, entre autres droits, permettent à l'utilisateur d'avoir accès au code source. La licence CPL exige que pour tout logiciel concédé en licence sous les termes de la licence CPL, qui est distribuée sous un format de code objet, le code source soit aussi mis à disposition de ces utilisateurs sous un format de code objet. Pour 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](mailto: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>.

### **OpenSSL cryptographic toolkit**

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact [openssl-core@openssl.org](mailto:openssl-core@openssl.org).

### **OpenSSL license**

Copyright © 1998-2011 The OpenSSL Project. Tous droits réservés.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment:  
“This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)”
4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact [openssl-core@openssl.org](mailto:openssl-core@openssl.org).
5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:  
“This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit.

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young ([ey@cryptsoft.com](mailto:ey@cryptsoft.com)).  
This product includes software written by Tim Hudson ([tjh@cryptsoft.com](mailto:tjh@cryptsoft.com)).

#### **Original SSLeay license**

Copyright © 1995–1998 Eric Young ([ey@cryptsoft.com](mailto:ey@cryptsoft.com)) All rights reserved.

This package is an SSL implementation written by Eric Young ([ey@cryptsoft.com](mailto:ey@cryptsoft.com)). The implementation was written so as to conform with Netscape’s SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson ([tjh@cryptsoft.com](mailto:tjh@cryptsoft.com)).

Copyright remains Eric Young’s, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

“This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)”

The word “cryptographic” can be left out if the routines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

“This product includes software written by Tim Hudson (tjh@cryptsoft.com)”

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License.]