

SOPHOS

Sophos Endpoint Security and Control Guide de test pour Windows XPe/Windows Embedded Standard

Version du produit : 9.0

Date du document : septembre 2009



Table des matières

1 A propos de ce guide.....	3
2 Préparation aux tests.....	3
3 Installation des logiciels de sécurité.....	3
4 Test de la détection des menaces.....	4
5 Test de contrôle des applications.....	5
6 Test de contrôle des données.....	6
7 Test de contrôle des périphériques.....	6
8 Copyright.....	7

1 A propos de ce guide

Ce guide est destiné à l'administrateur réseau qui veut protéger les ordinateurs utilisant Windows XP Embedded (Windows XPe) ou Windows Embedded Standard.

Les versions intégrées de Windows peuvent être compilées avec de nombreuses personnalisations différentes, ce guide ne tente donc pas de savoir si chacune d'entre elles peut être protégée avec succès. A la place, il indique comment exécuter des vérifications après installation pour voir si les logiciels de sécurité Sophos fonctionnent correctement.

Il est supposé dans ce guide que vous avez déjà utilisé Sophos Enterprise Console pour l'installation et l'administration des logiciels Sophos sur votre réseau.

Il y est décrit comment :

- Installer les logiciels de sécurité Sophos sur les ordinateurs utilisant Windows XPe/Windows Embedded Standard.
- Tester si les logiciels sont en cours de mise à jour.
- Tester la détection des menaces.
- Tester le contrôle des applications, des données et des périphériques.

Important : si vous réussissez tous les tests de ce guide, nous ferons tous les efforts commercialement raisonnables pour assurer un support technique conforme aux pratiques commerciales standard Sophos. Pour plus de détails, consultez l'article 63797 de la base de connaissances du support de Sophos (<http://www.sophos.fr/support/knowledgebase/article/63797.html>).

2 Préparation aux tests

Avant de commencer :

- Sélectionnez les ordinateurs d'extrémité exécutant Windows XPe/Windows Standard Embedded à utiliser comme ordinateurs de test.
- Assurez-vous que le fichier de test de détection virale EICAR est installé ou est prêt à être installé sur vos ordinateurs de test.
- Assurez-vous que MSN Messenger Live est disponible pour être installé sur les ordinateurs de test lors du test de contrôle des applications.

3 Installation des logiciels de sécurité

Avant de tester, vous devez :

- Installer les logiciels de sécurité sur les ordinateurs de test.
- Vérifier que les logiciels sont en cours de mise à jour.

3.1 Installation des logiciels

Installez Sophos Endpoint Security and Control 9.0 pour Windows de la même manière que vous l'installeriez sur n'importe quel autre poste d'extrémité Windows.

Vous pouvez exécuter l'une des deux opérations suivantes :

- **Installation automatique.** Dans l'Enterprise Console, recherchez les ordinateurs de test et assurez-vous qu'ils ont une stratégie de mise à jour valide. Sélectionnez-les, cliquez dessus avec le bouton droit de la souris et cliquez sur **Protéger les ordinateurs**.
- **Installation manuelle.** Sur les ordinateurs de test, naviguez vers le dossier à partir duquel les ordinateurs d'extrémité se mettent à jour et exécutez le programme d'installation Sophos.

Remarque : le dossier à partir duquel les ordinateurs se mettent à jour est disponible en consultant les **Emplacements des fichiers d'amorce** dans l'Enterprise Console.

3.2 Vérification de la mise à jour

Vérifiez que les ordinateurs de test reçoivent les mises à jour Sophos.

Sur les ordinateurs de test :

1. Dans la barre des tâches, cliquez avec le bouton droit de la souris sur l'icône Sophos et sélectionnez **Mettre à jour maintenant**. Attendez que la mise à jour se termine.
2. Ouvrez Sophos Endpoint Security and Control.
3. Dans la page d'accueil, dans le volet **Etat**, vérifiez que l'heure de **Dernière mise à jour** a changé.

4 Test de la détection des menaces

4.1 Vérification du fonctionnement de la détection

Pour vérifier que Sophos Endpoint Security and Control parvient à détecter les menaces, effectuez un test EICAR comme suit.

1. Sur les ordinateurs de test, tentez de copier un fichier test EICAR sur l'ordinateur (ou d'exécuter EICAR s'il est déjà sur l'ordinateur).

Les ordinateurs de test doivent afficher une alerte virale.

2. Vérifiez que les ordinateurs de test affichent le fichier EICAR dans le Gestionnaire de quarantaine et que les détails sont corrects.

4.2 Vérification des alertes

Allez dans l'Enterprise Console et procédez ainsi :

1. Vérifiez que les onglets dans la vue liste des ordinateurs indiquent le nom du virus, l'emplacement et l'heure de la découverte.
2. Vérifiez que les détails des ordinateurs de test sont corrects.

Vous devez maintenant effacer les alertes.

4.3 Effacement des alertes

1. Sur les ordinateurs de test, effacez l'alerte dans le Gestionnaire de quarantaine.
2. Dans l'Enterprise Console, effacez l'alerte dans la boîte de dialogue **Résoudre les alertes et les erreurs**.

5 Test de contrôle des applications

5.1 Configuration du contrôle des applications

1. Dans l'Enterprise console, ouvrez une stratégie de contrôle des applications.
2. Configurez la stratégie pour bloquer MSN Live Messenger.
3. Appliquez la stratégie aux ordinateurs de test.
4. Dans l'Enterprise Console, vérifiez que le changement de stratégie est en cours d'application et que les ordinateurs de test sont conformes à la stratégie.

5.2 Vérification du fonctionnement du contrôle des applications

1. Sur les ordinateurs de test, cliquez avec le bouton droit de la souris sur l'icône SESC et sélectionnez Mettre à jour maintenant.
2. Tentez d'installer et d'ouvrir MSN Live Messenger.
3. Vérifiez qu'une alerte est affichée. L'application devrait être affichée dans le Gestionnaire de quarantaine et tous les détails doivent être corrects, y compris le type.
4. Dans l'Enterprise Console, vérifiez la vue liste des ordinateurs et la page des détails des ordinateurs.

5.3 Effacement des alertes et réinitialisation de la stratégie

1. Sur les ordinateurs de test, effacez les alertes du Gestionnaire de quarantaine.
2. Dans l'Enterprise Console, repassez la stratégie de contrôle des applications à son paramétrage d'origine.
3. Vérifiez que le système d'extrémité et la console se conforment au changement de la stratégie.

6 Test de contrôle des données

6.1 Configuration du contrôle des données

1. Dans l'Enterprise Console, créez une stratégie de contrôle des données et ouvrez-la.
2. Dans l'onglet **Règles de la stratégie**, cliquez sur **Gérer les règles**.
3. Dans la boîte de dialogue **Gestion des règles de contrôle des données**, cliquez sur **Ajouter une règle de contenu**.
4. Entrez un nom de règle. Sous **Règle de contenu**, cliquez sur le lien dans "Où le fichier contient".
5. Dans la boîte de dialogue **Gestion des Listes de contrôle du contenu**, sélectionnez une Liste de contrôle du contenu (CCL) et cliquez sur **OK**.
6. Sous **Règle de contenu**, cliquez sur le lien "Sélectionner une destination" et cochez **Stockage amovible**. Cliquez sur **OK**.
7. Dans la boîte de dialogue **Gestion des règles de contrôle des données**, sélectionnez la règle que vous avez créée et cliquez sur **OK**.
8. Fermez toutes les boîtes de dialogue et appliquez la stratégie aux ordinateurs de test.

6.2 Vérification du fonctionnement du contrôle des données

1. Sur les ordinateurs de test, ouvrez Sophos Endpoint Security and Control.
2. Sur la page d'accueil, dans le volet **Etat**, vérifiez que le contrôle des données apparaît comme activé.
3. Cliquez sur l'icône **Journal du contrôle des données**. Vérifiez que le contrôle des données a commencé.

7 Test de contrôle des périphériques

7.1 Configuration du contrôle des périphériques

1. Dans l'Enterprise Console, ouvrez une stratégie de contrôle des périphériques.
2. Configurez la stratégie pour bloquer **Modems** et **Sans fil**.

Dans les Détails de l'ordinateur, la colonne Conformité à la stratégie de contrôle des périphériques doit indiquer "En attente du transfert de stratégies", puis "Identique à la stratégie".

3. Appliquez la stratégie aux ordinateurs d'extrémité de test.
4. Vérifiez que le système d'extrémité est désormais conforme à la stratégie.

7.2 Vérification du fonctionnement du contrôle des périphériques

1. Sur les ordinateurs d'extrémité, connectez modem et périphériques sans fil.
Une bulle d'avertissement doit apparaître pour chaque périphérique bloqué.
2. Ouvrez Sophos Endpoint Security and Control. Sur la page d'accueil, cliquez sur **Journal de contrôle des périphériques** et vérifiez que le périphérique est bloqué.
3. Vérifiez que le Gestionnaire de périphériques Windows indique que le périphérique a été désactivé.
4. Utilisez le périphérique sans fil pour tenter de contacter un réseau sans fil.
Windows doit indiquer que le périphérique est bloqué et ne peut pas détecter les réseaux.
5. Utilisez le Gestionnaire de périphériques Windows pour tester le périphérique du modem.
Vérifiez que le modem ne peut pas être testé.

7.3 Réinitialisation de la stratégie de contrôle des périphériques

1. Dans l'Enterprise Console, paramétrez la stratégie de contrôle des périphériques ainsi :
 - Modem : Accès intégral.
 - Sans fil : Accès intégral.
2. Appliquez la stratégie aux ordinateurs de test.
3. Vérifiez que les ordinateurs sont conformes à la stratégie.
4. Sur les ordinateurs de test, cliquez sur l'icône **Journal du contrôle des périphériques** et vérifiez que le périphérique est activé.
5. Sur le système d'extrémité, vérifiez que le périphérique sans fil peut détecter les réseaux sans fil.
6. Utilisez le Gestionnaire de périphériques Windows pour tester le périphérique du modem.
Vérifiez que le test automatique de périphérique est un succès.

8 Copyright

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

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

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.com 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>