

Sophos Endpoint Security and Control Guide du Deployment Packager

Version du produit : 9.7

Date du document : avril 2011



Table des matières

1	À propos de ce guide.....	3
2	À propos de l'outil Deployment Packager.....	4
3	Configuration requise.....	5
4	Création d'un package via l'interface graphique utilisateur.....	6
5	Annexe : création d'un package via la ligne de commande.....	9
6	Support technique.....	11
7	Mentions légales.....	12

1 À propos de ce guide

Ce guide vous explique comment utiliser l'outil gratuit Sophos Deployment Packager. Pour plus d'informations sur l'utilisation de cet outil par les MSP (Managed Service Providers), consultez le *Guide de Managed Service Provider*.

Ce guide suppose que vous êtes habitué à utiliser la Sophos Enterprise Console et Sophos Endpoint Security and Control.

La documentation Sophos est disponible sur www.sophos.fr/support/docs/.

2 À propos de l'outil Deployment Packager

Le Deployment Packager crée un fichier archive unique auto-extractible à partir d'une série de fichiers de configuration de systèmes d'extrémité émis par Sophos, en vue de l'installation d'Endpoint Security and Control sur les systèmes d'extrémité clients. Le fichier sous forme de package inclut des options de configuration telles que l'installation silencieuse/interactive, le choix des composants d'installation, les codes d'accès ou chemin de mise à jour et l'appartenance aux groupes de systèmes d'extrémité. Les packages créés avec le Deployment Packager tentent toujours de supprimer d'autres logiciels antivirus ou de sécurité en conflit potentiel lors de leur installation. Il peut s'avérer judicieux de créer plusieurs packages, chacun répondant aux conditions requises des différents types de systèmes d'extrémité.

L'outil Deployment Packager peut s'exécuter soit via l'interface graphique utilisateur soit via une ligne de commande.

- L'interface graphique utilisateur est plus facile à utiliser pour un déploiement unique.
- La ligne de commande est plus souple à utiliser pour des déploiements répétés.

Une chaîne de caractères utilisée pour appeler la version par ligne de commande peut être stockée dans un fichier texte avec toutes ses options ou exécutée régulièrement à partir d'un fichier de commandes planifié, garantissant ainsi la mise à jour permanente des packages d'installation. Si vous administrez un grand nombre d'ordinateurs nécessitant une installation fréquente sur les systèmes d'extrémité, il est préférable d'utiliser la ligne de commande.

Les instructions d'utilisation du Deployment Packager via la ligne de commande sont disponibles à la section [Annexe : création d'un package via la ligne de commande](#) à la page 9.

3 Configuration requise

Pour exécuter l'outil Deployment Packager, les configurations requises minimales sont les suivantes :

- Systèmes d'exploitation Windows : rendez-vous sur <http://www.sophos.fr/products/enterprise/endpoint/security-and-control/management/sysreqs.html>
- Espace disque : 1 Go
- Mémoire : 1 Go
- Processeur : Pentium 2 GHz ou équivalent

Vérifiez également les configurations requises des packages de composants des systèmes d'extrémité. Rendez-vous sur <http://www.sophos.fr/products/all-sysreqs.html>.

4 Création d'un package via l'interface graphique utilisateur

1. Pour créer un package via l'interface utilisateur, lancez DeploymentPackager.exe.

La boîte de dialogue Deployment Packager apparaît.

The screenshot shows the 'Deployment Packager' dialog box with the following settings:

- Archive:**
 - Source CID: \\SEC-console\CIDs\Win
 - Destination package: c:\Sophos\GroupInstallWin.exe
- Components:**
 - Remote management
 - Firewall
 - NAC (NAC server URL:)
 - Install the above components from the packaged CID
- Updating:**
 - Path: http://192.168.0.8
 - User: Updateuser
 - Password: [masked]
- Options:**
 - Silent
 - Non-interactive
 - Command line: -g \SEC-console\Group

2. Dans le volet **Archive**, saisissez les éléments suivants :

- a) Dans **Source CID**, spécifiez l'emplacement du répertoire d'installation centralisée contenant les fichiers d'installation des logiciels de systèmes d'extrémité. Il peut s'agir d'un nom de chemin UNC ou d'une URL.
- b) Dans **Destination package**, spécifiez le chemin de destination du package d'installation en sortie. Vous pouvez aussi spécifier un nom de fichier facultatif. Si celui-ci n'est pas fourni, le Deployment Packager utilise un nom de fichier par défaut.

3. Dans le volet **Components**, sélectionnez parmi les composants suivants :

■ **Remote management**

Ce composant installe et active le Sophos Remote Management System (RMS), qui permet à l'Enterprise Console de contrôler Endpoint Security and Control. Pour les systèmes administrés, vous devez activer ce composant. Pour plus d'informations sur les systèmes d'extrémité administrés indirectement, reportez-vous à l'article <http://www.sophos.fr/support/knowledgebase/article/67372.html>

Remarque : lorsque vous sélectionnez cette option, les systèmes d'extrémité obtiennent leurs chemins de mise à jour et leurs codes d'accès depuis l'Enterprise Console via RMS.

■ **Firewall**

Ce composant installe Sophos Client Firewall.

Remarque : si vous voulez installer cette option, vérifiez la configuration système requise pour les systèmes d'exploitation sur <http://www.sophos.fr/products/all-sysreqs.html>

■ **NAC**

Ce composant installe le contrôle d'accès réseau Sophos NAC (Network Access Control).

■ **Install the above components from the packaged CID**

Ceci inclut les composants choisis dans le package de déploiement. Autrement, seul Sophos AutoUpdate est inclus. Les autres composants sont téléchargés depuis la source de mise à jour.

Remarque : le programme d'installation des systèmes d'extrémité n'est pas en mesure d'utiliser un serveur proxy. Si un serveur proxy permet d'accéder à l'emplacement de mise à jour, les composants des systèmes d'extrémité requis doivent être inclus dans le package.

Remarque : si vous sélectionnez **Remote management** et **Install the above components from the deployment package**, tous les détails de l'option **Updating** sont récupérés depuis l'Enterprise Console et sont grisés.

4. Dans le volet **Updating**, pour les packages des systèmes d'extrémité administrés indirectement ou lorsque l'administration à distance est activée mais pas incluse dans le package, saisissez le chemin de mise à jour et les codes d'accès. Vous pouvez définir " :<numéro de port>" d'après une URL HTTP. S'il n'est pas défini, la valeur par défaut sera 80.

Remarque : les codes d'accès sont dissimulés dans le package. En revanche, les comptes définis pour les systèmes d'extrémité pour pouvoir lire les emplacements des serveurs de mise à jour doivent toujours être aussi restrictifs que possible, permettant seulement un accès en lecture seule.

Remarque : les systèmes d'extrémité tentent d'utiliser leurs paramètres proxy système seulement s'ils sont définis à l'aide des variables d'environnement `http_proxy` ou `all_proxy`. Les paramètres proxy dans les Options Internet du Panneau de configuration ou dans Internet Explorer sont ignorés. Les valeurs variables `_proxy` prennent le format `_proxy=[protocole://][utilisateur:motdepasse@]host[:port]`, par exemple `http_proxy=http://utilisateur:motdepasse@proxy:8080`

5. Dans le volet **Options**, sélectionnez les options qui déterminent comment le programme d'installation s'exécute sur les ordinateurs d'extrémité.

- **Silent**

Le programme fonctionne en mode silencieux. Si vous sélectionnez cette option, l'option **Non-interactive** est automatiquement sélectionnée et grisée.

- **Non-interactive**

Le programme fonctionne en mode non interactif.

- **Command line**

Utilisez cette zone de modification pour spécifier les options d'installation. Spécifiez toujours l'appartenance à un groupe à l'aide de l'option `-g`, comme le montre la capture d'écran ci-dessus, de manière à ce chaque programme d'installation soit spécifique et paramètre les systèmes d'extrémité pour qu'ils soient membres des groupes déjà existants.

Le Deployment Packager ne vérifie pas ces options à la recherche d'erreurs.

Pour plus de détails, rendez-vous sur

<http://www.sophos.fr/support/knowledgebase/article/12570.html>.

6. Cliquez sur **Build Package** pour créer l'archive auto-extractible.

Le bouton Help ouvre un article de la base de connaissances sur le site Web de Sophos.

5 Annexe : création d'un package via la ligne de commande

Avant d'utiliser cette section, reportez-vous à la section [Création d'un package via l'interface graphique utilisateur](#) à la page 6.

Pour exécuter le Deployment Packager en mode de ligne de commande, utilisez le format suivant :

DeploymentPackager -cli -mng yes -cidpath <cheminCID> -sfxpath <cheminSFX> -crt R

où <cheminCID> est le chemin vers le répertoire d'installation centralisée correspondant et <cheminSFX> le chemin du package résultant.

Le Packager renvoie une valeur de zéro lorsqu'il est exécuté avec succès et autre que zéro pour une condition d'erreur, accompagné d'un message vers stderr.

Vous pouvez aussi utiliser les qualificatifs de ligne de commande mentionnés ci-dessous.

Options de ligne de commande

-mng yes

Active l'administration à distance

-scf

Installe Sophos Client Firewall

-nac <URLNAC>

Installe le contrôle d'accès réseau avec <URLNAC> en tant qu'adresse du serveur NAC.

-sauonly

Inclut uniquement Sophos AutoUpdate (l'administration à distance et les composants du pare-feu et de NAC sont téléchargés à partir de la source de mise à jour). Si cette option n'est pas sélectionnée, les composants sont inclus dans le package.

-upd <chemin_mise à jour>

Chemin de mise à jour.

-user <nomutilisateur>

-pwd <mot de passe>

Nom utilisateur et mot de passe. Le Packager dissimule ces derniers dans le package. En revanche, si vous enregistrez une ligne de commande du Deployment Packager avec un nom utilisateur et un mot de passe clairs dans un fichier texte ou un fichier de commandes, assurez-vous qu'elle est sécurisée.

-opwd <mot de passe_dissimulé>

Mot de passe dissimulé. Pour plus d'informations sur la dissimulation des mots de passe, reportez-vous à l'article de la base de connaissances *Dissimulation du nom utilisateur et du mot de passe* sur <http://www.sophos.fr/support/knowledgebase/article/13094.html>

-s

Installation silencieuse

-ni

Installation non interactive

Autres options

Toutes les autres options sont compressées pour être exécutées avec le fichier de configuration du programme d'installation.

6 Support technique

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

- Rendez-vous sur le forum de la communauté SophosTalk en anglais sur <http://community.sophos.com/> et recherchez d'autres utilisateurs rencontrant le même problème que le vôtre.
- Rendez-vous sur la base de connaissances du support de Sophos sur <http://www.sophos.fr/support/>.
- Téléchargez la documentation des produits sur <http://www.sophos.fr/support/docs/>.
- Envoyez un courriel à support@sophos.fr, y compris le ou les numéros de version du logiciel Sophos, le ou les systèmes d'exploitation et le ou les niveaux de correctif ainsi que le texte du ou des messages d'erreur.

7 Mentions légales

Copyright © 2011 Sophos Limited. Tous droits réservés. Aucune partie de cette publication ne peut être reproduite, stockée dans un système de recherche documentaire ou transmise, sous quelque forme ou par quelque moyen que ce soit, électronique, mécanique, photocopie, enregistrement ou autre sauf si vous possédez une licence valide, auquel cas vous pouvez reproduire la licence conformément à ses termes ou si vous avez le consentement préalable écrit du propriétaire du copyright.

Sophos et Sophos Anti-Virus sont des marques déposées de Sophos Limited. Tous les autres noms de produits et de sociétés mentionnés sont des marques ou des marques déposées appartenant à leurs propriétaires respectifs.

OpenSSL cryptographic toolkit

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

OpenSSL license

Copyright © 1998–2006 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.

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 licence 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 licence [including the GNU Public Licence.]