Comment ajouter les exclusions prédéfinies pour Kaspersky Endpoint Security 10

vleclerc.wordpress.com/2013/07/22/comment-ajouter-les-exclusions-prdfinies-pour-kaspersky-endpoint-security-10

vleclerc

July 22, 2013

L'astuce de ce billet est de pouvoir créer et/ou ajouter les exclusions dans la stratégie de paramétrage de Kaspersky Endpoint Security 10.

En effet par défaut certaines exclusions ne sont pas ajoutées par l'assistant de démarrage rapide du serveur d'administration ou bien si vous avez choisi de convertir une ancienne stratégie qui ne possédait pas non plus une liste d'exclusion.

Etape 1 : Création

Ouvrir la console d'administration et créer un groupe de test pour pouvoir exporter/importer à une stratégie existante la liste d'exclusions ou bien créer directement cette stratégie dans le groupe de gestion concerné.

Groupes Stratégies Tâches Ordinateurs	
	Guide de démarrage » Test
Stratégies Les stratégies sont utilisées pour configurer les paramètres de protection et les paramètres généraux des applications.	
Actualiser Assistant de création d'une stratégie Assistant de création d'une stratégie	
EXClusions Utiliser les rècles standard nour les annications suivantes :	icher les stratégies héritées
Nom ^ Etat Applice Imbuku Pro Imbuku Pro Imbuku Pro Dameware Mini Remote Control Application Imbuku Pro Dameware Mini Remote Control Application Imbuku Pro Symantec Imbuku Pro Sulvant Annul Sulvant	er

Depuis l'onglet Stratégies, cliquer sur le lien "Créer une stratégie de Kaspersky Endpoint Security 10 for Windows".

Sélectionner l'ensemble des paramètres jusqu'à la boite de dialogue des Exclusions.

• Ici vous pouvez sélectionner les exclusions des principaux éditeurs, par

exemple pour Lotus Domino (IBM).

• Cocher les cases pour ajouter les règles recommandées pour les postes de travail et les serveurs.

Cliquer sur "suivant" et valider les autres configurations pour terminer l'assistant.

Il ne reste plus qu'à appliquer cette configuration.

Etape 2 : Export

ASTUCE ! Pour pouvoir exporter cette nouvelle liste, voici ce qu'il faut faire :

Ouvrir la stratégie précédemment créée

				Guide de démarrage > 1
Stratégies Les stratégies sont utilisées pour configu + Créer une stratégie	er les paramètre	s de protection et les paramètres généraux d Propriétés : Nouvelle stratégie Soctions	es antications.	
 Créer une stratégie de Kaspersk Importer une stratégie à partir d'un f Actualiser 	y Endpoint Secur	Général Evénements Endpoint Control Contrôle du lancement des applications Contrôle de l'activité des applications Surveillance des vulnérabilités	Parametres généraux Paramètres Paramètres généraux Paramètres Paramètres généraux Paramètres Paramètres généraux Paramètres Paramètres généraux Paramètres	Vindows au démarrage de l'ordinateur fection active • types suivants : ants :
m *	Etat	Contrôle des périphériques	 logiciels publicitaires, numéroteurs automatique 	25 ;
aspersky Endpoint Security 10 for 3	amoboil	Filtrage de contenu	- fichiers compressés qui peuvent nuire, fichiers	compressés à plusieurs reprises.
	ACCE	Paramètres généraux de chiffrement Chiffrement des disques durs Chiffrement des fichiers et des dossiers Chiffrement des disques amovibles Expont Protection Paramètres généraux Antivirus Fichiers Antivirus Courrier	Controle south: Controle south: Controler jous les ports réseau Contrôler jous les ports réseau Contrôler jous les ports réseau	Configuration
		Aide		OK Annuler Appliquer
			Chilfrement des fichiers et des dossiers Endpoint Protection Paramètres généraux Antivirus Courrier Antivirus Courrier Childra Marchand Childra	Chiffrement des disques amovibles Chiffrement des disques amovibles Chiffrement Chiffreme
			Antivirus IM ("Chat")	Pare-feu

Cliquer sur **"Paramètres généraux**" puis sur le bouton **"Configuration**" de la section **"Exclusions et zone de confiance**".



Nota : N'oubliez pas de changer certains chemins afin de correspondre à vos répertoires d'installation. Exemple pour les répertoires de Microsoft Exchange:

Par défaut : %ProgramFiles%\Exchsrvr\Mailroot\

Si votre répertoire d'installation est sur le disque D: changer le chemin comme suit :

Fichier ou dossier	Nom de l'objet
✓ %ProgramFiles % \Exchsrvr \Mailroot \	
✓ %ProgramFiles%\Exchsrvr\Srsdata*	8
✓ %ALLUSERSPROFILE%\Documents\SoftGrid Client\	*
✓ %SYSTEMDRIVE%\LC Archiving Data*.mdf	8
✓ %SYSTEMDRIVE%\LC Archiving Log*.ldf	8
✓ %SYSTEMDRIVE%\LC Data*.mdf	*
✓ %SYSTEMDRIVE%\LC Log*.ldf	🔀 Nom du fichier ou du dossier 🛛 🗙
♥ %ProgramFiles % Wicrosoft Operations Manager 2005 MOMHc	
✓ %ProgramFiles% Wicrosoft Operations Manager 2005 WebCo	Saisissez le nom ou le masque du nom du fichier ou du dossier :
SYSTEMDRIVE%\System Volume Information\catalog.wci	Diffusion with death
✓ %SYSTEMDRIVE%\Pagefile.sys	Parcourir
✓ %SYSTEMDRIVE%\Inetpub\mailroot\	Sous-dossiers compris
Description de la règle (cliquez sur les éléments soulignés pour les r	A Le chemin d'accès au dossier doit se terminer par "\".
Le fichier ou le dossier ne sera pas analysé quand les cooditions s Fichier ou dossiel : <u>%ProgramFiles%\Exchsrvr\Mailroot\</u> Modules de protec tion : quelconque	Aide OK Annuler

Une fois l'ensemble des exclusions définies, exporter les dans un fichier :



Sélectionner les règles à exporter.

Cliquer sur le bouton "**Exportation**" et cliquer sur le bouton "**Oui**" pour ne prendre que les éléments sélectionnés.

Nota : vous pouvez également prendre toutes les exclusions.

Bibliothèqu	ies + Documents +	× 🔯	Rechercher dans : Do	cuments	
Organiser 👻 Nouveau dos	sier			8= •	0
★ Favoris	Bibliothèque Documents Indut : 2 emplacements		Organiser par :	Dossier 🔻	
Emplacements réce	Nom *	Modifié le	Туре	Taille	
Bibliothèques Documents Images Musique Vidéos	 Integration Services Script Component Integration Services Script Task Network Monitor 3 SQL Server Management Studio Visual Studio 2005 Visual Studio 2008 	26/11/2010 16:01 26/11/2010 16:00 15/06/2011 21:18 10/05/2012 18:24 26/11/2010 16:03 26/11/2010 15:55	Dossier de fichiers Dossier de fichiers Dossier de fichiers Dossier de fichiers Dossier de fichiers Dossier de fichiers		
📜 Ordinateur	export_exclu_kes10.dat	13/06/2013 21:52	Fichier DAT		11 Ko
Disque local (C:) data (E:) Nom du ficher : export Type : *.dat	<pre> </pre> t_exclu_kes10.dat				•
Cacher les dossiers			Enregistrer	Annuler	

Indiquer le nom du fichier d'export et cliquer sur "enregistrer".

Vous pouvez ensuite fermer la stratégie modèle.

Etape 3 : Import des exclusions depuis le modèle

Ouvrir la stratégie de paramétrage dans laquelle importer les règles d'exclusions.

			Guide de démarrage » Format
Stratégies Les stratégies sont utilisées pour configurer les para	nètres de protection et les paramètres généraux	les annihrations.	
🕂 Créer une stratégie	Sections	Paramètres généraux	
Créer une stratégie de Kaspersky Endpoint: Importer une stratégie à partir d'un fichier Actualiser	Général Evénements Endpoint Control Contrôle du lancement des applications Contrôle de l'activité des applications Surveillance des vulnérabilités	Paramètres généraux Jancer Kaspersky Endpoint Security 10 fo Appliquer la technologie de réparation de Objets à détecter Activation de la détection des objets d	or Windows au démarrage de l'ordinateur l'Infection active des types suivants :
+ Etat	Contrôle des périphériques	 virus, vers, chevaux de Troie et outis maive logiciels publicitaires, numéroteurs automatie 	eilants; iques;
persky Endpoint Security 8 for Windows	Filtrage de contenu	- fichiers compressés qui peuvent nuire, fichie	ers compressés à plusieurs reprises.
Formation Klab France Stratégie KES 8.1 Actif	Chiffrement	Configuration	
spersky Endpoint Security 10 for Windows Formation Klab France Stratégie KES 10 Actif	Paramètres généraux de chiffrement Chiffrement des disques durs Chiffrement des fichiers et des dossier Chiffrement des disques amovibles	Exclusions et zone de confiance Règles : 27 (total de 27) Applications de confiance : 21 (total de 23) Ports confiance : 21 (total de 23)	Configuratio
	Endpoint Protection Paramètres généraux Antivirus Fichiers	C Contrôler tous les ports réseau C Contrôler uniquement les ports sélectionn	nés <u>C</u> onfiguration
	Antivirus Courrier	-	
	Aide	1	OK Annuler Appliquer
		Endpoint Protection Paramètres généraux Antivirus Courrier	Chiffrement des disques amovibles Antivirus Fichiers Antivirus Internet
		Antivirus IM ("Chat")	Pare-feu

Cliquer sur **"Paramètres généraux**" puis sur le bouton **"Configuration**" de la section **"Exclusions et zone de confiance**".

Nota : on remarque ici que les exclusions (il n'y en a que 27 au total) sont manquantes.

🌠 Zone de confiance		
Règles d'exclusion Applications de confiance		
Les règles d'exclusion permettent de désigner les fichiers ou les dossiers et les Endpoint Security 10 for Windows ne réalise l'analyse pendant leur fonctionne	noms des objets dans le classement de l'Encyclopédie des virus ment.	qui sont distincts ou auucn des modules de Kaspersky
🕂 Ajouter 🖉 Modifier 💥 Supprimer		
Fichier ou dossier	Nom de l'objet	
♥ %ProgramFiles%\DANWARE DATA\NETOP REMOTE CONTROL\GUEST\	Invader (loader)	
✓ %ProgramFiles(x86)%/DANWARE DATA/NETOP REMOTE CONTROL/G	Invader (loader)	
✓ %ProgramFiles% \DANWARE DATA \NETOP REMOTE CONTROL \HOST \N	Invader (loader)	
✓ %ProgramFiles(x86)%\DANWARE DATA\WETOP REMOTE CONTROL\H	Invader (loader)	
✓ %ProgramFiles%\TIMBUKTU PRO\TB2PRO.EXE	Invader (loader)	
✓ %ProgramFiles(x86)%\TIMBUKTU PRO\TB2PRO.EXE	Invader (loader)	
✓ %ProgramFiles%\TIMBUKTU PRO\TB2START.EXE	Private data and naceworde accese	
🗹 %ProgramFiles(x86)%\TIMBUKTU PRO\TB2STAR 🔀 Zone de confian		
✓ %ProgramFiles%\TIMBUKTU PRO\TNOTIFY.EXE		
%ProgramFiles(x86)%\TIMBUKTU PRO\TNOTIFY	ez-vous siguitar las áláments importás suv áláments	
♥ %SystemRoot%\SYSTEM32\DWRCS.EXE	ts ? Pour supprimer les éléments existants, cliquez sur	
✓ %winDir%\SysWOW64\DWRCS.EXE "Non".		-
Description de la règle (diquez sur les éléments soulio		
	Ou Non Annuier	
	6	
		-
		Lunbortago Axportation
Aide		OK <u>E</u> ermer

Cliquer sur le bouton "**Importation**" puis cliquer sur le bouton "**Oui**" pour ajouter les exclusions aux existantes.

K Ouvrir le fichier			×
Bibliothèques - Documents -	- 🖽	Rechercher dans : Docum	nents 😥
Organiser 🔻 Nouveau dossier		8== •	• 🔳 🔞
E 🖈 Favoris	Bibliothèque Documents Inclut : 2 emplacements	Organiser par : Do	ossier 🔻
Emplacements recents	Nom +	Modifié le	Туре
- Telechargements	Integration Services Script Component	26/11/2010 16:01	Dossier de fi
🖃 🥽 Bibliothèques	Integration Services Script Task	26/11/2010 16:00	Dossier de fi
Documents	Network Monitor 3	15/06/2011 21:18	Dossier de fi
	SQL Server Management Studio	10/05/2012 18:24	Dossier de fi
	Visual Studio 2005	26/11/2010 16:03	Dossier de fi
1 videos	Visual Studio 2008	26/11/2010 15:55	Dossier de fi
🖃 🏴 Ordinateur	export_exclu_kes10.dat	22/07/2013 15:20	Fichier DAT
E 🏭 Disque local (C:)			
• 📻 data (E:)			
Ouveau nom (F:)	1		
	(<u> </u>		<u> </u>
Nom du fichier : export_	exclu_kes10.dat	*.dat	*
		Ouvrir	Annuler //

Sélectionner le fichier créé à l'étape 2 et cliquer sur 'Ouvrir''.

s rècles d'exclusion permettent de désigner les fichiers ou les do	ssiers et les noms des ob	ets dans le classement de l'Encyclopédie des virus qui sont dis	tincts ou autor des modules de Kaspersky
dpoint Security 10 for Windows ne réalise l'analyse pendant leu	r fonctionnement.		and a second race mound are needed any
🗣 Ajouter 🖉 Modifier 💥 Supprimer			
Fichier ou dossier		Nom de l'objet	
%SystemRoot%\Cluster*			
%QuorumDrive%/MSCS\			
%SystemRoot%/system32%CatRoot2%Domain.edb			
%SystemRoot%/system32%CatRoot2/tmp.edb			
%SystemRoot%\system32\CatRoot2\edb.chk			
%SystemRoot%\system32\CatRoot2\res1.log			
%SystemRoot%\system32\CatRoot2\res2.log			
%SystemRoot%IntfrsIjetIjog*.log	•		
%SystemRoot% intfrs jet jog jedbres0000?.jrs			
%SystemRoot%/ntfrs/jet/sys/edb.dhk			
%SystemRoot%IntfrsIjetIntfrs.jdb	•		
%SystemRoot%intdsitemp.edb			

Cliquer sur le bouton "**OK**" pour valider l'import.

🔜 Propriétés : Formation Klab France St	ratégie KES 10	_ 🗆 🗙
Sections	Paramètres généraux	
Général Evénements Endpoint Control Contrôle du lancement des applications Contrôle de l'activité des applications Surveillance des vulnérabilités Contrôle des périphériques Filtrage de contenu Chiffrement Paramètres généraux de chiffrement Chiffrement des disques durs Chiffrement des fichiers et des dossiers Chiffrement des fichiers et menvilles	 Paramètres généraux Lancer Kaspersky Endpoint Security 10 for Windows au démarrage de l'ordinateur Appliquer la technologie de réparation de l'infection active Objets à détecter Activation de la détection des objets des types suivants : virus, vers, chevaux de Troie et outils malveillants ; logiciels publicitaires, numéroteurs automatiques ; fichiers compressés qui peuvent nuire, fichiers compressés à plusieurs reprises. Configuration Exclusions et zone de confiance Règles : 189 (total de 189) Applications de confiance : 21 (total de 23) 	<u>C</u> onfiguration
Endpoint Protection Paramètres généraux Antivirus Fichiers Antivirus Courrier	Contrôler tous les ports réseau Contrôler uniquement les ports sélectionnés	<u>C</u> onfiguration
Aide		Appliquer

Cliquer sur le bouton "OK" pour enregistrer et fermer la stratégie.

Nota : on remarque que le nombre d'exclusions est passé de 27 à 189.