

SOPHOS

Security made simple.

Sophos Enterprise Console

Guide de démarrage rapide

Version du produit : 5.2
Date du document : mars 2015



Table des matières

1	À propos de ce guide.....	4
2	Que faut-il installer ?.....	4
3	Quelles sont les étapes essentielles ?.....	5
4	Téléchargement du programme d'installation de l'Enterprise Console.....	6
5	Vérification de la configuration système requise.....	6
	5.1 Matériel et système d'exploitation.....	7
	5.2 Logiciels système Microsoft.....	7
	5.3 Conditions applicables à l'accès aux ports.....	8
6	De quels comptes avez-vous besoin ?.....	8
	6.1 Compte de base de données.....	8
	6.2 Compte Update Manager.....	9
7	Préparation de l'installation.....	9
8	Installation de l'Enterprise Console.....	9
9	Renforcement de la sécurité de la base de données.....	10
10	Téléchargement du logiciel de protection et du logiciel de chiffrement.....	11
11	Création de groupes d'ordinateurs.....	12
12	Configuration des stratégies de sécurité.....	12
	12.1 Configuration d'une stratégie de pare-feu.....	13
13	Recherche d'ordinateurs.....	13
14	Préparation de la protection des ordinateurs.....	14
	14.1 Préparation à la suppression automatique des logiciels de sécurité tiers.....	14
	14.2 Vérification que votre compte peut être utilisé pour l'installation du logiciel.....	14
	14.3 Préparation de l'installation du logiciel antivirus.....	15
15	Protection des ordinateurs.....	15
	15.1 Protection automatique des ordinateurs Windows.....	15
	15.2 Protection manuelle des ordinateurs Windows ou Mac.....	16
	15.3 Protection des ordinateurs Linux.....	17
16	Paramétrage du logiciel de chiffrement sur les ordinateurs	17
	16.1 Abonnement au logiciel de chiffrement.....	18
	16.2 Préparation de l'installation du logiciel de chiffrement.....	18
	16.3 Installation automatique du logiciel de chiffrement.....	20
	16.4 Installation manuelle du logiciel de chiffrement.....	21
	16.5 Première connexion après installation.....	21
17	Vérification du bon fonctionnement de votre réseau.....	23

18	Résolution des problèmes.....	23
19	Aide sur les tâches les plus courantes.....	23
20	Support technique.....	24
21	Mentions légales.....	24

1 À propos de ce guide

Ce guide vous indique comment protéger votre réseau avec le logiciel de sécurité Sophos.

Ce guide s'adresse à vous si :

- Vous installez le logiciel pour la première fois.
- Vous installez les fonctions de protection et de chiffrement (l'installation du chiffrement est facultative).

Si vous procédez à la mise à niveau, reportez-vous plutôt au *Guide de mise à niveau de Sophos Enterprise Console*.

Autres documents utiles

Si vous avez un réseau étendu, envisagez d'utiliser les options d'installation mentionnées dans le *Guide de démarrage avancé de Sophos Enterprise Console*.

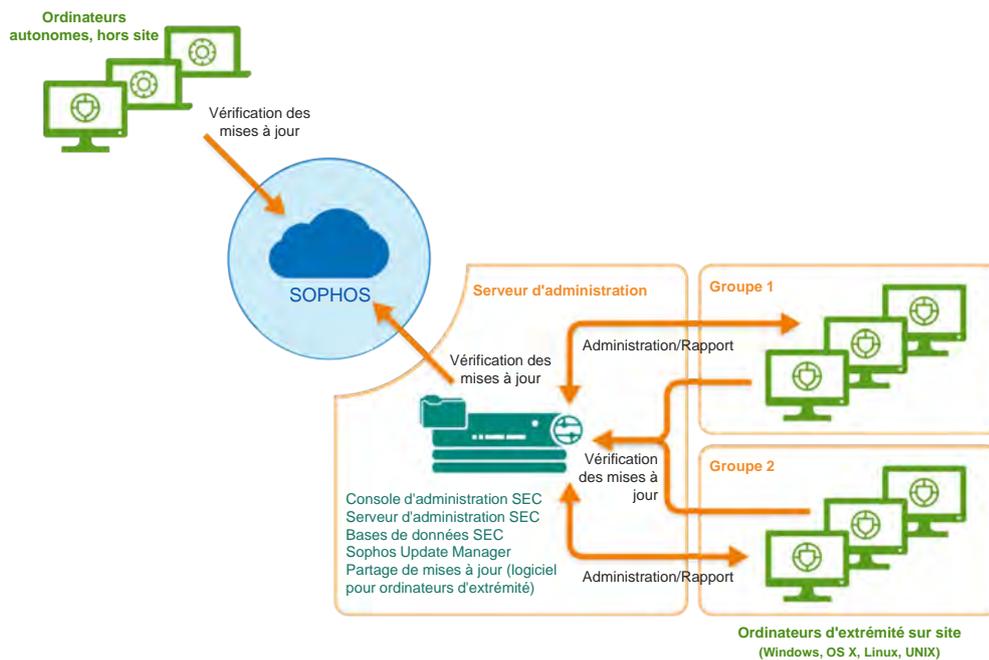
La documentation Sophos est disponible sur

<http://www.sophos.com/fr-fr/support/documentation.aspx>.

2 Que faut-il installer ?

Pour protéger votre réseau, installez :

- **Sophos Enterprise Console** sur votre serveur. Elle vous permet d'installer et d'administrer le logiciel de sécurité de Sophos.
- Le **logiciel de protection de Sophos** sur vos ordinateurs d'extrémité. Il vous permet de protéger les ordinateurs contre les menaces et envoie des alertes à l'Enterprise Console.
- Le **logiciel de chiffrement de Sophos** sur vos ordinateurs d'extrémité (s'il est inclus dans votre licence).



3 Quelles sont les étapes essentielles ?

Procédez aux étapes essentielles suivantes :

- Téléchargez le programme d'installation de l'Enterprise Console.
- Vérifiez la configuration système requise.
- Vérifiez de quels comptes vous avez besoin.
- Préparez l'installation.
- Installez l'Enterprise Console.
- Téléchargez le logiciel de protection et le logiciel de chiffrement.
- Créez des groupes d'ordinateurs.
- Configurez les stratégies de sécurité.
- Recherchez les ordinateurs.
- Préparez la protection des ordinateurs.
- Protégez les ordinateurs.
- Configurez le chiffrement sur les ordinateurs s'il est inclus dans votre licence.
- Vérifiez le bon fonctionnement de votre réseau.

4 Téléchargement du programme d'installation de l'Enterprise Console

▪ Si vous avez une licence Sophos

Les étapes suivantes supposent que vous avez un compte MySophos et que vous avez associé vos codes d'accès de licence à ce compte. Retrouvez plus d'aide sur www.sophos.com/fr-fr/support/knowledgebase/111195.aspx.

1. Allez sur www.sophos.com/fr-fr/support/downloads/.
2. Saisissez votre nom d'utilisateur et votre mot de passe MySophos.

Une page Web s'ouvre et affiche votre ou vos licences.

3. Sous votre nom de licence, rendez-vous dans les téléchargements pour la **Console**. Téléchargez le programme d'installation de l'Enterprise Console

▪ Si vous voulez évaluer l'Enterprise Console

1. Rendez-vous sur <http://www.sophos.com/fr-fr/products/free-trials/endpoint-protection.aspx>.
2. Remplissez le formulaire d'inscription.

Après avoir envoyé le formulaire d'inscription, vos codes d'accès d'évaluation apparaîtront. Les codes d'accès seront aussi envoyés à l'adresse électronique que vous avez saisie dans le formulaire d'inscription. Vous en aurez besoin lors du paramétrage de l'Enterprise Console.

3. Cliquez sur **Télécharger maintenant** et téléchargez le programme d'installation de l'Enterprise Console.

5 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.

Info : vous pouvez exécuter le programme d'installation de l'Enterprise Console pour vérifier si le serveur répond aux conditions requises pour l'installation, même si vous ne voulez pas passer à l'installation immédiatement. Vous pouvez voir les résultats de la vérification du système sur la page **Vérifications de la propriété du système** de l'assistant d'installation. Après avoir examiné les résultats, cliquez sur **Annuler** pour fermer l'assistant. Retrouvez plus d'informations sur les résultats de la vérification du système sur <http://www.sophos.com/fr-fr/support/knowledgebase/113945.aspx>.

5.1 Matériel et système d'exploitation

Pour voir les configurations requises en matière de matériels et de systèmes d'exploitation, consultez la page Configuration requise sur le site Web de Sophos (<http://www.sophos.com/fr-fr/products/all-system-requirements.aspx>).

5.2 Logiciels système Microsoft

L'Enterprise Console requiert l'utilisation de certains logiciels système Microsoft (par exemple, des logiciels de base de données).

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

Quel que soit le programme d'installation que vous utilisez, veuillez lire les conseils d'installation ci-dessous.

Remarque : après avoir installé les logiciels système requis, redémarrez vos ordinateurs. Retrouvez plus d'informations sur www.sophos.com/fr-fr/support/knowledgebase/65190.aspx.

Installation de SQL Server

Le programme d'installation tente d'installer SQL Server 2008 R2 Express Edition avec Service Pack 1 (SP1), sauf si vous choisissez d'utiliser une instance existante de SQL Server 2005 Express ou supérieur. Sachez que :

- Nous déconseillons d'installer SQL Server sur un contrôleur de domaine.
- SQL Server 2008 R2 Express n'est pas compatible avec Windows Server 2003 SP1 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 sur <http://support.microsoft.com/kb/322692>.

Installation de .NET Framework

Le programme d'installation tente d'installer .NET Framework 4.0 sauf s'il est déjà installé. Sachez que :

- Dans le cadre de l'installation de .NET Framework 4.0, certains services système (tel que le Service d'administration IIS) vont redémarrer.

Après l'installation de .NET Framework 4.0, vous allez voir un message vous demandant de redémarrer votre ordinateur. Si vous acceptez, nous vous conseillons de redémarrer l'ordinateur immédiatement ou juste après l'installation.

Installation de Microsoft Message Queuing

Le programme d'installation tente d'installer Microsoft Message Queuing (MSMQ) sauf s'il est déjà installé. Sachez que :

- Au cours de l'installation de MSMQ, les services suivants sont arrêtés : MSDTC, MSSQLServer, SQLSERVERAGENT. En conséquence, l'accès à la base de données SQL Server par défaut est interrompu.

Assurez-vous que les services peuvent être arrêtés en toute sécurité au cours de l'installation. Vérifiez également que vous les avez bien redémarrés par la suite.

5.3 Conditions applicables à l'accès aux ports

L'Enterprise Console nécessite l'ouverture d'un certain nombre de ports. Retrouvez plus d'informations sur <http://www.sophos.com/fr-fr/support/knowledgebase/38385.aspx>.

6 De quels comptes avez-vous besoin ?

Avant d'installer le logiciel Sophos, créez les comptes utilisateur dont vous avez besoin :

- **Compte de base de données.** Il s'agit d'un compte utilisateur Windows qui permet au service d'administration de l'Enterprise Console de se connecter à la base de données. Il est aussi utilisé par d'autres services Sophos.

Nous vous conseillons de nommer le compte de base de données **SophosManagement**.

- **Compte Update Manager.** Il s'agit d'un compte utilisateur Windows qui permet à vos ordinateurs d'extrémité d'accéder aux dossiers dans lesquels l'Enterprise Console place les mises à jour logicielles.

Nous vous conseillons de nommer le compte Update Manager **SophosUpdateMgr**.

6.1 Compte de base de données

Le compte de base de données doit :

- Pouvoir se connecter à l'ordinateur sur lequel vous allez installer Sophos Management Server (un composant de l'Enterprise Console).
- Pouvoir lire et écrire dans le répertoire temporaire du système, par exemple : « \windows\temp\ ». Par défaut, les membres du groupe « Utilisateurs » disposent de ce droit.
- Avoir un nom d'utilisateur principal (UPN, User Principal Name) associé au compte s'il s'agit d'un compte de domaine.

Tous les autres droits et abonnements de groupes dont il a besoin sont accordés automatiquement au cours de l'installation.

Le compte :

- Ne doit pas être paramétré pour expirer et ne doit avoir aucune limite de connexion.
- Ne doit pas être un compte administratif.
- Ne doit pas être modifié suite à l'installation.
- Est nommé **SophosManagement**.

Retrouvez plus de conseils et d'instructions sur www.sophos.com/fr-fr/support/knowledgebase/113954.aspx.

6.2 Compte Update Manager

Le compte Update Manager doit avoir un accès en lecture au dossier dans lequel l'Enterprise Console place les mises à jour logicielles. Par défaut, il s'agit de : \\[nomserveur]\SophosUpdate

Le compte :

- Ne doit pas être paramétré pour expirer et ne doit avoir aucune limite de connexion.
- Ne doit pas être un compte administratif.
- A un nom d'utilisateur principal (UPN, User Principal Name) associé au compte s'il s'agit d'un compte de domaine.
- Est nommé **SophosUpdateMgr**.

Retrouvez plus de conseils et d'instructions sur

www.sophos.com/fr-fr/support/knowledgebase/113954.aspx.

7 Préparation de l'installation

Préparez l'installation comme suit :

- 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 Contrôle de compte d'utilisateur (UAC) est activé sur le serveur, désactivez-le et redémarrez le serveur.

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

8 Installation de l'Enterprise Console

Pour installer l'Enterprise Console :

1. Sur l'ordinateur sur lequel vous souhaitez installer l'Enterprise Console, ouvrez une session avec les droits administrateur.
 - Si le serveur est dans un domaine, utilisez un compte de domaine disposant des droits d'administrateur local.
 - Si le serveur est dans un groupe de travail, utilisez un compte local disposant des droits d'administrateur local.
2. Recherchez le programme d'installation de l'Enterprise Console que vous avez téléchargé auparavant.
3. Cliquez deux fois sur le programme d'installation.
4. Lorsque vous y êtes invité, cliquez sur **Installer**.

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

5. L'assistant vous guide tout au long de l'installation. Procédez ainsi :
 - a) Acceptez les valeurs par défaut selon le cas.
 - b) Sur la page **Sélection des composants**, assurez-vous que tous les composants sont sélectionnés.
 - c) Sur la page **Vérifications de la propriété du système**, examinez les résultats de la vérification système et prenez des mesures si nécessaire. Retrouvez plus d'informations sur les résultats de la vérification du système sur <http://www.sophos.com/fr-fr/support/knowledgebase/113945.aspx>.
 - d) Sur la page **Détails de la base de données**, saisissez les détails du compte de base de données que vous avez créé dans [Compte de base de données](#) à la page 8.
 - e) Sur la page **Codes d'accès Sophos Update Manager**, saisissez les détails du compte Update Manager que vous avez créé dans [Compte Update Manager](#) à la page 9.
 - f) Sur la page **Administration du chiffrement**, cliquez sur **Administrer le chiffrement**, si vous voulez que l'Enterprise Console administre le chiffrement.
Remarque : si vous cliquez sur **Ne pas administrer le chiffrement** ou si SafeGuard Enterprise est installé sur cet ordinateur, aucune autre option d'installation ne vous sera proposée. Passez directement à l'étape 6.
 - g) Sur la page **Chiffrement Sophos**, sélectionnez **Nouvelles installations** si aucune version antérieure de Sophos Disk Encryption n'est installée sur le réseau. Vous êtes invité à saisir le mot de passe du magasin de sauvegarde des certificats. Notez le mot de passe.
6. Une fois l'installation terminée, il se peut que vous soyez invité à redémarrer. Cliquez sur **Oui** ou sur **Terminer**.

Important : la base de données d'audit de Sophos appelée **SophosSecurity** doit être présente et s'exécuter en même temps que les autres bases de données de l'Enterprise Console même si vous n'avez pas l'intention d'utiliser la fonction d'audit de Sophos. En effet, cette base de données est utilisée pour les événements de contrôle d'accès renforcé et de journalisation des audits.

9 Renforcement de la sécurité de la base de données

Audit de la base de données

En plus de la protection intégrée aux bases de données Enterprise Console, nous vous conseillons de paramétrer la protection supplémentaire au niveau de l'instance SQL Server (s'il n'est pas déjà en place) pour auditer les activités de l'utilisateur et les modifications qu'il a effectué sur votre SQL Server.

Par exemple, si vous utilisez une édition Enterprise de SQL Server 2008, vous pouvez utiliser la fonction SQL Server Audit. Des versions précédentes de SQL Server prennent en charge l'audit de connexion, l'audit par déclencheur externe et l'audit des événements à l'aide d'un utilitaire de suivi intégré.

Retrouvez plus d'informations sur les fonctions que vous pouvez utiliser pour procéder à l'audit des activités et des modifications sur votre système SQL Server dans la documentation correspondant à votre version de SQL Server. Par exemple :

- [SQL Server Audit \(moteur de base de données\)](#)
- [Audit \(moteur de base de données\), SQL Server 2008 R2](#)
- [Audit dans SQL Server 2008](#)
- [Audit \(moteur de base de données\), SQL Server 2008](#)

Chiffrement des connexions à la base de données

Nous vous conseillons fortement de chiffrer les connexions entre tous les clients et la base de données Enterprise Console. Retrouvez plus d'informations dans la documentation de SQL Server :

- [Activer les connexions chiffrées dans le moteur de base de données \(Gestionnaire de configuration SQL Server\)](#)
- [Chiffrement des connexions à SQL Server 2008 R2](#)
- [Comment faire pour activer le chiffrement SSL pour une instance de SQL Server à l'aide de la console MMC](#)

Contrôle de l'accès aux copies de sauvegardes de la base de données

Assurez-vous qu'un contrôle d'accès correct et restrictif aux copies de sauvegarde de la base de données est mis en place. Ceci permet de garantir que les utilisateurs non autorisés n'auront pas accès aux fichiers, ne pourront pas les altérer ou les supprimer accidentellement.

Remarque : les liens de cette section vous dirigent vers des informations mises à jour par des tiers et sont fournies pour vous aider. Même si nous vérifions régulièrement l'exactitude de ces liens, il se peut que ceux-ci soient modifiés sans que nous en ayons connaissance.

10 Téléchargement du logiciel de protection et du logiciel de chiffrement

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, 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 protection. Procédez ainsi :

1. Sur la page **Détails du compte de téléchargement Sophos**, saisissez le nom d'utilisateur et le mot de passe imprimés sur votre annexe de licence ou vos codes d'accès d'évaluation. Si vous accédez à Internet via un serveur proxy, sélectionnez la case à cocher **Accéder à Sophos via un serveur proxy** et saisissez les détails de votre proxy.
2. Sur la page **Sélection des plate-formes**, sélectionnez seulement celles que vous souhaitez protéger immédiatement.

3. Si votre licence inclut le chiffrement, sur la page **Type de logiciel**, sélectionnez **Chiffrement** si vous voulez le télécharger.

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

4. Sur la page **Téléchargement des logiciels**, vous pouvez voir la progression du téléchargement. Cliquez sur **Suivant**.
5. 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.

Remarque : retrouvez plus d'informations concernant la protection des ordinateurs Windows 8 sur <http://www.sophos.com/fr-fr/support/knowledgebase/118261.aspx>.

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

11 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. Rendez-vous à la section [Configuration des stratégies de sécurité](#) à la page 12.

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.

12 Configuration des stratégies de sécurité

L'Enterprise Console 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, sauf pour les exceptions suivantes :

- Si vous voulez utiliser Sophos Client Firewall, nous vous conseillons de paramétrer la stratégie de pare-feu avant de déployer le pare-feu sur les ordinateurs.
- Vous devez modifier les stratégies de contrôle des applications, de contrôle des périphériques, de correctif ou de contrôle du Web si vous voulez utiliser ces fonctions. Vous pouvez effectuer cette opération à tout moment.

- Par défaut, le chiffrement intégral du disque n'est pas activé après l'installation sur les ordinateurs. Vous devez modifier la stratégie de chiffrement intégral du disque pour chiffrer les lecteurs des ordinateurs. Vous pouvez effectuer cette modification à tout moment. Par défaut, l'authentification au démarrage est activée.

Vous devez modifier cette stratégie pour permettre aux administrateurs d'accéder aux ordinateurs et d'effectuer d'autres tâches d'installation ou de vérification. Vous devez configurer ceci avant d'installer le chiffrement intégral du disque. Reportez-vous à la section [Attribution de l'accès administrateur aux ordinateurs suite à l'installation](#) à la page 18.

Remarque : pour une première installation, nous vous conseillons de configurer le chiffrement en activant et en testant pas à pas chaque paramètre.

12.1 Configuration d'une stratégie de pare-feu

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.

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

1. Dans le volet **Stratégies**, cliquez avec le bouton droit de la souris sur **Pare-feu** et cliquez sur **Créer une stratégie**.

Une **Nouvelle stratégie** est ajoutée à la liste et son nom est mis en surbrillance. Saisissez le nom que vous voulez utiliser pour la stratégie.

2. Cliquez deux fois sur la stratégie 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**.

13 Recherche 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. Passez à la section [Préparation de la protection des ordinateurs](#) à la page 14.

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 **Détecter des 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 de **Détection**, les ordinateurs sont placés dans le groupe **Non affectés**.

14 Préparation de la protection 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.

14.1 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" du chapitre "Protection des ordinateurs" de l'Aide de l'Enterprise Console.

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

Vous allez être invité à saisir les détails d'un compte utilisateur Windows qui peut être utilisé pour installer le logiciel de sécurité. 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 Console.
- Avoir une autorisation de lecture de 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**.

Remarque : si le volet **Stratégies** (en bas à gauche de la fenêtre) n'apparaît pas, dans le menu **Affichage**, cliquez sur **Ordinateurs d'extrémité**.

Nous vous conseillons d'utiliser un compte qui :

- Ne soit pas un compte d'administrateur de domaine et qu'il soit configuré pour une délégation limitée.
- Ne dispose pas des droits administratifs ou de tout autre privilège élevé sur les ordinateurs sur les lesquels l'Enterprise Console est installée.
- Ne dispose pas de droit en écriture ou en modification sur l'emplacement depuis lequel les ordinateurs se mettront à jour.
- Est uniquement utilisé pour assurer la protection des ordinateurs et pas pour effectuer des tâches administratives générales.
- Change de mot de passe régulièrement.

14.3 Préparation de l'installation du logiciel antivirus

Vous pouvez avoir besoin de préparer les ordinateurs avant l'installation du logiciel antivirus. Retrouvez plus de conseils dans le guide de déploiement de Sophos Endpoint (http://downloads.sophos.com/tools/on-line/deployment_guide/en-us/index.html) à la section sur la préparation des ordinateurs au déploiement.

Nous vous conseillons d'utiliser un pare-feu sur les ordinateurs protégés.

Remarque : une fois que les ordinateurs sont protégés et apparaissent comme étant administrés dans l'Enterprise Console, envisagez de désactiver toutes les exceptions de pare-feu créées spécialement pour autoriser le déploiement sur les ordinateurs.

15 Protection des ordinateurs

Cette section vous indique comment :

- Protéger automatiquement les ordinateurs Windows.
- Protéger manuellement les ordinateurs Windows ou Mac.
- Protéger les ordinateurs Linux (si votre licence l'autorise).

Vous pouvez aussi utiliser vos propres outils ou scripts pour installer la protection sur les ordinateurs Windows. Retrouvez plus d'informations sur www.sophos.com/fr-fr/support/knowledgebase/114191.aspx.

15.1 Protection automatique des ordinateurs Windows

Pour protéger les ordinateurs :

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 **Bienvenue**, cliquez sur **Suivant**.
 - b) Sur la page **Type d'installation**, laissez l'option **Logiciel de protection** sélectionnée.
 - c) Sur la page **Sélection des fonctions**, vous pouvez choisir d'installer des fonctions supplémentaires.

La version actuelle du pare-feu (incluse dans la version 10.2 ou antérieure de Endpoint Security and Control) ne peut pas être installée sur les ordinateurs Windows 8.
 - d) Sur la page **Récapitulatif de la protection**, recherchez tous les problèmes relatifs à l'installation. Retrouvez plus d'aide à la section [Résolution des problèmes](#) à la page 23.
 - e) Sur la page **Codes d'accès**, saisissez les détails d'un compte utilisateur Windows 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**, vous devez voir le terme **Actif** qui indique que le contrôle viral sur accès s'exécute sur cet ordinateur.

15.2 Protection manuelle des ordinateurs Windows ou Mac

15.2.1 Localisation des programmes d'installation

Si vous avez des ordinateurs que vous ne pouvez pas protéger depuis l'Enterprise Console, vous pouvez les protéger 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.

Pour rechercher les programmes d'installation :

1. Dans l'Enterprise Console, dans le menu **Affichage**, cliquez sur **Emplacements des fichiers d'amorce**.

Une liste des emplacements apparaît.

2. Prenez note de l'emplacement de chaque système d'exploitation que vous souhaitez protéger.

15.2.2 Protection manuelle des ordinateurs Windows

Vous devez utiliser un compte administrateur sur les ordinateurs que vous souhaitez protéger.

1. Sur chaque ordinateur que vous voulez protéger, naviguez vers l'emplacement des fichiers d'amorce, recherchez `setup.exe` et cliquez deux fois dessus.

2. Dans la boîte de dialogue **Configuration de Sophos**, dans les **Détails du compte utilisateur**, saisissez les détails du compte Update Manager, **SophosUpdateMgr**, que vous avez créé pour accéder au partage où l'Enterprise Console place les mises à jour logicielles. Vous avez exécuté cette opération dans [Compte Update Manager](#) à la page 9.

Info : vous pouvez aussi utiliser tout compte avec faibles privilèges pouvant accéder à l'emplacement du fichier d'amorce. L'Enterprise Console appliquera ultérieurement une stratégie de mise à jour qui inclut les bonnes informations du compte utilisateur.

Remarque : retrouvez plus d'informations sur les paramètres de ligne de commande pour le fichier `setup.exe`, dans l'article <http://www.sophos.com/fr-fr/support/knowledgebase/12570.aspx>.

15.2.3 Protection des Mac

Vous devez utiliser un compte administrateur sur les Mac que vous souhaitez protéger.

1. Sur chaque ordinateur que vous voulez protéger, naviguez jusqu'à l'emplacement des fichiers d'amorce. Copiez le fichier du programme d'installation `Sophos Installer.app` et le répertoire `Sophos Installer Components` à l'emplacement de votre choix (par exemple, le Bureau) et cliquez deux fois dessus.
Un assistant vous guide tout au long de l'installation.
2. Acceptez les options par défaut. Lorsque vous y êtes invité, saisissez les détails d'un compte utilisateur pouvant installer le logiciel sur le Mac.

15.3 Protection des ordinateurs Linux

Retrouvez plus de renseignements sur la protection des ordinateurs Linux ou UNIX (si inclut dans votre licence) dans le *Guide de démarrage de l'Enterprise Console pour Linux et UNIX*.

16 Paramétrage du logiciel de chiffrement sur les ordinateurs

Lisez cette section si votre licence inclut le chiffrement et si vous avez installé l'Enterprise Console pour gérer le chiffrement.

Attention ! Si vous installez le logiciel de chiffrement de Sophos pour la première fois, nous vous conseillons fortement d'activer et de tester chaque paramètre l'un après l'autre.

Pour paramétrer le chiffrement intégral du disque sur les ordinateurs, vous devez :

- Vous abonner au logiciel de chiffrement.
- Préparer l'installation du logiciel de chiffrement.
- Installer le logiciel de chiffrement automatiquement ou, si nécessaire, manuellement.

Remarque : le chiffrement intégral du disque peut actuellement être installé seulement sur les ordinateurs Windows XP (32 bits), Windows Vista et Windows 7.

Avertissement : avant d'installer le chiffrement intégral du disque sur les ordinateurs, vous devez :

- Vous assurer que les lecteurs chiffrés avec le logiciel de chiffrement tiers ont été déchiffrés et que ce logiciel de chiffrement tiers est désinstallé.
- Créer une sauvegarde complète des données sur les ordinateurs.

Pour une liste complète des préparations, reportez-vous à la section [Préparation de l'installation du logiciel de chiffrement](#) à la page 18.

16.1 Abonnement au logiciel de chiffrement

Si vous ne vous êtes pas encore abonné au logiciel de chiffrement et ne l'avez pas téléchargé à l'aide de l'**Assistant de téléchargement des logiciels de sécurité**, ajoutez le logiciel de chiffrement à votre abonnement logiciels.

1. Dans l'Enterprise Console, dans le menu **Affichage**, cliquez sur **Gestionnaires de mise à jour**.
2. Dans le volet **Abonnements logiciels**, cliquez deux fois sur l'abonnement que vous voulez modifier (par exemple, "Recommended").
3. Sous **Produits de chiffrement**, sélectionnez la case à cocher **Windows XP and above**, cliquez dans la case **Versión** et sélectionnez la version "Recommended" (version 5.61 à l'heure de cette publication). Cliquez sur **OK**.

Le logiciel de chiffrement est téléchargé dans le partage par défaut
\\<nom_serveur>\SophosUpdate\CIDs\<abonnement>\ENCRYPTION.

Remarque : l'application des stratégies de mise à jour à un groupe d'ordinateurs n'installe pas le logiciel de chiffrement. Vous devez lancer l'installation du logiciel de chiffrement vous-même.

16.2 Préparation de l'installation du logiciel de chiffrement

La préparation des ordinateurs au chiffrement implique d'effectuer les tâches suivantes :

- Attribuer à l'administrateur l'accès aux ordinateurs suite à l'installation.
- Préparer les ordinateurs à l'installation.

16.2.1 Attribution de l'accès administrateur aux ordinateurs suite à l'installation

Les administrateurs peuvent avoir besoin d'accéder et de pré-configurer les ordinateurs après avoir installé le logiciel de chiffrement, par exemple pour installer d'autres logiciels. Toutefois, le premier utilisateur qui se connecte après l'installation active l'authentification au démarrage. Pour éviter ceci, ajoutez les administrateurs respectifs à la liste des exceptions comme suit :

1. Dans l'Enterprise Console, dans le volet **Stratégies**, cliquez deux fois sur **Chiffrement intégral du disque**. Cliquez deux fois sur la stratégie **Par défaut** pour la modifier.
2. Sous **Authentification au démarrage (POA)**, cliquez sur **Exceptions** près de **Activer l'authentification au démarrage**.

3. Dans **Exceptions**, cliquez sur **Ajouter**, saisissez le **Nom d'utilisateur** et le **Nom de l'ordinateur ou de domaine** du ou des comptes Windows correspondants et cliquez sur **OK**.
Vous pouvez utiliser des caractères joker comme premier ou dernier caractère. Dans le champ **Nom d'utilisateur**, le caractère ? n'est pas autorisé. Dans le champ **Nom de l'ordinateur ou de domaine**, les caractères / \ [] : ; | = , + ? < > " ne sont pas autorisés.
4. Dans la boîte de dialogue des stratégies **Par défaut**, cliquez sur **OK**.
5. Dans le volet **Stratégies**, sélectionnez la stratégie et déplacez-la sur le groupe auquel vous voulez appliquer la stratégie. Lorsque vous y êtes invité, confirmez si vous désirez continuer.

16.2.2 Préparation des ordinateurs à l'installation

Si votre licence inclut le chiffrement intégral du disque, effectuez d'abord les étapes suivantes avant d'installer le logiciel de chiffrement sur les ordinateurs :

- Assurez-vous que les lecteurs chiffrés avec le logiciel de chiffrement tiers ont été déchiffrés et que ce logiciel de chiffrement tiers est désinstallé.
- Créez une sauvegarde complète des données.
- Vérifiez si un compte utilisateur Windows avec codes d'accès est configuré et actif sur l'ordinateur d'extrémité.
- Avant de déployer le chiffrement intégral du disque, assurez-vous que l'ordinateur a déjà été protégé avec la version 10 du logiciel antivirus Sophos.
- Désinstallez les gestionnaires de démarrage tiers, tels que PROnetworks Boot Pro et Boot-US.
- Recherchez toutes les erreurs du ou des disques durs à l'aide de cette commande :

```
chkdsk %drive% /F /V /X
```

Il se peut que vous soyez invité à redémarrer votre ordinateur et à exécuter de nouveau la commande **chkdsk**. Retrouvez plus d'informations sur :

<http://www.sophos.com/fr-fr/support/knowledgebase/107799.aspx>.

Vous pouvez vérifier les résultats (fichier journal) dans l'Observateur d'événements Windows :

Windows XP : sélectionnez **Application, Winlogon**.

Windows 7, Windows Vista : sélectionnez **Journaux Windows, Application, Wininit**.

- Utilisez l'outil de défragmentation intégré de Windows appelé **defrag** pour localiser et consolider les fichiers de démarrage, les fichiers de données et les dossiers fragmentés sur les lecteurs locaux :

```
defrag %drive%
```

Retrouvez plus d'informations sur :

<http://www.sophos.com/fr-fr/support/knowledgebase/109226.aspx>.

- Si vous avez utilisé un outil d'image/de clone sur l'ordinateur, nettoyez l'enregistrement de démarrage principal (MBR, master boot record). Démarrez l'ordinateur à partir d'un DVD Windows et utilisez la commande **FIXMBR** dans la Console de récupération Windows. Retrouvez plus d'informations sur :
<http://www.sophos.com/fr-fr/support/knowledgebase/108088.aspx>.

- Si la partition de démarrage de l'ordinateur a été convertie du format FAT au format NTFS et si l'ordinateur n'a pas encore été redémarré, redémarrez l'ordinateur. Si vous ne faites pas cela, il est possible que l'installation ne s'effectue pas avec succès.
- Ouvrez le Pare-feu Windows avec fonctions avancées de sécurité en allant dans le Panneau de configuration et en cliquant sur **Outils d'administration**. Assurez-vous que les **Connexions entrantes** sont autorisées. Changez les **Règles de trafic entrant** pour activer les processus ci-dessous.

- 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

Lorsque l'installation est terminée et si vous souhaitez continuer à utiliser le pare-feu Windows, vous pouvez désactiver le processus.

16.3 Installation automatique du logiciel de chiffrement

Attention ! Si vous installez le logiciel de chiffrement de Sophos pour la première fois, nous vous conseillons fortement d'activer et de tester chaque paramètre l'un après l'autre.

Assurez-vous que les ordinateurs d'extrémité ont été préparés pour l'installation du chiffrement intégral du disque, mais surtout que le logiciel de chiffrement tiers a été désinstallé, que toutes les données ont été sauvegardées et que la version 10 du logiciel antivirus de Sophos a été installée.

Pour installer le logiciel de chiffrement automatiquement :

1. Dans l'Enterprise Console, sélectionnez les ordinateurs sur lesquels vous voulez installer le chiffrement intégral du disque.
2. Cliquez avec le bouton droit de la souris sur les ordinateurs, puis cliquez sur **Protéger les ordinateurs**. L'**Assistant de protection des ordinateurs** est lancé.
3. Sur la page **Bienvenue**, cliquez sur **Suivant**.
4. Sur la page **Type d'installation**, sélectionnez **Logiciel de chiffrement**.
5. Si plus d'un abonnement au chiffrement et plus d'un emplacement du programme d'installation (emplacement du fichier d'amorce) sont disponibles, la page **Emplacement du chiffrement** apparaît. Sélectionnez l'**Abonnement au chiffrement** et l'**Adresse** à partir de laquelle effectuer l'installation.
6. Sur la page **Récapitulatif du chiffrement**, vérifiez tous les problèmes d'installation.
7. 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.

Les ordinateurs vont redémarrer automatiquement dans les 30 minutes suivant l'installation du logiciel de chiffrement. Si le chiffrement est activé par une stratégie, il sera appliqué uniquement après le redémarrage de l'ordinateur.

Retrouvez plus d'informations sur le comportement de l'ordinateur au démarrage et à la première connexion suite à l'installation et à l'activation du chiffrement à la section [Première connexion après installation](#) à la page 21.

16.4 Installation manuelle du logiciel de chiffrement

Attention ! Si vous installez le logiciel de chiffrement de Sophos pour la première fois, nous vous conseillons fortement d'activer et de tester chaque paramètre l'un après l'autre.

S'il est impossible de protéger automatiquement certains de vos ordinateurs, protégez-les en exécutant un programme d'installation depuis le dossier partagé dans lequel le logiciel de chiffrement a été téléchargé. Ce dossier partagé est plus connu sous le nom d'*emplacement du fichier d'amorce*.

Assurez-vous que les ordinateurs d'extrémité ont été préparés pour l'installation du chiffrement intégral du disque, mais surtout que le logiciel de chiffrement tiers a été désinstallé, que toutes les données ont été sauvegardées et que la version 10 du logiciel antivirus de Sophos a été installée.

Lors de l'installation du chiffrement intégral du disque, assurez-vous qu'il n'y a qu'une seule session utilisateur active sur l'ordinateur d'extrémité. Si vous n'effectuez pas cette opération, l'installation échouera.

Vous devez ouvrir une session en tant qu'administrateur Windows sur les ordinateurs que vous souhaitez protéger.

Pour installer manuellement le logiciel de chiffrement sur les ordinateurs :

1. Dans l'Enterprise Console, dans le menu **Affichage**, cliquez sur **Emplacements des fichiers d'amorce**.

Une liste des emplacements apparaît. Prenez note de l'emplacement de chaque système d'exploitation que vous souhaitez protéger.

2. Sur l'ordinateur qui héberge l'emplacement du fichier d'amorce, créez un compte utilisateur en lecture seule.
3. Allez sur chaque ordinateur et connectez-vous avec les droits d'administrateur local.
4. Recherchez le programme de configuration du chiffrement setup.exe dans l'emplacement du fichier d'amorce et cliquez deux fois dessus.

Le programme de configuration du chiffrement est disponible à l'emplacement suivant :
\\<NomServeur>\SophosUpdate\CIDs\<Abonnement>\ENCRYPTION

5. Un assistant vous guide tout au long de l'installation du logiciel de chiffrement.

Retrouvez plus d'informations sur le comportement de l'ordinateur au démarrage et à la première connexion suite à l'installation et à l'activation du chiffrement à la section [Première connexion après installation](#) à la page 21.

16.5 Première connexion après installation

Après l'installation du chiffrement, l'ordinateur redémarre et l'utilisateur est invité à se connecter. Le comportement de l'ordinateur dépend du type de compte avec lequel l'utilisateur se connecte :

- Connexion en tant qu'utilisateur avec un compte Windows normal.
- Connexion pour tâches administratives avec un compte Windows répertorié sur une liste d'exceptions.

Connexion en tant qu'utilisateur avec un compte Windows normal

La procédure de connexion correspond seulement à celle décrite ici si l'authentification au démarrage et le chiffrement ont été activés dans la stratégie de chiffrement intégral du disque.

Lorsque l'ordinateur redémarre, un certain nombre de messages (par exemple, l'écran de connexion automatique) s'affichent. Ensuite, le système d'exploitation Windows démarre. L'utilisateur se connecte à Windows à l'aide de ses codes d'accès Windows. L'utilisateur est enregistré en tant qu'utilisateur Sophos SafeGuard sur l'ordinateur.

Remarque : pour confirmer le succès de l'enregistrement, une infobulle apparaît sur l'ordinateur d'extrémité.

S'il est activé par la stratégie, le chiffrement démarre sur les lecteurs sélectionnés. Le chiffrement et le déchiffrement sont exécutés en tâches de fond sans intervention de l'utilisateur. L'utilisateur peut continuer de travailler ou éteindre l'ordinateur pendant le processus de chiffrement. Aucun redémarrage n'est requis suite à l'installation du chiffrement.

Au prochain démarrage de l'ordinateur par l'utilisateur, l'authentification au démarrage est activée. Maintenant, l'utilisateur doit seulement saisir ses codes d'accès Windows à l'authentification au démarrage et est automatiquement connecté à Windows.

Remarque : lors du démarrage de l'ordinateur après mise en veille, l'utilisateur doit saisir ses codes d'accès Windows à l'authentification au démarrage et dans Windows.

Retrouvez plus d'informations dans le *Manuel d'utilisation de Sophos Disk Encryption*.

Connexion pour tâches administratives avec un compte Windows répertorié sur une liste d'exceptions

La procédure de connexion correspond seulement à celle décrite ici si l'utilisateur se connecte à un compte Windows qui a été placé dans une liste d'exceptions et si l'authentification au démarrage a été activée dans la stratégie de chiffrement intégral du disque.

Lorsque l'ordinateur redémarre, le système d'exploitation Windows démarre. La boîte de dialogue de connexion Windows apparaît. L'utilisateur se connecte à l'aide de ses codes d'accès définis auparavant dans la stratégie de chiffrement intégral du disque. L'utilisateur est connecté à Windows en tant qu'utilisateur invité. L'authentification au démarrage n'est pas activée. Le processus de chiffrement ne démarre pas. L'utilisateur peut procéder aux tâches postérieures à l'installation nécessaires.

17 Vérification du bon fonctionnement de votre réseau

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

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.

18 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. Retrouvez plus d'informations à la section [Protection des Mac](#) à la page 17. Pour les autres systèmes d'exploitation (si leur protection est incluse dans votre licence), consultez le *Guide de démarrage de Sophos Enterprise Console pour Linux et UNIX*.
- 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 règles de pare-feu bloquent l'accès nécessaire au déploiement du logiciel de sécurité.
- Vous avez essayé d'installer le chiffrement intégral du disque sur les ordinateurs sur lesquels le logiciel antivirus n'a pas encore été installé.

19 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.

Tâche	Document
Protéger les ordinateurs autonomes	Guide de démarrage avancé de l'Enterprise Console : « Protection des ordinateurs autonomes »

Tâche	Document
Configurer les stratégies de l'Enterprise Console	Aide de l'Enterprise Console : « Configuration des stratégies »
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 Enterprise Console	Aide de l'Enterprise Console : « Génération de rapports »

20 Support technique

Vous bénéficiez du support technique des produits Sophos de l'une des manières suivantes :

- Rendez-vous sur le forum de la communauté SophosTalk en anglais sur 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 www.sophos.com/fr-fr/support.aspx.
- Téléchargez la documentation des produits sur www.sophos.com/fr-fr/support/documentation.aspx.
- Ouvrez un incident support sur <https://secure2.sophos.com/fr-fr/support/contact-support/support-query.aspx>.

21 Mentions légales

Copyright © 2009–2015 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, Sophos Anti-Virus et SafeGuard sont des marques déposées de Sophos Limited, Sophos Group et de Utimaco Safeware AG, partout où ceci est applicable. Tous les autres noms de produits et d'entreprises cités dans ce document sont des marques ou des marques déposées de leurs propriétaires respectifs.

ACE™, TAO™, CIAO™, DAnCE™, and CoSMIC™

ACE™, TAO™, CIAO™, DAnCE™, and CoSMIC™ (henceforth referred to as "DOC software") are copyrighted by Douglas C. Schmidt and his research group at Washington University,

[University of California, Irvine](#), and [Vanderbilt University](#), Copyright (c) 1993-2014, all rights reserved. Since DOC software is open-source, freely available 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 any code built using DOC software that you release. No copyright statement needs to be provided if you just ship binary executables of your software products.

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 misappropriate the DOC software code, such as copyrighting it yourself or claiming authorship of the DOC software code, in a way 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](#) know so we can promote your project in the [DOC software success stories](#).

The [ACE](#), [TAO](#), [CIAO](#), [DAnCE](#), and [CoSMIC](#) web sites are maintained by the [DOC Group](#) at the [Institute for Software Integrated Systems \(ISIS\)](#) and the [Center for Distributed Object Computing](#) of Washington University, St. Louis for the development of open-source software as part of the open-source software community. Submissions are provided by the submitter "as is" with no warranties whatsoever, including any warranty of merchantability, noninfringement of third party intellectual property, or fitness for any particular purpose. In no event shall the submitter be liable for any direct, indirect, special, exemplary, punitive, or consequential damages, including without limitation, lost profits, even if advised of the possibility of such damages. Likewise, 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. 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.

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](#) 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. Likewise, DOC software is compliant with the new US daylight savings rule passed by Congress as "The Energy Policy Act of 2005," which established new daylight savings times (DST) rules for the United States that expand DST as of March 2007. Since DOC software obtains time/date and calendaring information from operating systems users will not be affected by the new DST rules as long as they upgrade their operating systems accordingly.

The names [ACE™](#), [TAO™](#), [CIAO™](#), [DAnCE™](#), [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. This license grants no permission to call products or services derived from this source [ACE™](#), [TAO™](#), [CIAO™](#), [DAnCE™](#), or [CoSMIC™](#), nor does it grant permission for the name Washington University, UC Irvine, or Vanderbilt University to appear in their names.

If you have any suggestions, additions, comments, or questions, please let [me](#) know.

[Douglas C. 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>.

Boost

Version 1.0, 17 August 2003

Permission is hereby granted, free of charge, to any person or organization obtaining a copy of the software and accompanying documentation covered by this license (the "Software") to use, reproduce, display, distribute, execute, and transmit the Software, and to prepare derivative works of the Software, and to permit third-parties to whom the Software is furnished to do so, all subject to the following:

The copyright notices in the Software and this entire statement, including the above license grant, this restriction and the following disclaimer, must be included in all copies of the Software, in whole or in part, and all derivative works of the Software, unless such copies or derivative works are solely in the form of machine-executable object code generated by a source language processor.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR ANYONE DISTRIBUTING THE SOFTWARE BE LIABLE FOR ANY DAMAGES OR OTHER LIABILITY, WHETHER IN CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

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 chaque logiciel couvert par la licence CPL, le code source est disponible sur commande par courrier postal envoyé à Sophos, par e-mail à support@sophos.fr ou par Internet sur <http://www.sophos.com/fr-fr/support/contact-support/contact-information.aspx>. 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.

Loki

The MIT License (MIT)

Copyright © 2001 by Andrei Alexandrescu

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

OpenSSL Cryptography and SSL/TLS 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.

OpenSSL license

Copyright © 1998-2011 The OpenSSL Project. All rights reserved.

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.
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 (<http://www.openssl.org/>)”

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

Original SSLeay license

Copyright © 1995–1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (eay@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).

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.]