

# SOPHOS

## Sophos Endpoint Security and Control 9.5 Guide de démarrage rapide

Date du document : juin 2010



# Table des matières

1 A propos de ce guide.....	3
2 Que faut-il installer ?.....	3
3 Quelles sont les étapes essentielles ?.....	3
4 Vérification de la configuration système requise.....	4
5 Préparation de l'installation.....	5
6 Téléchargement des programmes d'installation.....	6
7 Installation de l'Enterprise Console.....	6
8 Téléchargement des logiciels de sécurité.....	7
9 Installation du NAC Manager.....	7
10 Création de groupes d'ordinateurs.....	8
11 Configuration des stratégies de sécurité.....	8
12 Recherche d'ordinateurs.....	9
13 Protection des ordinateurs.....	9
14 Vérification du bon fonctionnement de votre réseau.....	11
15 Résolution des problèmes.....	11
16 Aide sur les tâches les plus courantes.....	12
17 Support technique.....	13
18 Mentions légales.....	13

## 1 A propos de ce guide

Ce guide vous indique comment protéger votre réseau avec les logiciels de sécurité Sophos.

Si vous installez les logiciels Sophos pour la première fois, lisez ce guide.

Si vous procédez à la mise à niveau, rendez-vous au **Centre de mise à niveau Endpoint Security and Control 9.5** sur <http://www.sophos.fr/support/upgrades/>

**Remarque :** si vous avez un réseau étendu, envisagez d'utiliser les options d'installation du *Guide de démarrage avancé de Sophos Endpoint Security and Control*.

## 2 Que faut-il installer ?

Installez deux outils d'administration :

- **Sophos Enterprise Console.** Elle vous permet d'installer et d'administrer les logiciels de sécurité sur vos ordinateurs.
- **Sophos NAC Manager.** Il vous permet d'utiliser le “contrôle d'accès réseau”, lequel peut bloquer l'accès aux ordinateurs non autorisés ou non conformes à vos normes de sécurité.

L'installation du NAC Manager est facultative.

**Remarque :** installez les outils séparément en utilisant deux programmes de configuration différents.

**Remarque :** vous pouvez installer les deux outils sur le même serveur. En revanche, si vous avez plus de 1 000 ordinateurs, installez les outils sur des serveurs différents. La procédure est identique.

## 3 Quelles sont les étapes essentielles ?

Exécutez les étapes essentielles suivantes :

- Vérification de la configuration système requise.
- Préparation de l'installation.
- Téléchargement des programmes d'installation.
- Installation de l'Enterprise Console.
- Téléchargement des logiciels de sécurité.
- Installation de NAC Manager.
- Création de groupes d'ordinateurs.
- Configuration des stratégies de sécurité.
- Recherche d'ordinateurs.
- Protection des ordinateurs.

- Vérification du bon fonctionnement de votre réseau.

## 4 Vérification de la configuration système requise

Vérifiez la configuration requise pour le matériel, le système d'exploitation et les logiciels système avant de commencer l'installation.

### 4.1 Matériel et système d'exploitation

La configuration système requise dépend du ou des outils que vous installez.

Les configurations requises ci-dessous sont des recommandations. Elles supposent que les outils d'administration sont installés sur un serveur unique et qu'il y a jusqu'à 1 000 ordinateurs sur l'ordinateur.

Un accès Internet est obligatoire dans tous les cas.

**Remarque :** la configuration requise ci-dessous répertorie uniquement les systèmes d'exploitation serveur. Si vous avez besoin de plus de détails pour les configurations requises, visitez <http://www.sophos.fr/products/all-sysreqs.html>.

#### Enterprise Console seulement

Processeur	Espace disque	Mémoire	Système d'exploitation
Pentium 2 GHz ou équivalent	Jusqu'à 2 Go pour la base de données	512 Mo	Windows Server 2008 R2 Windows Server 2008 (32 ou 64 bits) Windows Server 2008 Hyper-V Windows Server 2003 R2 Windows Server 2003 SP1+ (32 ou 64 bits) VMWare ESX 3.0 ou 3.5 VMWare Workstation 6.5

## Enterprise Console et NAC Manager

Processeur	Espace disque	Mémoire	Système d'exploitation
Pentium 2 GHz ou équivalent	Jusqu'à 3 Go pour la base de données	1 Go	Windows Server 2008 R2 Windows Server 2008 (32 ou 64 bits) Windows Server 2003 R2 Windows Server 2003 SP1+ (32 ou 64 bits)

## 4.2 Logiciels système Microsoft

Les logiciels système Microsoft suivants doivent être installés pour permettre l'exécution du programme d'installation de Sophos Enterprise Console :

- Microsoft Windows Installer, version 4.5, avec le correctif KB958655
- Mise à jour de sécurité pour Microsoft XML Core Services 6.0
- Microsoft .NET Framework 3.5 SP1
- Microsoft SQL Server 2005 Express

Si vous n'avez pas ces versions (ou des versions ultérieures) des logiciels système de Microsoft, le programme d'installation de l'Enterprise Console les installe pour vous.

### Remarques

Le programme d'installation installe SQL Server 2008 Express, sauf si vous êtes déjà équipé de SQL Server 2005 Express ou supérieur. SQL Server 2008 Express n'est pas compatible avec Windows Server 2003 SP1 ou Windows Essential Business Server 2008.

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.

Suite à l'installation des logiciels système requis, il se peut que vous ayez à redémarrer vos ordinateurs. Pour plus d'informations sur la configuration requise pour le redémarrage du système, consultez l'article 65190 de la base de connaissances du support Sophos (<http://www.sophos.fr/support/knowledgebase/article/65190.html>).

## 5 Préparation de l'installation

Sur un serveur satisfaisant à la configuration système requise, 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 vous avez Microsoft SQL Server 2000 ou MSDE 2000 avec une instance de base de données autre que "SOPHOS", mettez-la à niveau vers Microsoft SQL Server 2005.

- Si le serveur utilise Windows Server 2008 ou supérieur, désactivez le Contrôle de compte d'utilisateur (UAC) 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.

## 6 Téléchargement des programmes d'installation

Téléchargez les programmes d'installation Sophos sur le serveur sur lequel vous souhaitez installer les outils 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 de téléchargements de **Endpoint Security and Data Protection** :
  - Téléchargez le programme d'installation de l'Enterprise Console.
  - Si vous utilisez le NAC Manager, téléchargez le programme d'installation de Sophos NAC.

Si vous prévoyez d'installer NAC Manager sur un serveur différent que celui de l'Enterprise Console, téléchargez le programme d'installation sur ce serveur.

## 7 Installation de l'Enterprise Console

Pour installer l'Enterprise Console :

1. Ouvrez une session en tant qu'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, ouvrez une session en tant qu'administrateur local.

2. Recherchez le programme d'installation de l'Enterprise Console que vous avez téléchargé auparavant.

**Astuce :** le nom de fichier du programme d'installation inclut le mot "sec".

3. Cliquez deux fois sur le programme d'installation.
4. Dans la boîte de dialogue **Programme d'installation réseau de Sophos Endpoint Security and Control 9.5**, cliquez sur **Installer**.

Les fichiers d'installation sont copiés sur l'ordinateur et l'assistant d'installation démarre.

5. Dans la boîte de dialogue **Sophos Enterprise Console**, cliquez sur **Suivant**.
6. Un assistant vous guide tout au long de l'installation. Procédez ainsi :
  - a) Acceptez les valeurs par défaut selon le cas.
  - b) Sélectionnez une configuration **complète**.

7. Une fois l'installation terminée, il se peut que vous soyez invité à redémarrer. Cliquez sur **Oui** ou sur **Terminer**.

## 8 Téléchargement des logiciels de sécurité

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

**Remarque :** si vous avez utilisé le Bureau à distance pour l'installation, cette dernière 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 plate-formes**, sélectionnez seulement celles que vous souhaitez protéger immédiatement.

Lorsque vous cliquez sur **Suivant**, l'Enterprise Console commence à télécharger vos logiciels.

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

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

## 9 Installation du NAC Manager

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.

**Remarque :** si vous installez NAC Manager sur un serveur différent de l'Enterprise Console, installez d'abord manuellement une base de données SQL Server 2005 ou supérieure.

1. Ouvrez une session en tant qu'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, ouvrez une session en tant qu'administrateur local.
2. Recherchez le programme d'installation de Sophos NAC que vous avez téléchargé auparavant.

**Astuce :** le nom de fichier du programme d'installation inclut le mot "nac".

3. Cliquez deux fois sur le programme d'installation.
4. Dans la boîte de dialogue **Sophos NAC Manager**, cliquez sur **Install**.
5. Un assistant vous guide tout au long de l'installation.

## 10 Création de groupes d'ordinateurs

Si vous avez utilisé l'**Assistant de téléchargement des logiciels de sécurité** pour paramétrer vos groupes d'ordinateurs (d'après vos groupes Active Directory), vous pouvez passer cette section. Allez au chapitre *Configuration des stratégies de sécurité* à la page 8.

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

1. Si l'Enterprise Console n'est pas déjà ouverte, ouvrez-la.
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.

## 11 Configuration des stratégies de sécurité

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

- Configurez une stratégie de pare-feu immédiatement.
- Modifiez les stratégies de contrôle d'accès réseau, de contrôle des applications, de contrôle des données et de contrôle des périphériques si vous souhaitez utiliser ces fonctions. Vous pouvez effectuer cette opération à tout moment.

### 11.1 Configuration d'une stratégie de pare-feu

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

Par défaut, le pare-feu bloque toutes les connexions qui ne sont pas essentielles. Vous devez, par conséquent, configurer le pare-feu avant de protéger vos ordinateurs.

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'imprimantes**, sélectionnez **Autoriser le partage de fichiers et d'imprimantes**.

## 12 Recherche d'ordinateurs

Vous devez rechercher les ordinateurs sur le réseau avant que l'Enterprise Console ne puisse les protéger et les administrer.

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.
3. Saisissez les détails du compte, si nécessaire, et spécifiez où vous voulez effectuer la recherche.

Si vous utilisez une des options **Rechercher**, les ordinateurs sont placés dans le dossier **Non affectés**.

## 13 Protection des ordinateurs

Pour protéger les ordinateurs, vous devez :

- Préparer les ordinateurs.
- Protéger automatiquement les ordinateurs Windows.
- Protéger manuellement les ordinateurs Windows ou Mac OS X.

### 13.1 Préparation de la protection des ordinateurs

Avant de protéger les ordinateurs, procédez ainsi :

#### **Préparez 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 Console.

### **Assurez-vous que votre compte peut être utilisé pour l'installation de logiciels**

Vous allez être invité à saisir les détails d'un compte qui peut être utilisé pour installer des logiciels de sécurité. Généralement, il s'agit d'un compte d'administrateur de domaine. Il doit :

- Disposer des droits d'administrateur local sur les ordinateurs que vous souhaitez protéger.
- Pouvoir se connecter à l'ordinateur sur lequel vous avez installé l'Enterprise Console.
- Avoir un accès en lecture à l'emplacement depuis lequel les ordinateurs se mettront à jour. Pour vérifier cet emplacement, dans le volet **Stratégies**, cliquez deux fois sur **Mise à jour**, puis cliquez deux fois sur **Par défaut**.

### **Préparez l'installation du contrôle d'accès réseau**

Avant de pouvoir installer le contrôle d'accès réseau sur les ordinateurs, vous devez :

- Spécifier l'URL de l'ordinateur sur lequel vous avez installé le NAC Manager. Dans l'Enterprise Console, sélectionnez **Outils > Configurer l'URL de NAC**.

## **13.2 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**, vous pouvez installer des fonctions supplémentaires. Sélectionnez **Contrôle de conformité** si vous voulez le contrôle d'accès réseau.
  - 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 11.
  - 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.

Une fois l'installation terminée, consultez de nouveau la liste des ordinateurs. Dans la colonne **Sur accès**, le mot **Actif** indique que le contrôle viral sur accès fonctionne sur cet ordinateur.

## 13.3 Protection manuelle des ordinateurs Windows ou Mac OS X

Si vous avez des ordinateurs que vous ne pouvez pas protéger automatiquement, protégez-les en exécutant un programme de configuration depuis un répertoire centralisé.

Pour savoir dans quel répertoire figure le programme d'installation, ouvrez l'Enterprise Console et sélectionnez **Affichage > Emplacements des fichiers d'amorce**.

1. Allez sur chaque ordinateur et connectez-vous avec les droits d'administrateur local.
2. Recherchez le programme d'installation dans le répertoire d'installation centralisée et cliquez deux fois dessus.
  - Pour Windows, le programme est appelé setup.exe.
  - Pour Mac OS X, le programme est appelé Sophos Anti-Virus.mpkg
3. Un assistant vous guide tout au long de l'installation.

## 14 Vérification du bon fonctionnement de votre réseau

Pour vérifier le bon fonctionnement de votre réseau depuis l'Enterprise Console, procédez ainsi :

1. Dans la barre de menus, cliquez sur l'icône **Tableau de bord** (si le Tableau de bord n'apparaît pas).

Le Tableau de bord vous montre combien d'ordinateurs :

  - Ont détecté des menaces.
  - Ne sont pas à jour.
  - Ne sont pas conformes aux stratégies.
2. Si vous utilisez NAC, vous pouvez aussi :
  - a) Sélectionner **Fichier > Ouvrir > NAC**.
  - b) Dans le NAC Manager, sélectionner **Report > Compliance**.

Vous savez ainsi si les ordinateurs sont conformes à la stratégie NAC.

## 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 est impossible sur ce système d'exploitation. Effectuez une installation manuelle. Reportez-vous à la section [Protection manuelle des ordinateurs Windows ou Mac OS X](#) à la page 11. Pour voir plus de systèmes d'exploitation, reportez-vous au [Guide de démarrage avancé de Sophos Endpoint Security and Control](#).

- 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

Cette section vous indique où trouver des informations sur la manière d'effectuer les tâches les plus courantes.

SESC = Sophos Endpoint Security and Control

Tâche	Document
Protéger les ordinateurs Linux	Guide de démarrage SESC 9.5 pour Linux, NetWare et UNIX : "Protection des ordinateurs Linux"
Protéger les ordinateurs autonomes	Guide de démarrage avancé SESC 9.5 : "Protection des ordinateurs autonomes"
Configurer l'antivirus et HIPS (Host Intrusion Prevention System)	Aide de l'Enterprise Console : "Configuration de la stratégie antivirus et HIPS"
Configurer le contrôle des applications	Aide de l'Enterprise Console : "Configuration de la stratégie de contrôle des applications"
Configurer le contrôle des données	Aide de l'Enterprise Console : "Configuration de la stratégie de contrôle des données"
Configurer le contrôle des périphériques	Aide de l'Enterprise Console : "Configuration de la stratégie de contrôle des périphériques"
Configurer la protection antialtération	Aide de l'Enterprise Console : "Configuration de la stratégie de protection antialtération"
Configurer NAC	Aide du NAC Manager : "Aperçu de la zone Manage"
Donner l'accès réseau aux utilisateurs invités	Guide de configuration de Sophos Compliance Agent "Agent temporaire"
Traiter les alertes	Aide de l'Enterprise Console : "Traitement des alertes et des erreurs"
Nettoyer les ordinateurs	Aide de l'Enterprise Console : "Nettoyage des ordinateurs"
Générer des rapports SEC	Aide de l'Enterprise Console : "Génération de rapports"

Tâche	Document
Générer des rapports NAC	Aide du NAC Manager : "Aperçu de la zone Report"

## 17 Support technique

Vous pouvez obtenir du support technique pour les produits Sophos de l'une des manières suivantes :

- Visitez le forum SophosTalk à l'adresse <http://community.sophos.com/> et recherchez d'autres utilisateurs qui connaissent le même problème.
- Visitez la base de connaissances du support de Sophos à l'adresse <http://www.sophos.fr/support/>
- Téléchargez la documentation des produits à l'adresse <http://www.sophos.fr/support/docs/>
- Envoyez un courriel à [support@sophos.fr](mailto:support@sophos.fr), y compris le ou les numéros de versions du logiciel Sophos, le ou les systèmes d'exploitation et le ou les niveaux de correctif ainsi que le texte de tout message d'erreur.

## 18 Mentions légales

Copyright © 2010 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 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.

Les logiciels Sophos mentionnés dans le présent document 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>