Kaspersky Endpoint Security 8 for Smartphone

Manuel de mise en place

VERSION DE L'APPLICATION : 8.0

Cher utilisateur,

Merci d'avoir choisi notre produit. Nous espérons que cette documentation vous sera utile dans votre travail et vous apportera toutes les réponses sur notre produit logiciel.

Date d'édition : 20 mai 11

http://www.kaspersky.com/fr
http://support.kaspersky.fr

TABLE DES MATIERES

A PROPOS DE CE MANUEL

Les experts de Kaspersky Lab vous souhaitent la bienvenue. Nous espérons que les informations présentées dans ce manuel, vous seront utiles dans votre travail avec Kaspersky Endpoint Security 8 for Smartphone.

Ce manuel est destiné aux administrateurs de réseaux d'entreprise. Il décrit les procédures d'installation et de configuration de l'application sur les appareils mobiles d'utilisateurs via les plates-formes suivantes :

- Kaspersky Administration Kit.
- Microsoft System Center Mobile Device Manager.
- Sybase Afaria.

Les informations sur l'utilisation de Kaspersky Anti-Virus sur les appareils mobiles avec différents systèmes d'exploitation sont présentées dans les Guides de l'utilisateur de Kaspersky Endpoint Security 8 for Smartphone pour chacun des systèmes d'exploitation.

Si vous ne trouvez pas une réponse à votre question sur Kaspersky Endpoint Security 8 for Smartphone dans ce manuel, vous pouvez consulter d'autres sources d'information (cf. la rubrique "Sources d'informations complémentaires" à la page 8).

DANS CETTE SECTION

DANS CE DOCUMENT

Ce document reprend les sections suivantes :

- *Sources d'informations complémentaires* (à la page 8). Cette section présente les informations sur les possibilités d'obtenir les informations sur le logiciel (en dehors des documents qui font partie du kit de distribution) ainsi que sur les modalités de contacter Kaspersky Lab en cas d'urgence.
- *Administration des licences (à la page 20).* Cette section présente des informations détaillées sur les notions clé liées à la gestion des licences de Kaspersky Endpoint Security 8 for Smartphone, ainsi que les informations sur l'installation et la suppression de la licence de Kaspersky Endpoint Security 8 for Smartphone pour les appareils mobiles d'utilisateurs.
- *Kaspersky Endpoint Security 8 for Smartphone* (à la page 10). Cette section décrit les fonctions clé de Kaspersky Endpoint Security 8 for Smartphone, les différences de Kaspersky Endpoint Security 8 for Smartphone par rapport à sa version précédente et la configuration matérielle et logicielle des appareils mobiles et du système de gestion administrative.
- *Présentation des composants de Kaspersky Endpoint Security 8 for Smartphone* à la page 14). Cette section décrit l'affectation de chacun des composants, son algorithme de fonctionnement et les systèmes d'exploitation qui prennent en charge ce composant et les fonctions qu'il assure.
- *Déploiement de l'application via Kaspersky Administration Kit* (à la page 23). Cette section décrit la procédure de déploiement de Kaspersky Endpoint Security 8 for Smartphone via Kaspersky Administration Kit.
- *Déploiement de l'application via MS SCMDM* (à la page 77). Cette section décrit la procédure de déploiement de Kaspersky Endpoint Security 8 for Smartphone via Mobile Device Manager.
- *Déploiement de l'application via Sybase Afaria* (à la page 116). Cette section décrit la procédure de déploiement de Kaspersky Endpoint Security 8 for Smartphone via Sybase Afaria.
- *Contacter le service du Support Technique*. La section décrit les règles des appels au service du Support Technique.
- *Glossaire*. La section reprend les termes utilisés dans ce manuel.
- *Kaspersky Lab* (à la page 147). Cette section présente la société Kaspersky Lab.

- *Informations sur l'utilisation de code tiers*. La section reprend les informations relatives au code tiers utilisé dans l'application.
- *Index*. Cette section vous aidera à trouver rapidement les informations nécessaires dans le document.

CONVENTIONS

Les conventions décrites dans le tableau ci-dessous sont utilisées dans le manuel.

Таблица 1. Conventions

EXEMPLE DE TEXTE	DESCRIPTION DE LA CONVENTION
N'oubliez pas que ...	Les avertissements apparaissent en rouge et sont encadrés. Les avertissements contiennent des informations importantes, par exemple, les informations liées aux actions critiques pour la sécurité de l'ordinateur.
Il est conseillé d'utiliser...	Les remarques sont encadrées. Les remarques fournissent des conseils et des informations d'assistance.
Exemple : ...	Les exemples sont présentés sur un fond jaune sous le titre "Exemple".
La *mise à jour*, c'est ...	Les nouveaux termes sont en italique.
ALT+F4	Les noms des touches du clavier sont en caractères mi-gras et en lettres majuscules. Deux noms de touche unis par le caractère "+" représentent une combinaison de touches.
Activer	Les noms des éléments de l'interface sont en caractères mi-gras : les champs de saisie, les commandes du menu, les boutons.
➧ *Pour planifier une tâche, procédez comme suit :*	Les instructions sont indiquées à l'aide d'une flèche. Les phrases d'introduction sont en italique.
`help`	Les textes dans la ligne de commande ou les textes des messages affichés sur l'écran par l'application sont en caractères spéciaux.
<adresse IP de votre ordinateur>	Les variables sont écrites entre chevrons. La valeur correspondant à la variable remplace cette variable à chaque fois. Par ailleurs, les parenthèses angulaires sont omises.

SOURCES D'INFORMATIONS COMPLEMENTAIRES

Pour toute question sur le choix, l'achat, l'installation ou l'utilisation de Kaspersky Endpoint Security 8 for Smartphone, vous pouvez rapidement trouver des réponses en utilisant plusieurs sources d'information. Vous pouvez sélectionner celle qui vous convient le mieux en fonction de l'importance et de l'urgence du problème.

DANS CETTE SECTION

SOURCES DE DONNEES POUR DES CONSULTATIONS INDEPENDANTES

Vous disposez des informations suivantes sur l'application :

- page de l'application sur le site de Kaspersky Lab ;
- page de l'application sur le site du serveur du Support technique (Base de connaissances) ;
- système d'aide en ligne ;
- documentation.

Page sur le site de Kaspersky Lab

http://www.kaspersky.com/fr/endpoint-security-smartphone

Utilisez cette page pour obtenir des informations générales sur Kaspersky Endpoint Security 8 for Smartphone, ses possibilités et ses caractéristiques de fonctionnement. Vous pouvez acheter Kaspersky Endpoint Security 8 for Smartphone ou renouveler la licence d'utilisation dans notre boutique en ligne.

Page de l'application sur le serveur du Support technique (Base de connaissances)

http://support.kaspersky.com/fr/kes8m

Cette page contient des articles publiés par les experts du Service d'assistance technique.

Ils contiennent des informations utiles, des recommandations et des réponses aux questions fréquemment posées sur l'acquisition, l'installation et l'utilisation de Kaspersky Endpoint Security 8 for Smartphone. Ces questions sont regroupées par sujet, par exemple " Utilisation des fichiers de licence ", " Mise à jour des bases " ou " Résolution des problèmes ". Les articles répondent non seulement à des questions sur Kaspersky Endpoint Security 8 for Smartphone, mais aussi sur d'autres produits Kaspersky Lab ; ils peuvent contenir des informations générales récentes du Service d'assistance technique.

Système d'aide en ligne

Le système d'aide en ligne de Kaspersky Endpoint Security 8 for Smartphone comprend l'aide contextuelle pour le plug-in de gestion de l'application via Kaspersky Administration Kit et aides contextuelles pour les appareils mobiles d'utilisateurs tournant sous les systèmes d'exploitation suivants :

- Microsoft Windows® Mobile.
- Symbian.
- BlackBerry®.
- Android™.

- L'aide contextuelle contient les informations sur les fenêtres / les onglets spécifiques de l'application.
- Documentation
- La documentation de Kaspersky Endpoint Security 8 for Smartphone contient la majeure partie d'informations nécessaires pour assurer son fonctionnement. Il s'agit des documents suivants:
  - **Guide de l'utilisateur**. Les guides de l'utilisateur pour l'application installée sur appareils mobiles tournant sous Windows Mobile, Symbian BlackBerry et Android. Chaque guide de l'utilisateur contient les informations qui aident l'utilisateur à installer, à configurer et à activer l'application sur l'appareil mobile.
  - **Manuel de mise en place**. Le manuel de mise en place permet à l'administrateur d'installer et de configurer l'application sur les appareils mobiles d'utilisateurs via les plates-formes suivantes :
    - Kaspersky Administration Kit.
    - Microsoft System Center Mobile Device Manager.
    - Sybase Afaria.

DISCUSSION SUR LES APPLICATIONS DE KASPERSKY LAB DANS LE FORUM

Si votre question n'est pas urgente, vous pouvez en discuter avec les experts de Kaspersky Lab et d'autres utilisateurs dans notre forum à l'adresse http://forum.kaspersky.com/index.php?showforum=5.

Le forum permet de lire les conversations existantes, d'ajouter des commentaires, de créer de nouvelles rubriques et il dispose d'une fonction de recherche.

CONTACTER L'ÉQUIPE DE REDACTION DE LA DOCUMENTATION POUR LES UTILISATEURS

Si vous avez des questions concernant la documentation, si vous y avez trouvé une erreur ou si vous voulez envoyer un commentaire sur nos documents, vous pouvez contacter les spécialistes du Groupe de rédaction de la documentation pour les utilisateurs. Pour contacter l'Équipe de rédaction de la documentation, envoyez un message à docfeedback@kaspersky.com. L'objet du message devra être " Kaspersky Help Feedback: Kaspersky Endpoint Security 8 for Smartphone ".

KASPERSKY ENDPOINT SECURITY 8 FOR SMARTPHONE

Kaspersky Endpoint Security 8 for Smartphone protège les appareils mobiles tournant sous Symbian, Microsoft Windows Mobile, BlackBerry et Android contre les menaces connues et nouvelles ainsi que contre les appels et les SMS indésirables. L'application contrôle les SMS envoyés et l'activité de réseau et protège les données confidentielles contre l'accès non autorisé. Chaque type de menace est traité par un composant distinct de l'application. Cela permet de configurer en souplesse les paramètres de l'application en fonction des besoins d'un utilisateur particulier.

Kaspersky Endpoint Security 8 for Smartphone prend en charge les systèmes d'administration distante Kaspersky Administration Kit, MS SCMDM et Sybase Afaria. Ces systèmes permettent à l'administrateur d'effectuer à distance ce qui suit :

- installer l'application sur les appareils mobiles ;
- supprimer l'application des appareils par MS SCMDM ;
- configurer les paramètres de fonctionnement de l'application pour plusieurs appareils en même temps ou pour chacun des appareils ;
- produire des rapports sur le fonctionnement des composants de l'application installée sur les appareils mobiles via Kaspersky Administration Kit.

Kaspersky Endpoint Security 8 for Smartphone reprend les composants de protection suivants :

- **Protection**. Protège le système de fichiers de l'appareil mobile contre l'infection. Le composant Protection est lancée au démarrage du système d'exploitation, est chargée en permanence dans la mémoire vive de l'appareil et analyse tous les fichiers ouverts, enregistrés et exécutés, y compris sur la carte mémoire. De plus, la Protection recherche la présence éventuelle de virus connus dans tous les fichiers entrants. Il sera possible d'utiliser le fichier uniquement si l'objet est simple ou s'il a pu être réparé.
- **Analyse de l'appareil**. Aide à identifier et à neutraliser les objets malveillants sur l'appareil mobile. Il faut réaliser l'analyse de l'appareil à intervalles réguliers afin d'éviter la propagation d'objets malveillants qui n'auraient pas été découverts par la Protection.
- **Anti-Spam**. Analyse tous les SMS et appels entrants à la recherche de spam. Le composant peut bloquer tous les SMS et appels qu'il considère comme indésirables. Les appels et les SMS sont filtrés sur la base de listes noire et/ou blanche de numéros. Tous les SMS et les appels en provenance des numéros de la liste noire sont bloqués. Les SMS et les appels en provenance des numéros de la liste blanche sont toujours acceptés par l'appareil mobile. Le composant permet également de configurer la réponse de l'application aux SMS en provenance de numéros sans chiffres, ainsi qu'aux appels et aux SMS en provenance des numéros qui ne figurent pas dans les Contacts.
- **Antivol** Protège les données de l'appareil contre l'accès non autorisé en cas de perte ou de vol. Le composant permet de verrouiller l'appareil à distance en cas de perte ou de vol, de supprimer les données confidentielles et de contrôler le remplacement de la carte SIM. Il permet également de définir les coordonnées géographiques de l'appareil (si celui-ci est doté d'un récepteur GPS).
- **Contacts personnels**. Dissimule les informations confidentielles de l'utilisateur pendant que l'appareil est utilisé par d'autres personnes. Le composant permet d'afficher ou de masquer toutes les informations liées aux numéros désignés, par exemple les données de la liste de contacts, les échanges de SMS et les entrées du journal des appels. Le composant permet également de dissimuler la réception des appels et de SMS entrants en provenance de numéros sélectionnés.
- **Pare-feu**. Contrôle les connexions de réseau de votre appareil mobile. Le composant permet de définir les connexions autorisées ou interdites.
- **Chiffrement**. Protège les informations que la consultation par des tiers, même s'ils ont accès à l'appareil. Le composant peut chiffrer un nombre indéfini de dossiers non système enregistrés dans la mémoire de l'appareil ou sur les cartes mémoire. Les données du dossier sont accessibles uniquement après la saisie d'un code secret.

De plus, l'application propose les fonctions de service suivantes. Elles permettent de maintenir l'actualité de l'application, d'élargir les possibilités de celle-ci et de venir en aide à l'utilisateur durant l'utilisation.

- Mise à jour des bases du programme. Cette fonction permet de maintenir les bases antivirus de Kaspersky Endpoint Security 8 for Smartphone à jour. L'utilisateur de l'appareil peut lancer la mise à jour à la main ou programmer la mise à jour avec une fréquence définie dans les paramètres de l'application.

- État de la protection. Les états des composants de l'application sont affichés. En fonction des informations reçues, l'utilisateur peut évaluer l'état actuel de protection de son appareil.
- Journal des événements. Les informations sur le fonctionnement de chacun des composants (par exemple, opération effectuée, détails sur un objet bloqué, rapport d'analyse, mise à jour) sont consignées dans un journal d'événements spécifique.
- Licence. Lors de l'achat de Kaspersky Endpoint Security 8 for Smartphone votre société passe avec Kaspersky Lab un contrat de licence qui donne le droit aux employés de la société d'utiliser l'application, de recevoir les mises à jour des bases de l'application et de contacter le service d'assistance technique durant une période déterminée. La durée d'utilisation ainsi que toute autre information requise pour le fonctionnement complet de l'application figurent dans la licence.

Kaspersky Endpoint Security 8 for Smartphone ne réalise pas de copies de sauvegarde des données en vue d'une restauration ultérieure.

DANS CETTE SECTION

NOUVEAUTES

Les différences entre Kaspersky Endpoint Security 8 for Smartphone et la version précédente de l'application sont les suivantes :

- Prise en charge de nouvelles plates-formes : Sybase Afaria et Microsoft System Center Mobile Device Manager (MS SCMDM).
- Installation de l'application sur les appareils par une diffusion des messages électroniques.
- L'accès au programme est régi par un mot de passe.
- La liste des fichiers exécutables analysés par l'application en cas de limitation des types de fichiers analysés par les composants Protection et Analyser est enrichie. L'application analyse uniquement les fichiers exécutables des applications aux formats suivants : EXE, DLL, MDL, APP, RDL, PRT, PXT, LDD, PDD, CLASS. Si la fonction de l'analyse des archives est activée, l'application décompresse et analyse les archives des formats suivants : ZIP, JAR, JAD, SIS, SISX, RAR и CAB.
- Pour les contacts confidentiels, le composant Contacts personnels permet de masquer les informations suivantes : entrées dans les Contacts, correspondance SMS, journal des appels, SMS reçus et appels entrants. Les informations confidentielles sont accessibles si la fonction de dissimulation est désactivée.
- Le composant Chiffrement permet de chiffrer les dossiers enregistrés dans la mémoire de l'appareil ou sur une carte mémoire. Le composant stocke les informations confidentielles en mode crypté et ne permet d'accéder aux informations chiffrées qu'après avoir saisi le code secret de l'application.
- La version actualisée de l'Antide l'Antivol propose la fonction de Géolocalisation qui permet de recevoir les coordonnées géographiques de l'appareil au numéro de téléphone ou à l'adresse de la messagerie électronique définie en cas de perte ou de vol. De plus, Antivol propose une version actualisée de la fonction de Suppression qui permet de supprimer à distance non seulement les données personnelles de l'utilisateur, stockées dans la mémoire de l'appareil ou sur la carte mémoire, mais aussi les fichiers de la liste des dossiers à supprimer que vous avez créée.
- Pour réduire le trafic, l'application propose une nouvelle fonctionnalité qui permet de désactiver automatiquement la mise à jour des bases de l'application en itinérance.
- L'application propose également une nouvelle fonction de service Affichage des astuces : Kaspersky Endpoint Security 8 for Smartphone affiche une brève description du composant avant la configuration de ses paramètres.
- L'application est compatible avec les appareils tournant sous Android.

DISTRIBUTION

Vous pouvez acheter Kaspersky Endpoint Security 8 for Smartphone chez les revendeurs ou dans une des boutiques en ligne (par exemple, http://www.kaspersky.ru, rubrique **Magasin en ligne**). De plus, Kaspersky Endpoint Security 8 for Smartphone fait partie de la distribution de tous les produits de la gamme Kaspersky Open Space Security.

Lors de l'achat de Kaspersky Endpoint Security 8 for Smartphone dans un magasin en ligne vous passez une commande et recevez après le règlement une lettre d'information à votre adresse électronique avec le fichier de licence pour activer l'application et le lien pour télécharger la distribution de l'application. Pour en savoir plus sur les modalités d'achat et le kit de distribution, contactez notre Département commercial à l'adresse info@kaspersky.fr.

Si votre société utilise Kaspersky Administration Kit pour le déploiement de Kaspersky Endpoint Security 8 for Smartphone, la distribution de l'application contient une archive auto-extractible KES8_forAdminKit_fr.exe avec des fichiers suivants qui assurent l'installation de l'application sur les appareils mobiles :

- klcfginst.exe : fichier d'installation du plug-in de gestion de Kaspersky Endpoint Security 8 for Smartphone via Kaspersky Administration Kit ;
- endpoint_8_0_x_xx_fr.cab : fichier d'installation de l'application pour le système d'exploitation Microsoft Windows Mobile ;
- endpoint8_mobile_8_x_xx_eu4_signed.sis : fichier d'installation de l'application pour le système d'exploitation Symbian ;
- Endpoint8_Mobile_8_x_xx_fr_release.zip : fichier d'installation de l'application pour le système d'exploitation BlackBerry ;
- Endpoint8_8_x_xx_release.apk : fichier d'installation de l'application pour Android ;
- AdbWinUsbApi.dll, AdbWinApi.dll, adb.exe : ensemble de fichiers indispensable à l'installation de l'application sur les appareils Android ;
- installer.ini : fichier de configuration avec des paramètres de connexion au Serveur d'administration ;
- kmlisten.ini : fichier de configuration avec des paramètres de l'utilitaire de transmission du paquet d'installation ;
- kmlisten.kpd : fichier avec la description de l'application ;
- kmlisten.exe : utilitaire de transmission du paquet d'installation sur l'appareil mobile depuis le poste de travail ;
- Documentation
  - Manuel de mise en place de Kaspersky Endpoint Security 8 for Smartphone ;
  - Guide de l'utilisateur de Kaspersky Endpoint Security 8 for Smartphone pour Microsoft Windows Mobile ;
  - Guide de l'utilisateur de Kaspersky Endpoint Security 8 for Smartphone pour Symbian ;
  - Guide de l'utilisateur de Kaspersky Endpoint Security 8 for Smartphone pour BlackBerry ;
  - Guide de l'utilisateur de Kaspersky Endpoint Security 8 for Smartphone pour Android ;
  - L'aide contextuelle du plug-in de gestion de Kaspersky Endpoint Security 8 for Smartphone ;
  - L'aide contextuelle de l'application pour Microsoft Windows Mobile ;
  - L'aide contextuelle de l'application pour Symbian ;
  - L'aide contextuelle de l'application pour BlackBerry ;
  - L'aide contextuelle de l'application pour Android.

Si votre société utilise Mobile Device Manager pour le déploiement de Kaspersky Endpoint Security 8 for Smartphone, la distribution de l'application contient une archive auto-extractible KES8_forMicrosoftMDM_fr.exe avec des fichiers suivants qui assurent l'installation de l'application sur les appareils mobiles :

- endpoint_MDM_Afaria_8_0_x_xx_fr.cab : fichier d'installation de l'application pour le système d'exploitation Microsoft Windows Mobile ;
- endpoint8_fr.adm : fichier du modèle d'administration avec les paramètres des stratégies pour les gérer ;
- endpoint8_ca.cer : fichier de certification du centre de certification ;
- endpoint8_cert.cer : fichier de certification qui sert de signature pour le fichier d'installation de l'application ;
- kes2mdm.exe : utilitaire pour convertir le fichier de licence de l'application ;

- kl.pbv, licensing.dll, oper.pbv : ensemble de fichiers qui assurent le fonctionnement de l'utilitaire kes2mdm.exe ;
- Documentation
  - Manuel de mise en place de Kaspersky Endpoint Security 8 for Smartphone ;
  - Guide de l'utilisateur de Kaspersky Endpoint Security 8 for Smartphone pour Microsoft Windows Mobile ;
  - L'aide contextuelle de l'application pour Microsoft Windows Mobile.

Si votre société utilise Sybase Afaria pour le déploiement de Kaspersky Endpoint Security 8 for Smartphone, la distribution de l'application contient une archive auto-extractible KES8_forSybaseAfaria_fr.exe avec des fichiers suivants qui assurent l'installation de l'application sur les appareils mobiles :

- endpoint_MDM_Afaria_8_0_x_xx_fr.cab : fichier d'installation de l'application pour le système d'exploitation Microsoft Windows Mobile ;
- endpoint8_mobile_8_x_xx_eu4.sisx : fichier d'installation de l'application pour le système d'exploitation Symbian ;
- Endpoint8_Mobile_Installer.cod : fichier d'installation de l'application pour le système d'exploitation BlackBerry ;
- KES2Afaria.exe : utilitaire de gestion de la stratégie pour l'application Kaspersky Endpoint Security 8 for Smartphone ;
- kl.pbv, licensing.dll, oper.pbv : ensemble des fichiers qui font partie de l'utilitaire KES2Afaria.exe et assurent son fonctionnement ;
- Documentation
  - Manuel de mise en place de Kaspersky Endpoint Security 8 for Smartphone ;
  - Guide de l'utilisateur de Kaspersky Endpoint Security 8 for Smartphone pour Microsoft Windows Mobile ;
  - Guide de l'utilisateur de Kaspersky Endpoint Security 8 for Smartphone pour Symbian ;
  - Guide de l'utilisateur de Kaspersky Endpoint Security 8 for Smartphone pour BlackBerry ;
  - L'aide contextuelle du plug-in de gestion de Kaspersky Endpoint Security 8 for Smartphone ;
  - L'aide contextuelle de l'application pour Microsoft Windows Mobile ;
  - L'aide contextuelle de l'application pour Symbian ;
  - L'aide contextuelle de l'application pour BlackBerry.

CONFIGURATION LOGICIELLE ET MATERIELLE

Pour assurer un bon fonctionnement de Kaspersky Endpoint Security 8 for Smartphone, les appareils mobiles d'utilisateurs doivent satisfaire aux spécifications suivantes.

Configuration matérielle :

- Symbian OS 9.1, 9.2, 9.3, 9.4 Series 60® UI, Symbian^3 (uniquement pour les appareils mobiles Nokia®).
- Windows Mobile 5,0, 6,0, 6,1, 6,5.
- BlackBerry 4.5, 4.6, 4.7, 5.0, 6.0.
- Android 1.5, 1.6, 2.0, 2.1, 2.2, 2.3.

Pour assurer le déploiement de Kaspersky Endpoint Security 8 for Smartphone dans le réseau, le système d'administration distante doit satisfaire aux spécifications suivantes :

Configuration logicielle :

- Kaspersky Administration Kit 8.0 Critical Fix 2.
- Mobile Device Manager Software Distribution Microsoft Corporation Version : 1.0.4050.0000 (SP).
- System Center Mobile Device Manager Microsoft Corporation Version : 1.0.4050.0000.
- Sybase Afaria 6.50.4607.0.

PRESENTATION DES COMPOSANTS DE KASPERSKY ENDPOINT SECURITY 8 FOR SMARTPHONE

Kaspersky Endpoint Security 8 for Smartphone comprend les composants suivants :

- Anti-Virus Fichier (à la page 14).
- Antivol (à la page 16).
- Contacts personnels (à la page 17).
- Anti-Spam (à la page 17).
- Pare-feu (à la page 18).
- Chiffrement (à la page 18).

Cette section décrit l'affectation de chacun des composants, son algorithme de fonctionnement et les systèmes d'exploitation qui prennent en charge ce composant et les fonctions qu'il assure.

DANS CETTE SECTION

ANTI-VIRUS FICHIER

Le composant Anti-Virus Fichier assure une protection des appareils mobiles contre les virus. Il propose les fonctions suivantes : Protection (à la page 14), Analyse à la demande (à la page 15), Mise à jour (à la page 16).

DANS CETTE SECTION

PROTECTION

Le composant Protection analyse tous les processus exécutés dans le système de fichiers, surveille les événements qui se produisent sur l'appareil, analyse tous les fichiers neufs, ouverts ou modifiés (y compris ceux qui se trouvent sur une carte mémoire) ainsi que toutes les applications afin de détecter la présence éventuelle d'un code malveillant juste avant que l'utilisateur ne les sollicite.

La Protection utilise l'algorithme de fonctionnement suivant :

1. La Protection est lancée au démarrage du système d'exploitation.

2. La Protection analyse les fichiers du type sélectionné lorsque l'utilisateur essaie de les accéder. La Protection est effectuée à l'aide des bases antivirus de l'application.
3. Selon les résultats de l'analyse, la Protection exécute l'action en fonction du système d'exploitation.

   Pour les systèmes d'exploitation Symbian et Microsoft Windows Mobile, le composant Protection peut adopter les comportements suivants :

   - quand du code malveillant est découvert dans le fichier, la Protection le bloque, agit conformément aux paramètres définis, notifie l'utilisateur sur la détection d'un objet malveillant et consigne l'information dans le journal d'événements ;
   - si aucun code malveillant n'est découvert, le fichier est immédiatement restitué.

   Sous Android, le composant Protection peut adopter les comportements suivants :

   - quand du code malveillant est découvert dans le fichier, la protection agit conformément aux paramètres définis ;
   - si aucun code malveillant n'est découvert, le fichier est immédiatement restitué.
4. Le composant Protection consigne les événements et les actions de l'utilisateur dans un journal d'événements (pour Symbian et Microsoft Windows Mobile).

   Les rapports sur les événements et les actions de l'utilisateur ne sont pas proposés dans Kaspersky Endpoint Security 8 for Smartphone pour le système d'exploitation Android.

La Protection n'est pas prise en charge par le système d'exploitation BlackBerry.

ANALYSE A LA DEMANDE

L'analyse à la demande assure la recherche d'objets malveillants dans le système de fichiers des appareils mobiles. Kaspersky Endpoint Security 8 for Smartphone permet de réaliser une analyse complète du système de fichiers ou une analyse partielle de l'appareil. Autrement dit, il peut analyser uniquement le contenu de la mémoire intégrée de l'appareil ou un dossier spécifique (y compris les dossiers stockés sur la carte mémoire). L'analyse complète peut être lancée à la main automatiquement selon un horaire défini. L'analyse partielle ne peut être lancée qu'en mode manuel par l'utilisateur directement depuis l'application installée sur l'appareil mobile.

L'analyse de l'appareil s'opère selon l'algorithme suivant :

1. Kaspersky Endpoint Security 8 for Smartphone analyse les fichiers du type sélectionné définis dans les paramètres de vérification.
2. Pendant la vérification, Kaspersky Endpoint Security 8 for Smartphone analyse le fichier pour détecter des objets malveillants éventuels. Les objets malveillants sont détectés en les comparants aux bases antivirus utilisées par le logiciel.
3. Selon les résultats de l'analyse, l'application exécute une action en fonction du système d'exploitation.

   Sous les systèmes d'exploitation Symbian et Microsoft Windows Mobile, Kaspersky Endpoint Security 8 for Smartphone peut adopter un des comportements suivants :

   - Lorsqu'un code malveillant est découvert dans un fichier, Kaspersky Endpoint Security 8 for Smartphone bloque le fichier, exécute l'action sélectionnée conformément aux paramètres définis et notifie l'utilisateur.

     Sous Android, si l'analyse d'un fichier met en évidence un code malveillant, l'application exécute l'action sélectionnée en fonction des paramètres configurés.
   - Si aucun code malveillant n'est découvert, le fichier peut être directement manipulé.
4. Les informations relatives au déroulement de l'analyse et aux événements sont consignées dans le journal d'événements (pour les systèmes d'exploitation Symbian et Microsoft Windows Mobile).

   Kaspersky Endpoint Security 8 for Smartphone pour Android ne propose pas de rapports sur l'analyse.

Analyse à la demande n'est pas prise en charge par le système d'exploitation BlackBerry.

Les paramètres définis par l'administrateur via le système d'administration distante sont utilisés pour l'analyse complète ou partielle de l'appareil.

De plus, l'administrateur peut configurer le lancement automatique de l'analyse complète programmée de l'appareil. Le lancement de l'analyse partielle via le système d'administration distante n'est pas prévu.

MISES A JOUR

La Protection et l'Analyse à la demande fonctionnent avec les bases antivirus qui contiennent une description de toutes les applications malveillantes connues à ce jour et des moyens de les neutraliser, ainsi que des descriptions d'autres objets indésirables. Il est extrêmement important d'assurer la mise à jour des bases antivirus. La mise à jour peut être lancée à la main ou automatiquement selon un horaire défini. Pour assurer la fiabilité du système de protection anti-virus, il faut mettre les bases antivirus à jour régulièrement.

La mise à jour des bases antivirus de l'application s'opère selon l'algorithme suivant :

1. L'application établit la connexion à Internet ou utilise la connexion existante.
2. Les bases antivirus de l'application installées sur votre appareil sont comparées aux bases disponibles sur un serveur de mise à jour défini.
3. Kaspersky Endpoint Security 8 for Smartphone exécute une des opérations suivantes :
   - Si les bases de l'application installées sur l'appareil sont à jour, la mise à jour sera annulée. L'application notifie l'utilisateur sur l'état de la mise à jour des bases antivirus.
   - Si les bases installées sont différentes, un nouveau paquet de mises à jour sera téléchargé et installé sur l'appareil.

     Une fois la mise à jour terminée, la connexion est automatiquement coupée. Si la connexion était déjà établie avant la mise à jour, elle reste alors disponible pour d'autres opérations.
4. Les informations sur la mise à jour sont consignées dans le journal d'évènement.

La mise à jour n'est pas prise en charge par le système d'exploitation BlackBerry.

ANTIVOL

Antivol protège les informations stockées sur l'appareil mobile contre l'accès non autorisé.

Antivol dispose des fonctions suivantes :

- Verrouillage (à la page 16).
- Suppression (à la page 17).
- SIM-Surveillance (à la page 17).
- Géolocalisation (à la page 17).

Kaspersky Endpoint Security 8 for Smartphone permet à l'utilisateur de lancer à distance les fonctions Antivol via l'envoi d'une instruction SMS depuis un autre appareil mobile. L'instruction SMS est envoyée sous forme d'un SMS crypté qui contient le code secret de l'application, installée sur l'autre appareil l'appareil destinataire de l'instruction. La réception de l'instruction passera inaperçue sur l'appareil destinataire de l'instruction SMS. Le coût du SMS envoyé est celui de l'opérateur de téléphonie mobile de l'autre appareil mobile.

Antivol est pris en charge par tous les systèmes d'exploitation.

DANS CETTE SECTION

VERROUILLAGE

La fonction Verrouillage permet de verrouiller l'appareil à distance et de définir le texte qui apparaîtra à l'écran de l'appareil bloqué.

SUPPRESSION

La fonction Suppression permet de supprimer à distance les données personnelles de l'utilisateur stockées sur l'appareil (entrées des Contacts, SMS, galerie, calendrier, journaux, paramètres de connexion à Internet), ainsi que les informations sur les cartes mémoire et dans les dossiers à supprimer sélectionnés par l'administrateur et l'utilisateur. L'utilisateur ne pourra pas restaurer ces données !

L'administrateur peut définir les dossiers à supprimer dans la stratégie. L'administrateur peut sélectionner des dossiers qui se trouvent sur la carte mémoire ou dans la mémoire de l'appareil. S'agissant des appareils tournant sous Android, l'administrateur peut sélectionner des dossiers à supprimer qui se trouvent uniquement sur la carte mémoire. La sélection de dossiers dans la mémoire de l'appareil n'est pas possible.

L'utilisateur ne peut pas annuler la suppression des dossiers définis par l'administrateur. Il peut cependant spécifier les dossiers à supprimer sur son appareil mobile via l'interface locale de l'application (voir le Guide de l'utilisateur pour le système d'exploitation correspondant). Si l'administrateur n'a pas défini les dossiers à supprimer, l'application ne supprimera que les dossiers spécifiés par l'utilisateur.

SIM-SURVEILLANCE

La fonction SIM-Surveillance permet de garder le numéro de téléphone en cas de remplacement de la carte SIM et de verrouiller l'appareil en cas de remplacement de la carte SIM ou de mise sous tension de l'appareil sans cette carte. Le message avec le nouveau numéro de téléphone est envoyé vers le numéro de téléphone et / ou l'adresse de la messagerie électronique que vous avez spécifiés. De plus, SIM-Surveillance permet de verrouiller l'appareil en cas de remplacement de la carte SIM ou si l'appareil est allumé sans carte.

GEOLOCALISATION

La fonction Géolocalisation permet de déterminer les coordonnées de l'appareil. Le message avec les coordonnées géographiques de l'appareil est envoyé au numéro de téléphone qui a émis l'instruction SMS spéciale, ainsi qu'à l'adresse de la messagerie électronique.

En fonction du système d'exploitation, l'algorithme de fonctionnement de la Géolocalisation est le suivant :

- Sous Symbian, Microsoft Windows Mobile et BlackBerry, la fonction est opérationnelle uniquement sur les appareils dotés d'un récepteur GPS. Le récepteur GPS est activé automatiquement après la réception de l'instruction SMS spéciale. Si l'appareil se trouve dans une zone couverte par satellite, la fonction Géolocalisation reçoit et envoie les coordonnées de l'appareil. Au cas où les satellites ne seraient pas disponibles au moment de la requête, des tentatives pour les trouver sont lancées par la Géolocalisation à intervalles réguliers.
- Sous Android, si les appareils sont dotés d'un récepteur GPS, il est activé automatiquement à la réception d'une instruction SMS spéciale. Si la fonction Localisation ne peut pas recevoir les coordonnées de l'appareil à l'aide de GPS, elle définit les coordonnées approximatives de l'appareil selon les stations de base.

CONTACTS PERSONNELS

Les Contacts personnels dissimulent les informations confidentielles sur la base de la Liste de contacts créée qui reprend les numéros confidentiels. Les Contacts personnels masquent les entrées dans les Contacts, les SMS entrants, sortants et brouillons, ainsi que les enregistrements dans le journal des appels pour des numéros confidentiels. Les Contacts personnels bloquent le signal de réception du SMS et le masquent dans la liste des SMS reçus. Les Contacts personnels interdisent les appels entrants d'un numéro confidentiel et l'écran n'indiquera rien au sujet de ces appels. Dans ce cas, la personne qui appelle entendra la tonalité "occupé". Il faut désactiver la dissimulation des informations confidentielles pour pouvoir consulter les appels et les SMS entrants pour la période d'activation de cette fonction. A la réactivation de la dissimulation les informations ne seront pas affichées.

La fonction Contacts personnels n'est pas prise en charge par le système d'exploitation BlackBerry.

ANTI-SPAM

Anti-Spam empêche la réception d'appels et de SMS non sollicités sur la base des listes noire et blanche créées par l'utilisateur.

Les listes contiennent les enregistrements. L'enregistrement dans chaque liste contient les informations suivantes :

- Numéro de téléphone que l'Antique l'Anti-Spam refuse pour la liste noire et accepte pour la liste blanche.
- Type d'événement que l'Antique l'Anti-Spam refuse pour la liste noire et accepte pour la liste blanche. Types d'informations représentés : appels et SMS, appels seuls, SMS seuls.
- Expression clé qui permet à Anti-Spam d'identifier si les SMS sont sollicités ou non. S'il s'agit de la liste noire, Anti-Spam va refuser les SMS avec cette expression clé et accepter les autres SMS sans cette expression clé. S'il s'agit des numéros de la liste blanche, Anti-Spam va accepter les SMS avec cette expression clé et refuser les SMS sans cette expression clé.

Anti-Spam filtre les SMS et les appels entrants selon le mode sélectionné par l'utilisateur. Les modes de fonctionnement Anti-Spam disponibles :

- **Désactivé** : accepte tous les appels et les SMS entrants.
- **Liste noire** : accepte tous les appels et les SMS, sauf ceux qui proviennent des numéros de la liste noire.
- **Liste blanche** : accepte uniquement les appels et les SMS en provenance des numéros de la liste blanche.
- **Les deux listes** : accepte les appels et les SMS en provenance des numéros de la liste blanche et interdit ceux qui proviennent des numéros de la liste noire. Après la conversation ou la réception d'un SMS en provenance du numéro qui ne figure sur aucune des listes, Anti-Spam invitera l'utilisateur à ajouter ce numéro sur une des listes.

Anti-Spam analyse, sur la base du régime, chaque SMS ou appel entrant et détermine si ce SMS ou cet appel est sollicité ou non. L'analyse se termine dès que l'Antique l'Anti-Spam a attribué l'état de sollicité ou non au SMS ou à l'appel.

L'information sur les SMS et les appels refusés est consignée dans le journal d'événement.

Anti-Spam est pris en charge par tous les systèmes d'exploitation.

PARE-FEU

Le Pare-feu contrôle les connexions de réseau sur l'appareil selon le mode sélectionné. Les modes de fonctionnement Pare-feu disponibles :

- **Désactivé** : autorisation de la moindre activité de réseau.
- **Protection minimum** : bloque uniquement les connexions entrantes. Les connexions sortantes sont autorisées.
- **Protection maximum** : bloque toutes les connexions entrantes. L'utilisateur peut recevoir les messages électroniques, surfer sur le Web et télécharger les fichiers. Les connexions sortantes peuvent être réalisées uniquement via les ports SSH, HTTP, IMAP, SMTP, POP3.
- **Tout bloquer** : bloque toute activité de réseau, sauf la mise à jour des bases antivirus et la connexion au système d'administration distante.

En fonction du mode sélectionné, le Pare-feu permet d'établir les connexions qui sont autorisées et bloque les connexions interdites. L'information sur les connexions bloquées est consignée dans le journal d'événement. Le Pare-feu permet également de configurer les notifications de l'utilisateur sur les connexions bloquées.

Le Pare-feu n'est pas pris en charge par les systèmes d'exploitation BlackBerry et Android.

CHIFFREMENT

Le chiffrement chiffre les informations dans les dossiers définis par l'administrateur et l'utilisateur. La fonction Chiffrement repose sur une fonction de cryptage intégrée au système d'exploitation de l'appareil.

L'administrateur peut définir les dossiers à chiffrer dans la stratégie. L'utilisateur ne peut pas annuler le chiffrement des dossiers définis par l'administrateur. Il peut cependant spécifier les dossiers à chiffrer sur son appareil mobile via l'interface locale de l'application (voir le Guide de l'utilisateur pour le système d'exploitation correspondant). Si l'administrateur n'a pas défini les dossiers à chiffrer, l'application ne chiffrera que les dossiers spécifiés par l'utilisateur.

La fonction Chiffrement permet de chiffrer tous les types de dossiers, sauf les dossiers système. Le chiffrement des dossiers stockés dans la mémoire de l'appareil ou sur une carte mémoire est pris en charge. L'utilisateur ne peut accéder aux informations chiffrées qu'après avoir saisi le code secret de l'application qu'il a défini à la première exécution de l'application.

Le Chiffrement permet de définir la période à l'issue de laquelle l'interdiction de l'accès aux dossiers chiffrés sera activée et un code secret de l'application sera nécessaire pour accéder à ces dossiers. La fonction est activée quand l'appareil nomade est en mode d'économie d'énergie.

Le Chiffrement n'est pas pris en charge par les systèmes d'exploitation BlackBerry et Android.

ADMINISTRATION DES LICENCES

Dans le cadre de l'octroi de licences pour l'utilisation des applications de Kaspersky Lab, il est important de comprendre les notions suivantes :

- contrat de licence ;
- licences ;
- fichier de licence ;
- activation de l'application.

Ces notions sont liées les unes aux autres et forment un ensemble unique. Examinons chacune d'entre elles en détail.

DANS CETTE SECTION

PRESENTATION DU CONTRAT DE LICENCE

Le contrat de licence : contrat entre une personne physique ou morale détenant une copie légale de Kaspersky Endpoint Security et Kaspersky Lab ZAO. Le contrat de licence est inclus dans chaque application de Kaspersky Lab. Il décrit en détail les droits et les restrictions d'utilisation de Kaspersky Endpoint Security.

Conformément aux termes du contrat de licence, vous avez le droit de détenir une copie de l'application après avoir acheté et installé celle-ci.

Kaspersky Lab est ravie de vous proposer des services complémentaires :

- assistance technique ;
- mise à jour des bases de Kaspersky Endpoint Security.

Pour pouvoir les obtenir, vous devez acheter une licence et activer l'application.

PRESENTATION DES LICENCES DE KASPERSKY ENDPOINT SECURITY 8 FOR SMARTPHONE

La *licence* : droit d'utilisation de Kaspersky Endpoint Security 8 for Smartphone sur un ou plusieurs appareils mobiles et des services complémentaires associés offerts par Kaspersky Lab ou ses partenaires.

Chaque licence se définit par sa durée de validité et son type.

La *durée de validité de la licence* désigne la période pendant laquelle vous pouvez bénéficier des services complémentaires. Le volume des services proposés dépend du type de licence.

Les types de licence suivants existent :

- *Evaluation* : licence gratuite dont la validité est limitée, par exemple 30 jours, et qui permet de découvrir Kaspersky Endpoint Security 8 for Smartphone.

  Attention ! La licence d'évaluation ne peut être utilisée qu'une seule fois et ne peut pas être activée après l'expiration d'une licence commerciale.

Elle est fournie avec la version d'évaluation. La licence d'utilisation donne l'accès au Service d'assistance technique. Une fois la licence d'évaluation expirée, Kaspersky Endpoint Security 8 for Smartphone arrête de fonctionner. Seules les fonctions suivantes sont accessibles :

- désactiver des composants Chiffrement et Contacts personnels ;
- l'administrateur peut déchiffrer les dossiers qu'il a sélectionnés pour le chiffrement ;
- l'utilisateur peut déchiffrer les dossiers qu'il a sélectionnés pour le chiffrement ;
- consulter le système d'aide ;
- synchroniser avec le système d'administration distante.

- *Commerciale* : licence payante avec une durée de validité définie (par exemple, un an) octroyée à l'achat de Kaspersky Endpoint Security 8 for Smartphone. La distribution de cette licence est soumise aux restrictions de licence relatives, par exemple, au nombre d'appareils mobiles couverts.

  Toutes les fonctionnalités de l'application et les services complémentaires sont accessibles pendant la période de validité de la licence commerciale.

Une fois que la licence commerciale a expiré, les fonctionnalités de Kaspersky Endpoint Security 8 for Smartphone seront limitées. Vous pouvez toujours utiliser les composants Anti-Spam et Pare-feu, effectuer l'analyse antivirus de votre appareil mobile et utiliser les composants de protection, mais la date de mise à jour des bases antivirus sera celle de l'expiration de la licence. La mise à jour des bases antivirus n'est plus effectuée. Pour les autres composants, seules les fonctions suivantes sont accessibles :

- désactivation des composants Chiffrement, Antivol et Contacts personnels ;
- l'administrateur peut déchiffrer les dossiers qu'il a sélectionnés pour le chiffrement ;
- l'utilisateur peut déchiffrer les dossiers qu'il a sélectionnés pour le chiffrement ;
- consulter le système d'aide ;
- synchroniser avec le système d'administration distante.

Pour pouvoir utiliser l'application et les services complémentaires, il faut acheter une licence commerciale et activer l'application.

L'activation de l'application est effectuée via l'installation d'un fichier de licence associé à la licence.

PRESENTATION DES FICHIERS DE LICENCE DE KASPERSKY ENDPOINT SECURITY 8 FOR SMARTPHONE

Le fichier de licence : moyen technique qui permet d'installer la licence et d'activer l'application et, ce faisant, votre droit d'utilisation de l'application et des services complémentaires.

Le fichier de licence fait partie du kit de distribution de l'application si vous l'achetez chez un revendeur de Kaspersky Lab. Si vous l'achetez dans un magasin en ligne, il sera envoyé à votre adresse électronique.

Le fichier de licence contient les informations suivantes :

- Durée de validité de la licence.
- Type de licence (évaluation, commerciale).
- Restrictions de licence (par exemple, nombre d'appareils mobiles couverts par la licence).
- Contacts du Service d'assistance technique.
- Durée de validité du fichier de licence.

Durée de validité du fichier de licence : en quelque sorte, une date limite d'emploi définie pour le fichier de licence au moment de son attribution. Il s'agit d'une période à l'issue de laquelle le fichier de licence n'est plus valide ce qui bloque l'installation de la licence associée au fichier.

Prenons un exemple pour expliquer les liens entre la période de validité du fichier de licence et la durée de validité de la licence.

Exemple :

Durée de validité de la licence : 300 jours.

Date d'émission du fichier de licence : 01/09/2010.

Durée de validité du fichier de licence : 300 jours.

Date d'installation du fichier de licence : 10/09/2010, soit 9 jours après la date d'émission.

Résultat :

Durée de validité calculée pour la licence : 300 jours - 9 jours = 291 jours.

ACTIVATION DU LOGICIEL

Une fois installée sur l'appareil mobile, l'application Kaspersky Endpoint Security 8 for Smartphone reste opérationnelle pendant trois jours sans être activée.

Si l'activation n'est pas effectuée dans les trois jours, les fonctionnalités de l'application seront limitées automatiquement. Dans ce mode de fonctionnement, la plupart de composants de Kaspersky Endpoint Security 8 for Smartphone sont désactivés (cf. la rubrique "Présentation des licences de Kaspersky Endpoint Security 8 for Smartphone" à la page 20).

L'activation de l'application est effectuée via l'installation de la licence sur l'appareil mobile. L'appareil reçoit la licence avec la stratégie crée dans le système d'administration distante. Pendant les trois jours qui suivent l'installation de l'application, l'appareil établit une connexion automatique avec le système d'administration distante toutes les six heures. Durant cette période, l'administrateur doit ajouter la licence à la stratégie. L'application installée sur l'appareil sera activée dès la réception de la stratégie par l'appareil mobile.

VOIR AUSSI

Installation de la licence via Kaspersky Administration Kit 44

Activation du logiciel 103

Ajout de la licence via Sybase Afaria 136

DEPLOIEMENT DE L'APPLICATION VIA KASPERSKY ADMINISTRATION KIT

Cette section décrit la procédure de déploiement de Kaspersky Endpoint Security 8 for Smartphone via Kaspersky Administration Kit.

DANS CETTE SECTION

CONCEPTION DE LA GESTION DE L'APPLICATION VIA KASPERSKY ADMINISTRATION KIT

Kaspersky Endpoint Security 8 for Smartphone prend en charge la gestion via le système de gestion distante centralisée des applications de Kaspersky Lab Kaspersky Administration Kit. La gestion des appareils mobiles et de l'application Kaspersky Endpoint Security 8 for Smartphone installée sur ces appareils est effectuée de la même façon que la gestion des ordinateurs clients et des applications de Kaspersky Lab installées sur ces ordinateurs (voir le Guide de l'Administrateur de Kaspersky Administration Kit).

L'administrateur crée des groupes d'appareils mobiles et élabore une stratégie pour Kaspersky Endpoint Security 8 for Smartphone. Une stratégie est un ensemble des paramètres de fonctionnement de l'application. Les stratégies permettent de définir les mêmes valeurs des paramètres de fonctionnement de l'application pour tous les appareils mobiles du groupe. Pour en savoir plus sur les stratégies et les groupes d'administration, consultez le Guide de l'administrateur de Kaspersky Administration Kit.

La particularité de Kaspersky Endpoint Security 8 for Smartphone est que cette application ne prend pas en charge la création des tâches. Tous les paramètres du fonctionnement de l'application, y compris la licence, l'horaire de la mise à jour des bases de l'application, l'horaire de l'analyse de l'appareil sont définis via la stratégie (cf. la rubrique "Utilisation des stratégies" à la page 45) ou les paramètres locaux de l'application (cf. la rubrique "Configuration des paramètres locaux de l'application" à la page 59).

Si vous envisagez d'installer et d'utiliser l'application Kaspersky Endpoint Security 8 for Smartphone dans le réseau de votre entreprise, l'administrateur doit le prendre en considération à l'étape de la conception de la structure des groupes d'administration et pendant l'installation des composants logiciels de Kaspersky Administration Kit.

Lors de l'installation du Serveur d'administration, il faut installer un composant qui assure la gestion de la protection des appareils mobiles via Kaspersky Administration Kit (cf. la rubrique "Installation du Serveur d'administration" à la page 26). Lors de l'installation de ce composant est créé un *certificat du Serveur d'administration pour les appareils mobiles*. Il est utilisé pour l'authentification des appareils mobiles pendant l'échange de données avec le Serveur d'administration. Il est impossible de connecter les appareils mobiles au Serveur d'administration sans ce certificat.

L'interaction entre les appareils mobiles et le Serveur d'administration s'effectue lors de la synchronisation des appareils avec le Serveur d'administration. Cette fonctionnalité est assurée par l'application Kaspersky Endpoint Security 8 for Smartphone, alors, l'installation de l'Agent d'administration sur les appareils mobiles n'est pas nécessaire.

L'échange de données entre les appareils mobiles et le Serveur d'administration est effectué via Internet. Le trafic sortant est entrant est payé par les utilisateurs d'appareils mobiles aux tarifs de l'opérateur de la téléphonie mobile. Le volume moyen des données transmises pendant une séance de synchronisation remonte à 20-40 KB. Le volume des données dépend du nombre des rapports à transmettre. Plus rarement la synchronisation est effectuée, plus de rapports sont transmis au Serveur d'administration.

Pour gérer la protection des appareils mobiles, il est conseillé de créer dans le nœud **Ordinateurs administrés** un groupe ou des groupes spécifiques (en fonction du nombre des systèmes d'exploitation installés sur les appareils), en cas d'installation de l'application via les postes de travail des utilisateurs, il est conseillé de créer également un groupe spécifique pour les postes de travail en question (cf. la rubrique "Création de groupes" à la page 29).

PROCEDURE DU DEPLOIEMENT VIA KASPERSKY ADMINISTRATION KIT

Procédure du déploiement de Kaspersky Endpoint Security 8 for Smartphone dépend de la modalité d'installation de l'application sur les appareils mobiles sélectionnée par l'administrateur. L'installation de l'application peut être effectuée par un des moyens suivants :

- via les postes de travail qui servent à connecter les appareils mobiles d'utilisateurs (cf. la rubrique "Installation de l'application via le poste de travail" à la page 29) ;
- par une diffusion des messages électroniques aux adresses des utilisateurs avec la distribution de l'application ou avec une instruction sur son téléchargement (cf. la rubrique "Installation de l'application par une diffusion des messages électroniques" à la page 43).

L'administrateur assure la préparation de la distribution de l'application à l'installation sur les appareils mobiles d'utilisateurs. La copie de la distribution sur les appareils mobiles et l'installation de l'application sur les appareils mobiles sont effectuées par les utilisateurs. Une fois l'application installée, l'administrateur doit ajouter les appareils mobiles aux ordinateurs administrés et créer une stratégie pour envoyer la licence et les paramètres de fonctionnement de l'application vers les appareils mobiles.

Ainsi, pendant la gestion de l'application via Kaspersky Administration Kit l'administrateur peut utiliser les procédures du déploiement suivantes : déploiement de l'application via les postes de travail (cf. la rubrique "Déploiement de l'application via le poste de travail" à la page 24) et déploiement de l'application par une diffusion des messages électroniques (cf. la rubrique "Procédure du déploiement de l'application par une diffusion des messages électroniques" à la page 25).

Avant de déployer l'application, l'administrateur doit s'assurer que la version installée de Kaspersky Administration Kit prend en charge la gestion de la protection des appareils mobiles.

DANS CETTE SECTION

DEPLOIEMENT DE L'APPLICATION VIA LE POSTE DE TRAVAIL

Le déploiement de l'application via le poste de travail est utilisé si les utilisateurs connectent les appareils mobiles à leurs postes de travail et comprend les étapes suivantes :

1. Configuration de la gestion des appareils mobiles via Kaspersky Administration Kit. Cette étape assure la possibilité de connecter les appareils mobiles au Serveur d'administration (cf. la rubrique "Préparation au déploiement de l'application via Kaspersky Administration Kit" à la page 25).
2. Création de groupes d'administration pour le placement des appareils mobiles et les postes de travail qui servent à transmettre la distribution de l'application Kaspersky Endpoint Security 8 for Smartphone vers les appareils mobiles.
3. Création du paquet d'installation pour la tâche d'installation à distance de Kaspersky Endpoint Security 8 for Smartphone.

4. Configuration des paramètres du paquet d'installation pour la tâche d'installation à distance de Kaspersky Endpoint Security 8 for Smartphone.
5. Création de la tâche d'installation à distance qui permettra à transmettre la distribution de l'application Kaspersky Endpoint Security 8 for Smartphone vers les postes de travail et d'installer l'utilitaire de transmission de la distribution vers les appareils mobiles.
6. Transmission de la distribution de l'application vers l'appareil mobile. À cette étape, l'utilisateur copie la distribution de l'application sur l'appareil mobile à l'aide de l'utilitaire kmlisten.exe.
7. Installation de l'application sur l'appareil mobile. À cette étape, l'utilisateur effectue l'installation de l'application sur l'appareil mobile.
8. Création de la stratégie de gestion des paramètres de Kaspersky Endpoint Security 8 for Smartphone.

PROCEDURE DE DEPLOIEMENT DE L'APPLICATION PAR UNE DIFFUSION DES MESSAGES ELECTRONIQUES

Le déploiement de l'application par une diffusion des messages électroniques est utilisé si pour une raison ou une autre l'installation de l'application via le poste de travail est impossible ou inefficace. Par exemple, le poste de travail de l'utilisateur tourne sous le système d'exploitation Mac OS. La procédure comprend les étapes suivantes :

1. Configuration de la gestion des appareils mobiles via Kaspersky Administration Kit.
2. Placement de la distribution de l'application sur un serveur FTP / HTTP À cette étape, l'administrateur place la distribution de l'application sur un serveur FTP / HTTP et configure l'accès à la distribution via Internet. Par la suite, pendant la composition du message qui sera envoyé aux utilisateurs des appareils mobiles, l'administrateur pourra y ajouter le lien sur cette distribution. Si l'administrateur envisage d'ajouter la distribution de l'application au message en tant que pièce jointe, cette étape est ignorée.
3. Création de groupes d'administration pour le placement des appareils mobiles et les postes de travail qui servent à transmettre la distribution de l'application Kaspersky Endpoint Security 8 for Smartphone vers les appareils mobiles.
4. Composition et envoi du message avec la distribution de l'application aux utilisateurs des appareils mobiles.
5. Téléchargement de la distribution de l'application sur l'appareil mobile. À cette étape, l'utilisateur télécharge sur l'appareil la distribution de l'application jointe au message ou placée sur un serveur FTP / HTTP par l'administrateur.
6. Installation de l'application sur l'appareil mobile.
7. Création de la stratégie de gestion des paramètres de Kaspersky Endpoint Security 8 for Smartphone.
8. Déplacement de l'appareil dans le groupe d'administration.
9. Activation de la licence de l'application sur les appareils mobiles d'utilisateurs.
10. Configuration des paramètres locaux de l'application.

PREPARATION AU DEPLOIEMENT DE L'APPLICATION VIA KASPERSKY ADMINISTRATION KIT

Avant de procéder au déploiement de l'application Kaspersky Endpoint Security 8 for Smartphone, l'administrateur doit configurer la gestion des appareils mobiles via Kaspersky Administration Kit. Pour ce faire, procédez comme suit :

1. Installez ou assurez-vous que les composants de Kaspersky Administration Kit sont installés dans le réseau : Serveur d'administration et Console de gestion (voir Manuel de déploiement de Kaspersky Administration Kit).

2. Assurez-vous que les composants installés satisfont les configurations logicielles pour l'installation de l'application Kaspersky Endpoint Security 8 for Smartphone.

   Lors de l'installation du Serveur d'administration, il faut installer un composant qui assure la gestion de la protection des appareils mobiles via Kaspersky Administration Kit (cf. la rubrique "Installation du Serveur d'administration" à la page 26). Si ce composant n'a pas été installé ou si la version du Serveur d'administration ne satisfait pas les configurations pour l'installation de Kaspersky Endpoint Security 8 for Smartphone l'administrateur doit supprimer l'ancienne version du composant et installer la version indiquée dans les configurations logicielles après avoir effectué une copie de sauvegarde des données du Serveur d'administration.

3. Configurez la prise en charge des appareils mobiles dans les paramètres du Serveur d'administration (cf. la rubrique "Configuration des paramètres du Serveur d'administration" à la page 27).

4. Installez sur le poste de travail de l'administrateur le plug-in de gestion de l'application Kaspersky Endpoint Security 8 for Smartphone.

DANS CETTE SECTION

INSTALLATION DU SERVEUR D'ADMINISTRATION

L'installation du Serveur d'administration est décrite dans le Manuel de déploiement de Kaspersky Administration Kit. Pour assurer la gestion de la protection des appareils mobiles via Kaspersky Administration Kit à l'étape **Sélection des composants**, il faut obligatoirement cocher la case **Prise en charge des appareils nomades** (cf. ill. ci-après).

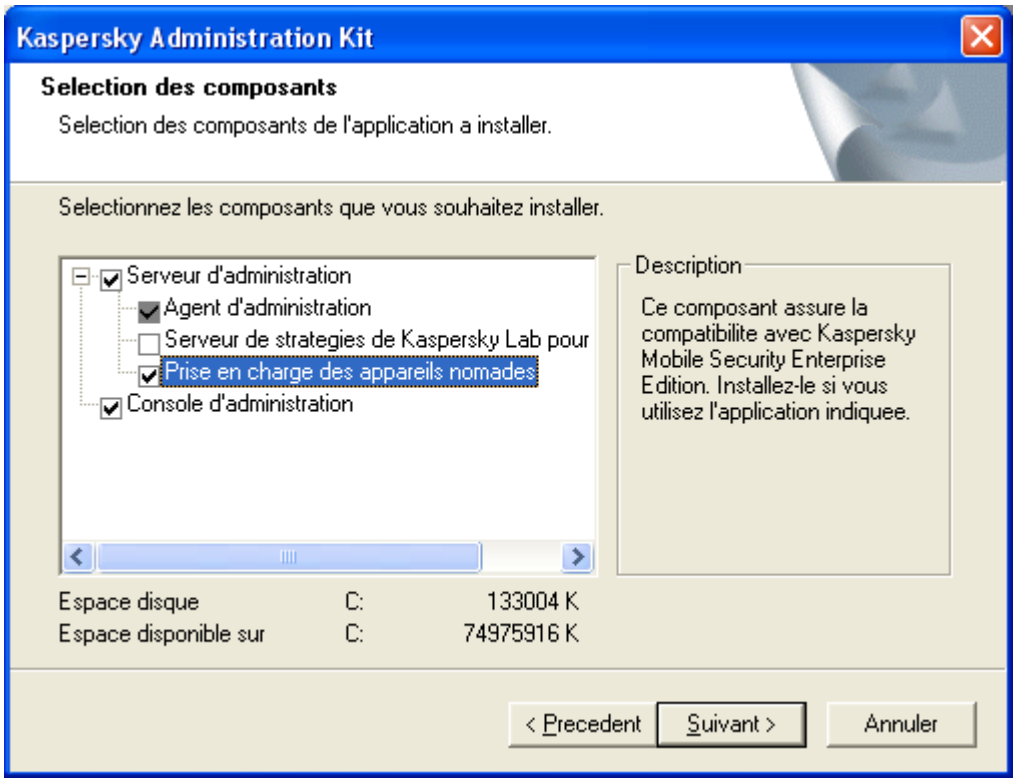


Figure 1 : installation des composants de Kaspersky Administration Kit. Sélection des composants

Pendant l'installation du composant Prise en charge des appareils mobiles est créé un *certificat du Serveur d'administration pour les appareils mobiles*. Il est utilisé pour l'authentification des appareils mobiles pendant l'échange de données avec le Serveur d'administration. L'échange d'informations est effectué par le protocole SSL (Secure Socket Layer). Il est impossible de connecter les appareils mobiles au Serveur d'administration sans ce certificat.

Le certificat pour les appareils mobiles est enregistré dans le dossier d'installation de l'application Kaspersky Administration Kit dans le sous-dossier Cert. Pendant la première synchronisation de l'appareil mobile avec le Serveur d'administration, une copie de certificat est transmise sur l'appareil et enregistrée dans un dossier spécifique sur l'appareil.

Si l'utilisateur change le nom ou supprime le certificat pour l'appareil mobile de son appareil, le Serveur d'administration enverra automatiquement une copie du certificat sur l'appareil pendant la synchronisation suivante.

MISE A JOUR DU COMPOSANT SERVEUR D'ADMINISTRATION

Si pendant l'installation du Serveur d'administration la case **Prise en charge des appareils nomades** n'a pas été cochée ou une ancienne version de Kaspersky Administration Kit sans prise en charge de Kaspersky Endpoint Security 8 for Smartphone a été installée, il faut mettre à jour la version installée du composant Serveur d'administration.

Pour mettre à jour la version installée du composant Serveur d'administration, procédez comme suit :

1. Effectuez une copie de sauvegarde des données du Serveur d'administration (voir le Manuel de référence de Kaspersky Administration Kit).
2. Installez la version du Serveur d'administration indiquée dans les configurations logicielles pour l'installation de l'application Kaspersky Endpoint Security 8 for Smartphone (cf. la rubrique "Configuration logicielle et matérielle" à la page 13).

   Pour assurer la gestion de la protection des appareils mobiles via Kaspersky Administration Kit à l'étape **Sélection des composants**, il faut obligatoirement cocher la case **Prise en charge des appareils nomades**.
3. Restaurez les données du Serveur d'administration depuis la copie de sauvegarde (voir le Manuel de référence de Kaspersky Administration Kit).

CONFIGURATION DES PARAMETRES DU SERVEUR D'ADMINISTRATION

Pour assurer la synchronisation des appareils mobiles avec le Serveur d'administration avant l'installation de Kaspersky Endpoint Security 8 for Smartphone, il faut configurer les paramètres de connexion des appareils mobiles dans les propriétés du Serveur d'administration.

Pour configurer les paramètres de connexion des appareils mobiles dans les propriétés du Serveur d'administration, procédez comme suit :

1. Sélectionnez dans l'arborescence de la console le Serveur d'administration.
2. Ouvrez le menu contextuel et sélectionnez l'élément **Propriétés**.
3. Ouvrez l'onglet **Paramètres** dans la fenêtre de propriétés du Serveur d'administration qui s'affiche.
4. Cochez la case **Ouvrir le port pour les périphériques mobiles** dans le groupe **Paramètres de connexion au Serveur d'administration**. Dans le champ **Port pour les périphériques mobiles** spécifiez le port pour la connexion des appareils mobiles au Serveur d'administration. Le numéro de port par défaut est 13292 (cf. ill. ci-après). Si la case n'est pas cochée ou le port est incorrect, les appareils ne pourront pas se connecter au serveur pour envoyer ou recevoir les informations.

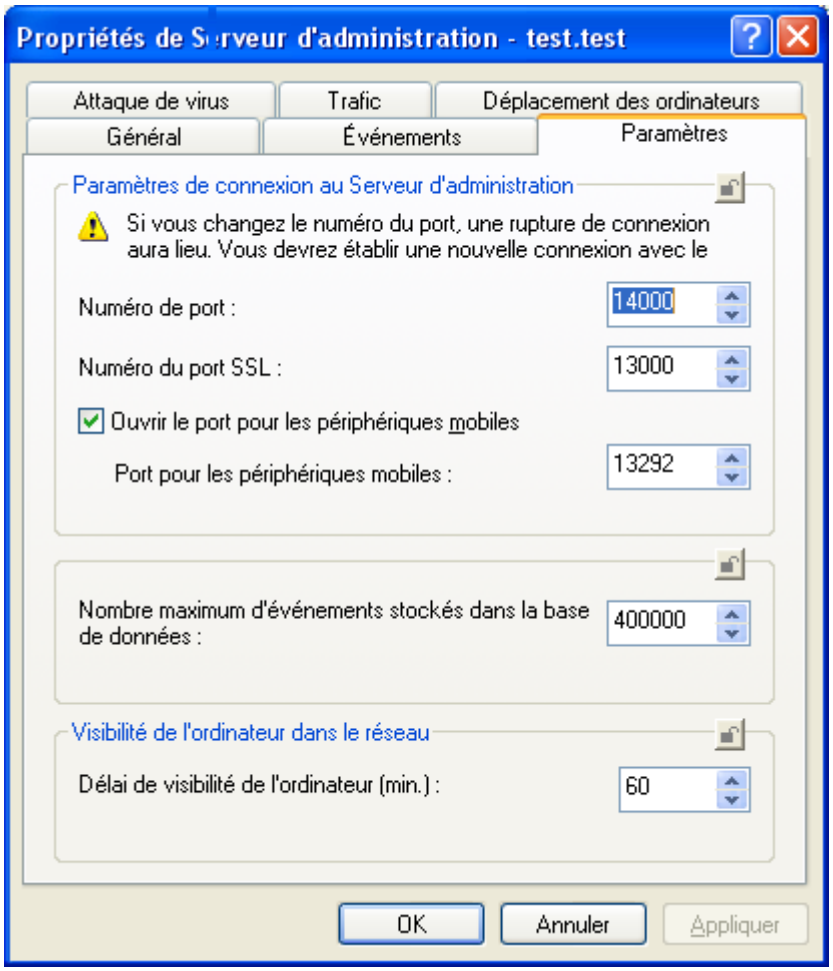


Figure 2 : configuration des paramètres de connexion des appareils mobiles au serveur d'administration

INSTALLATION DU PLUG-IN DE GESTION DE KASPERSKY ENDPOINT SECURITY 8 FOR SMARTPHONE

Pour accéder à l'interface de gestion de l'application à l'aide de Kaspersky Administration Kit, il faut installer le plug-in de gestion de l'application Kaspersky Endpoint Security 8 for Smartphone sur le poste de travail de l'administrateur.

Pour installer le plug-in de gestion de l'application Kaspersky Endpoint Security 8 for Smartphone,

copiez le fichier d'installation du plug-in depuis la distribution de l'application et exécutez-le sur le poste de travail de l'administrateur.

Pour vous assurer que le plug-in est installé, consultez la liste des plug-ins dans les propriétés du Serveur d'administration. Pour les détails, consultez le guide de Kaspersky Administration Kit.

PLACEMENT DE LA DISTRIBUTION DE L'APPLICATION SUR UN SERVEUR FTP / HTTP

Si la modalité d'installation de l'application est installation par une diffusion des messages électroniques (cf. la rubrique "Installation de l'application par une diffusion des messages électroniques" à la page 43), vous pouvez placer sur le serveur FTP / HTTP le fichier d'installation qui sera utilisé pendant l'installation de l'application sur les appareils mobiles. Il faut configurer l'accès via Internet au dossier où sera placé le fichier d'installation de l'application sur le serveur FTP / HTTP. Si les appareils mobiles d'utilisateurs tournent sous différents systèmes d'exploitation, vous pouvez ajouter dans le dossier plusieurs fichiers pour chacun des systèmes d'exploitation.

Ensuite, pendant la composition du message avec la distribution de l'application pour les utilisateurs des appareils mobiles, il faut ajouter au texte du message le lien sur le fichier d'installation. Ce lien permet à l'utilisateur de télécharger le fichier d'installation sur son appareil mobile et d'effectuer l'installation de l'application (cf. la rubrique "Installation de l'application par une diffusion des messages électroniques" à la page 43).

CREATION DE GROUPES

La gestion des programmes installés sur les appareils mobiles est effectuée à l'aide des stratégies de groupes appliquées aux appareils en question. Aussi, avant d'installer l'application sur les appareils mobiles faut-il créer un groupe spécifique d'administration pour ces appareils dans le noeud **Ordinateurs administrés**. Une fois l'installation terminée, il faut déplacer tous les appareils avec l'application installée dans ce groupe (cf. la rubrique "Déplacement des appareils dans le groupe Ordinateurs administrés" à la page 55).

Si la modalité d'installation de Kaspersky Endpoint Security 8 for Smartphone est l'installation de l'application sur les appareils mobiles via le poste de travail, vous pouvez créer sur le Serveur d'administration un groupe spécifique pour les postes de travail utilisés pour connecter les appareils mobiles d'utilisateurs. Ensuite, vous pourrez créer pour ce groupe une tâche de groupe pour l'installation de l'application Kaspersky Endpoint Security 8 for Smartphone à distance et utilisez cette tâche pour installer l'application sur tous les postes de travail qui font partie de groupe en même temps.

Pour en savoir plus sur la création de groupes, consultez le Guide de l'administrateur Kaspersky Administration Kit.

INSTALLATION DE L'APPLICATION DEPUIS UN POSTE DE TRAVAIL

Pour installer Kaspersky Endpoint Security 8 for Smartphone via le poste de travail, il faut faire un paquet d'installation et configurer ses paramètres, créer et lancer la tâche d'installation à distance pour les postes de travail qui servent à connecter les appareils mobiles d'utilisateurs. Pour créer la tâche, l'administrateur peut utiliser chacune des modalités prévues par Kaspersky Administration Kit :

- créer la tâche de groupe d'installation à distance si les postes de travail font partie du groupe ;
- créer une tâche pour un ensemble d'ordinateurs si les postes de travail font partie de différents groupes ou du groupe **Ordinateurs non répartis** ;
- utiliser l'assistant d'installation à distance.

L'exécution de la tâche d'installation à distance permet de transmettre le paquet d'installation avec la distribution de l'application Kaspersky Endpoint Security 8 for Smartphone vers les postes de travail d'utilisateurs, ainsi que d'installer et de lancer automatiquement *l'utilitaire de transmission de l'application vers l'appareil mobile kmlisten.exe*. L'utilitaire contrôle la connexion des appareils mobiles à l'ordinateur. Si l'utilisateur connecte au poste de travail un appareil qui satisfait les spécifications système d'installation de Kaspersky Endpoint Security 8 for Smartphone, l'utilitaire affiche sur l'écran un message qui l'invite à installer l'application sur l'appareil mobile connecté. Si l'utilisateur accepte cette invitation, l'utilitaire télécharge la distribution de l'application sur l'appareil mobile. Une fois le téléchargement terminé, l'appareil lance l'assistant d'installation de l'application. En suivant les instructions de l'assistant, l'utilisateur effectue l'installation de Kaspersky Endpoint Security 8 for Smartphone sur son appareil.

DANS CETTE SECTION

CREATION DU PAQUET D'INSTALLATION

Le paquet d'installation de Kaspersky Endpoint Security 8 for Smartphone est une archive auto-extractible KES8_forAdminKit_fr.exe qui contient les fichiers nécessaires pour installer l'application sur les appareils mobiles :

- endpoint_8_0_x_xx_fr.cab : fichier d'installation de l'application pour le système d'exploitation Windows Mobile ;
- endpoint8_mobile_8_x_xx_eu4_signed.sis : fichier d'installation de l'application pour le système d'exploitation Symbian ;
- Endpoint8_Mobile_8_x_xx_fr_release.zip : fichier d'installation de l'application pour le système d'exploitation BlackBerry ;
- Endpoint8_8_x_xx_release.apk : fichier d'installation de l'application pour Android ;
- installer.ini : fichier de configuration avec des paramètres de connexion au Serveur d'administration ;
- kmlisten.ini : fichier de configuration avec des paramètres de l'utilitaire de transmission du paquet d'installation ;
- kmlisten.kpd : fichier avec la description de l'application ;
- AdbWinUsbApi.dll, AdbWinApi.dll, adb.exe : ensemble de fichiers indispensable à l'installation de l'application sur les appareils Android ;
- kmlisten.exe : utilitaire de transmission de la distribution de l'application sur l'appareil mobile depuis le poste de travail.

Pour créer le paquet d'installation pour installer Kaspersky Endpoint Security 8 for Smartphone, procédez comme suit :

1. Connectez-vous au Serveur d'administration.
2. Sélectionnez dans le noeud **Zones de stockage** de l'arborescence de la console le dossier **Paquets d'installation**.
3. Ouvrez le menu contextuel et sélectionnez l'option **Créer →Paquet d'installation** ou utilisez l'option similaire dans le menu **Action**. Finalement l'Assistant est lancé. Suivez ses instructions.
4. Spécifiez le nom du paquet d'installation.
5. Spécifiez l'application à installer (cf. ill. ci-après).

   Sélectionnez dans la liste déroulante l'élément **Générer le paquet d'installation pour l'application de Kaspersky Lab**.

Cliquez sur **Sélectionner** pour ouvrir le dossier avec la distribution de l'application et sélectionnez l'archive auto-extractible KES8_forAdminKit_fr.exe. Si l'archive a été déjà décompressé, vous pouvez sélectionnez le fichier avec la description de l'application kmlisten.kpd qui fait partie de l'archive. Finalement les champs se remplissent automatiquement avec le nom et le numéro de version de l'application.

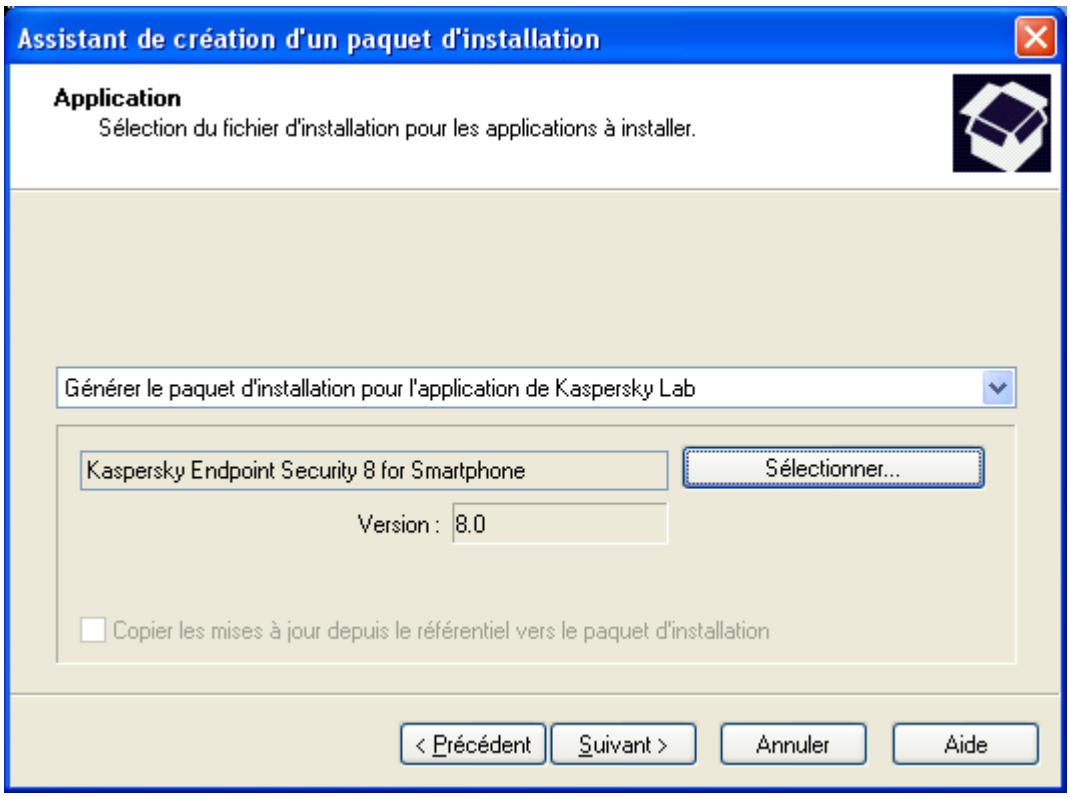


Figure 3 : création d'un paquet d'installation. Sélection du programme à installer

6. À cette étape, le paquet d'installation sera téléchargé sur le serveur d'administration dans le dossier de partage.

Après la fermeture de l'assistant, le paquet d'installation créé sera ajouté au nœud **Paquets d'installation** et affiché dans la barre des résultats.

Avant d'utiliser le paquet d'installation créé pour installer l'application, il faut configurer les paramètres du paquet d'installation (cf. la rubrique "Configuration des paramètres du paquet d'installation" à la page 31).

CONFIGURATION DES PARAMETRES DU PAQUET D'INSTALLATION

Pour configurer les paramètres du paquet d'installation, procédez comme suit :

1. Connectez- vous au serveur d'administration.
2. Sélectionnez dans le noeud **Zones de stockage** de l'arborescence de la console le dossier **Paquets d'installation**.
3. Sélectionnez dans la barre des résultats le paquet d'installation créé dont les paramètres vous souhaitez configurer.
4. Ouvrez le menu contextuel et sélectionnez l'élément **Propriétés**.
5. Sous l'onglet **Paramètres** spécifiez les paramètres de connexion des appareils mobiles au Serveur d'administration et le nom du groupe où les appareils mobiles seront ajoutés automatiquement après la première synchronisation avec le Serveur d'administration (cf. ill. ci-après). Pour ce faire, exécutez les actions suivantes :
   - Dans le groupe **Connexion au serveur d'administration**, spécifiez dans le champ **Adresse du serveur** l'adresse du Serveur d'administration dans le format qui est utilisé pour les propriétés du Serveur d'administration sous l'onglet **Général** dans le champ **Adresse**. En d'autres termes, si dans les propriétés du Serveur d'administration une adresse IP est indiquée, saisissez la même adresse IP dans le champ **Adresse du serveur**. Si dans les propriétés du Serveur d'administration un nom DNS est indiqué,

saisissez le même nom DNS dans le champ **Adresse du serveur**. Saisissez dans le champ **Numéro du port SSL** le numéro du port ouvert sur le Serveur d'administration pour connecter les appareils mobiles. Le numéro de port par défaut est 13292.

- Dans le groupe **Placement des ordinateurs dans le groupe**, saisissez dans le champ **Nom du groupe** le nom du groupe où les appareils mobiles seront ajoutés après la première synchronisation avec le Serveur d'administration (KES8 par défaut). Le groupe indiqué sera créé automatiquement dans le dossier **Ordinateurs non répartis**. Dans le groupe **Actions lors de l'installation** cochez la case **Demander l'adresse électronique** pour permettre à l'application de demander l'adresse électronique d'entreprise à l'utilisateur à la première exécution après la saisie du code secret. L'adresse électronique de l'utilisateur est utilisée pour créer le nom des appareils mobiles lorsqu'ils sont ajoutés dans le groupe d'administration. Le nom de l'appareil mobile de l'utilisateur est composé de la façon suivante :

  - Pour les appareils mobiles tournant sous Microsoft Windows Mobile :

    ```
    <adresse électronique de l'utilisateur (modèle de l'appareil mobile - IMEI)>
    ```

  - Pour les appareils mobiles tournant sous Symbian :

    ```
    <adresse électronique de l'utilisateur (modèle de l'appareil mobile - IMEI)>
    ```

  - pour les appareils mobiles tournant sous Blackberry :

    ```
    <adresse électronique de l'utilisateur (modèle de l'appareil mobile - IMEI)>
    ```

  - Pour les appareils mobiles tournant sous Android :

    ```
    <adresse électronique de l'utilisateur (modèle de l'appareil mobile – device pin)>
    ```

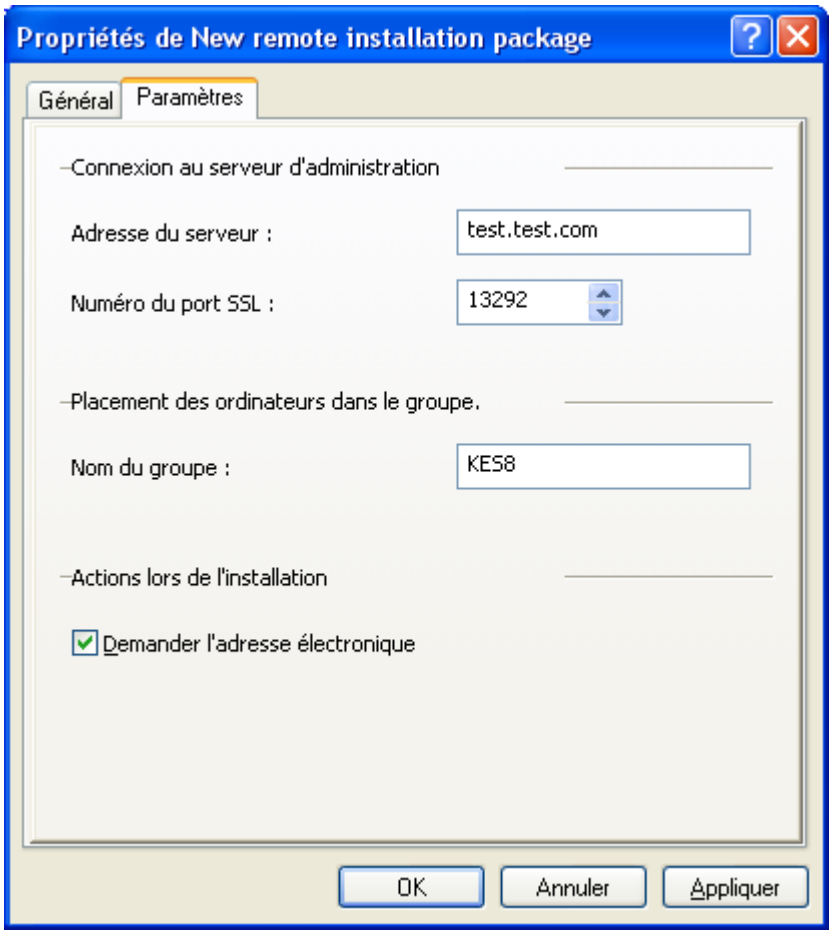


Figure 4 : configuration des paramètres du paquet d'installation

CREATION D'UNE TACHE D'INSTALLATION A DISTANCE

La tâche d'installation à distance est créée avec *l'assistant de création de la tâche d'installation à distance* ou avec *l'assistant d'installation à distance*. En fonction du mode d'installation sélectionné, la séquence des étapes de l'assistant et les paramètres configurés peuvent varier. Faites attention à la configuration des paramètres aux étapes suivantes :

1. Sélection du type de la tâche. À cette étape, vous serez invité à spécifier l'application pour laquelle la tâche est créée et le type de la tâche. Pour installer Kaspersky Endpoint Security 8 for Smartphone, il faut créer la tâche pour l'application Kaspersky Administration Kit, le type de la tâche étant **Installation à distance de l'application**.

2. Sélection de paquet d'installation. À cette étape, vous serez invité à sélectionner le paquet d'installation avec la distribution de l'application Kaspersky Endpoint Security 8 for Smartphone. Vous pouvez sélectionner un paquet d'installation pour Kaspersky Endpoint Security 8 for Smartphone qui existe déjà ou créer un paquet d'installation à cette étape directement. En cas de création d'un paquet d'installation, il faut spécifier l'archive auto-extractible KES8_forAdminKit_fr.exe. Si l'archive a été déjà décompressé, vous pouvez sélectionnez le fichier qui fait partie de l'archive et contient la description de l'application kmlisten.kpd (cf. la rubrique "Création du paquet d'installation" à la page 30).

3. Sélection de méthode d'installation. Il existe deux méthodes d'installation des applications sur les postes de travail dans Kaspersky Administration Kit : celle de l'installation forcée et celle qui utilise le script d'ouverture de session. La méthode d'installation forcée permet d'effectuer une installation du logiciel à distance sur les postes de travail spécifiques. La méthode d'installation par script d'ouverture de session permet d'assigner le lancement de l'installation à un profil spécifique d'utilisateur (de plusieurs utilisateurs).

   Cette étape est omise pour l'assistant d'installation à distance et l'assistant de création de la tâche de groupe, parce qu'ils effectuent l'installation sur des postes de travail spécifiques en utilisant la méthode de l'installation forcée. Pour installer l'application Kaspersky Endpoint Security 8 for Smartphone avec la tâche pour un ensemble d'ordinateurs, l'administrateur peut utiliser chacune des méthodes.

   Pour en savoir plus sur les méthodes d'installation, consultez le Manuel de référence de Kaspersky Administration Kit.

4. Sélection d'ordinateurs pour l'installation. À cette étape, vous serez invité à créer une liste des postes de travail qui serviront à installer l'application sur les appareils mobiles. Vous avez le choix parmi les options suivantes :

   - **Installer sur le groupe d'ordinateurs administrés**. Sélectionnez cette option si pendant la préparation à l'installation de l'application vous avez créé un groupe d'administration dans le noeud **Ordinateurs administrés** et si vous y avez déplacé tous les ordinateurs qui servent à connecter les appareils mobiles (cf. la rubrique "Création de groupes" à la page 29).

   - **Sélectionnez les ordinateurs pour l'installation**. Sélectionnez cette option si le groupe n'a pas été créé. À l'étape suivante, l'assistant vous invitera à créer une liste d'ordinateurs pour installer l'application.

5. Sélection du mode de téléchargement du paquet d'installation. À cette étape, vous serez invité à configurer les paramètres de transmission du paquet d'installation sur les postes de travail. Il existe deux modes de transmission du paquet d'installation sur les postes de travail :

   - **A l'aide de l'Agent d'administration**. Sélectionnez cette option si l'Agent d'administration est installé et connecté au Serveur d'administration actuel sur les postes de travail qui servent à installer Kaspersky Endpoint Security 8 for Smartphone.

     Si l'Agent d'administration n'est pas installé, mais vous envisagez son installation, vous pouvez utiliser l'installation partagée proposée à l'étape suivante de l'assistant.

   - **Via les outils Microsoft Windows depuis le dossier partagé**. Sélectionnez cette option si l'Agent d'administration n'est pas installé sur les postes de travail ou s'il est connecté à un autre Serveur d'administration. Dans ce cas, la transmission des fichiers nécessaires à l'installation de l'application est effectuée par des outils de Windows via les dossiers de partage.

6. Sélection du paquet d'installation supplémentaire pour l'installation. À cette étape, vous serez invité à installer l'Agent d'administration sur les postes de travail. Utilisez l'installation partagée si vous avez sélectionné à l'étape précédente le mode de téléchargement du paquet d'installation **À l'aide de l'Agent d'administration**, mais l'Agent d'administration n'est pas encore installé sur les postes de travail. Dans ce cas, il faut d'abord installer sur les postes de travail l'Agent d'administration, et ensuite transmettre le paquet d'installation à l'aide de l'Agent d'administration.

   L'installation partagée n'est pas nécessaire si la transmission de la distribution sur les postes de travail est effectuée par des outils de Microsoft Windows ou si une version de l'Agent d'administration qui satisfait les spécifications système d'installation de Kaspersky Endpoint Security 8 for Smartphone a déjà été installée.

Une description détaillée du processus de création de tâches et du fonctionnement de l'assistant d'installation est fournie dans le Manuel de mise en place de Kaspersky Administration Kit. Voici la description de la création de la tâche de groupe d'installation à distance.

Pour créer la tâche de groupe d'installation à distance de Kaspersky Endpoint Security 8 for Smartphone, procédez comme suit :

1. Connectez-vous au Serveur d'administration.
2. Dans l'arborescence de la console, sélectionnez le groupe pour lequel vous souhaitez créer une tâche.
3. Sélectionnez le dossier **Tâches de groupe** appartenant au groupe.
4. Ouvrez le menu contextuel et sélectionnez l'option **Créer** → **Tâche** ou cliquez sur le lien **Créer une nouvelle tâche** situé sur la barre des tâches. Cette action lance un Assistant. Suivez les instructions de l'Assistant.
5. Indiquez le nom de la tâche. Si une tâche de ce nom existe déjà dans le groupe, un "_1" sera automatiquement ajouté au nouveau nom.
6. Sélectionnez le type de la tâche **Installation à distance de l'application** pour l'application **Kaspersky Administration Kit** (cf. ill. ci-après).

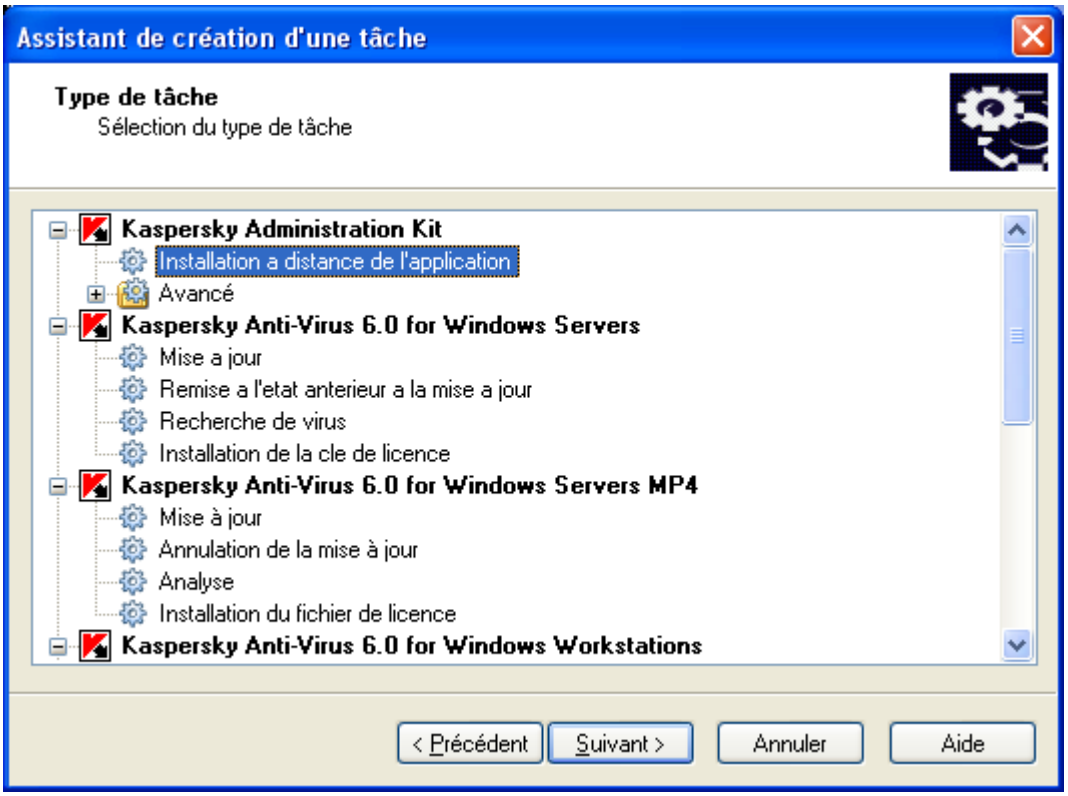


Figure 5 : création d'une tâche Choix de l'application et du type de tâche

7. Sélectionnez dans la liste le paquet d'installation que vous avez créée pour installer l'application Kaspersky Endpoint Security 8 for Smartphone ou créez un nouveau paquet d'installation en cliquant sur **Nouveau** (cf. ill. ci-après).

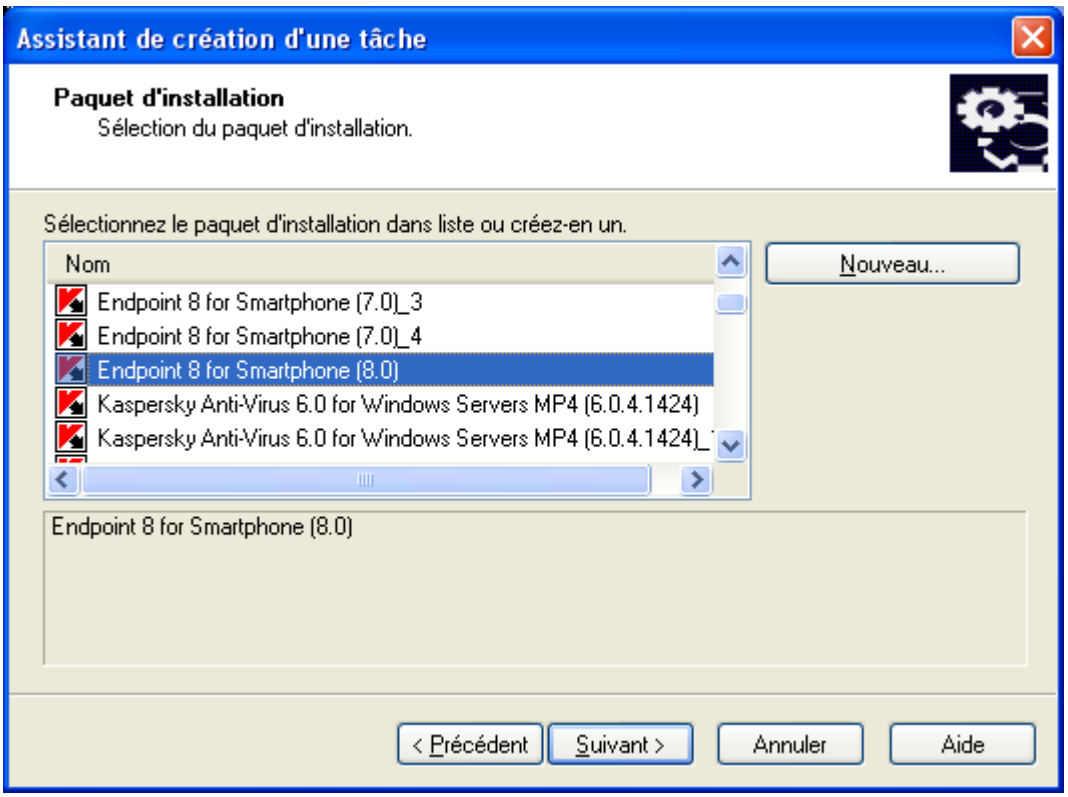


Figure 6 : création d'une tâche Sélection de paquet d'installation

8. Sélectionnez le mode de téléchargement du paquet d'installation (cf. ill. ci-après). Pour ce faire, cochez ou décochez les cases suivantes :

   - **A l'aide de l'Agent d'administration**. Dans ce cas, la transmission des fichiers sur les postes de travail est effectuée par l'Agent d'administration installé sur chacun des postes.

- **Via les outils Microsoft Windows depuis le dossier partagé**. Dans ce cas, la transmission des fichiers nécessaires à l'installation de l'application sur les postes de travail est effectuée par des outils de Windows via les dossiers de partage.

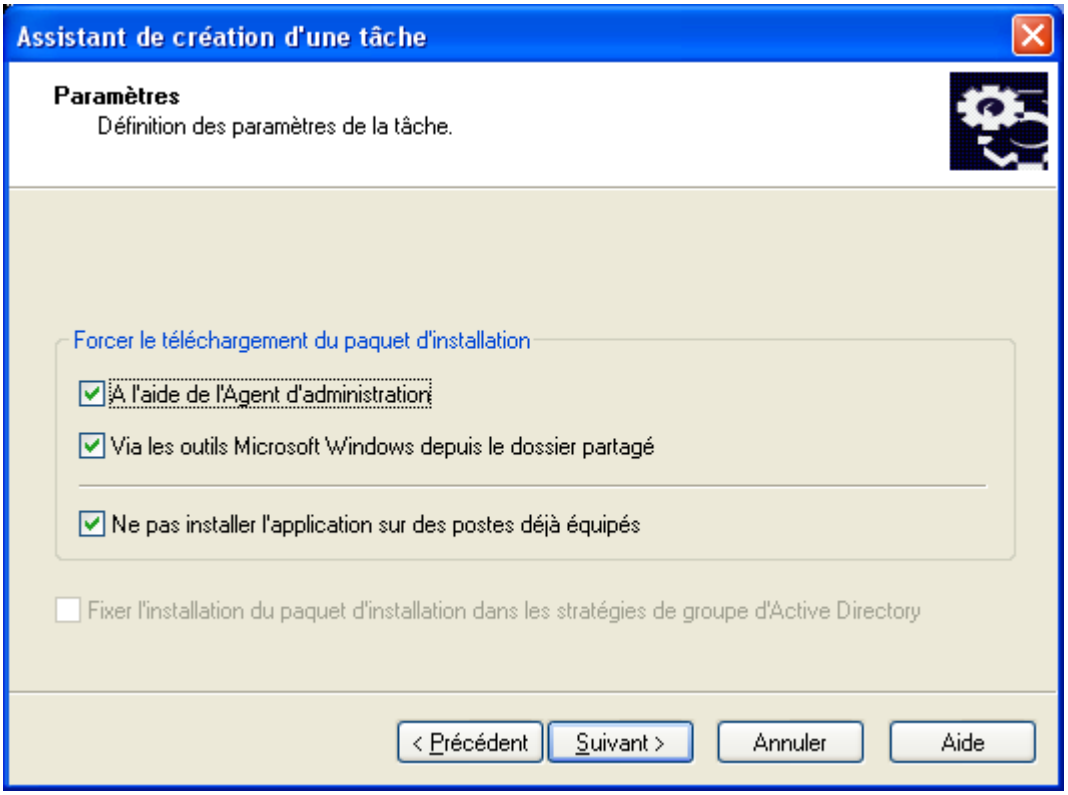


Figure 7 : création d'une tâche Configuration des paramètres de téléchargement du paquet d'installation

9. Cochez la case **Installer l'Agent d'administration avec cette application**, si vous avez sélectionné à l'étape précédente le téléchargement du paquet d'installation **À l'aide de l'Agent d'administration**, mais ce composant n'a pas été installé sur les postes de travail ou si la version installée n'est pas compatible avec celle du Serveur d'administration (cf. ill. ci-après). Dans ce cas, il faut d'abord installer l'Agent d'administration sur le poste de travail pour transmettre ensuite le paquet d'installation de Kaspersky Endpoint Security 8 for Smartphone vers le poste de travail à l'aide de l'Agent d'administration.

   Si vous avez sélectionné à l'étape précédente le téléchargement du paquet d'installation par des **Outils de Microsoft Windows depuis le dossier de partage**, décochez la case **Installer l'Agent d'administration avec cette application**. Dans ce cas, l'Agent d'administration ne sera pas installé sur le poste de travail.

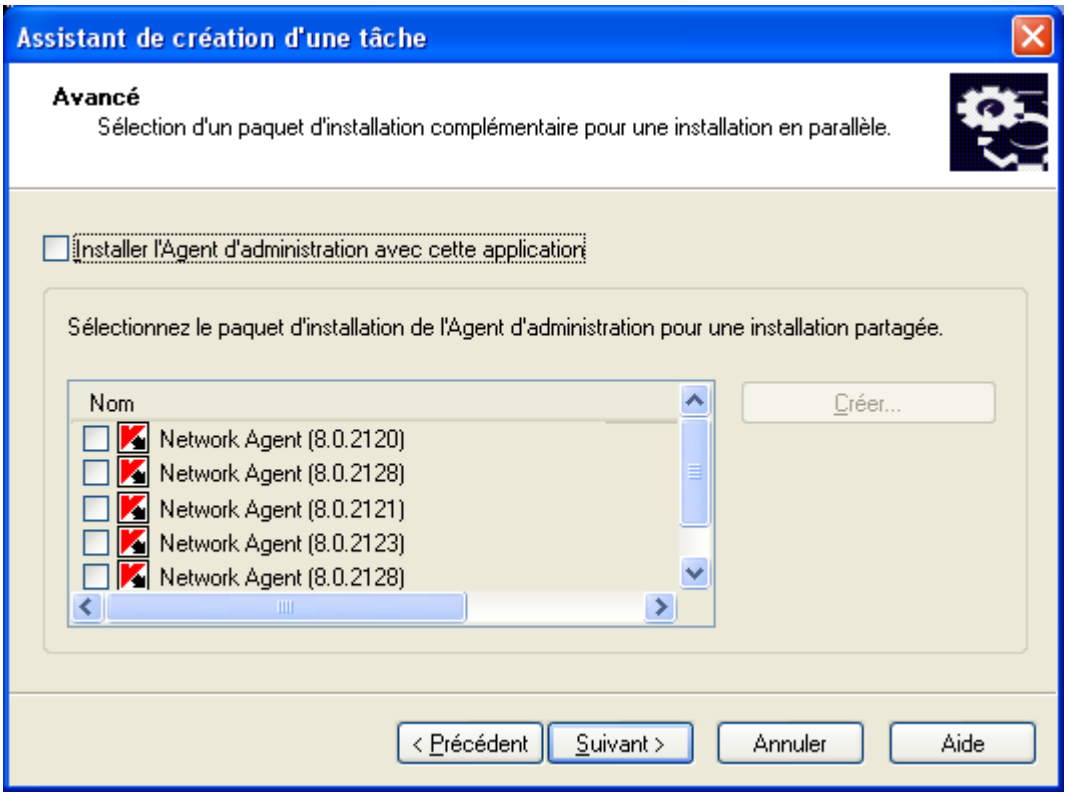


Figure 8 : création d'une tâche Sélection d'un paquet d'installation supplémentaire pour l'installation partagée

10. Sélectionnez l'action à exécuter si après l'installation de l'application il faut redémarrer l'ordinateur (cf. ill. ci-après) :

    - **Ne pas redémarrer l'ordinateur**.
    - **Redémarrer l'ordinateur**.
    - **Confirmer auprès de l'utilisateur** (valeur par défaut).

    Cochez la case **Forcée la fermeture des applications dans les sessions bloquées** si le redémarrage du système d'exploitation nécessite une fermeture forcée des applications actives dans des séances bloquées.

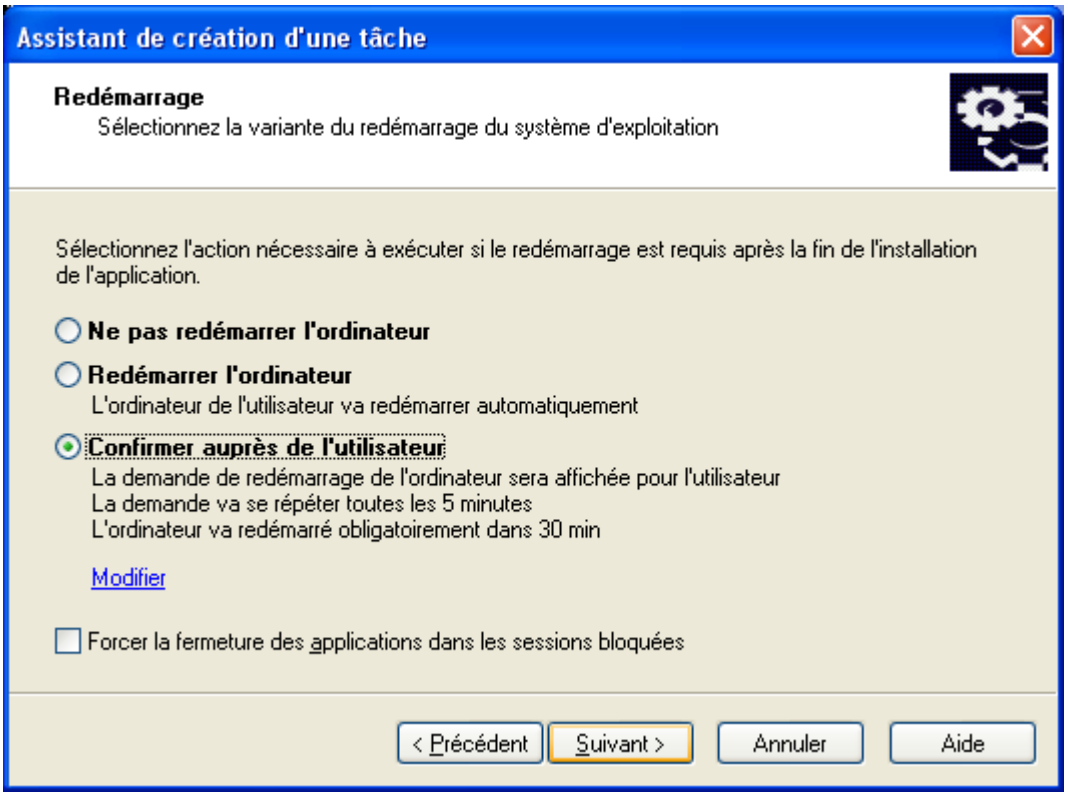


Figure 9 : création d'une tâche Sélection de mode de redémarrage du système

11. Créez une liste des profils d'utilisateurs qui serviront à lancer la tâche d'installation à distance sur les ordinateurs (cf. ill. ci-après).

    Pour ajouter un profil utilisateur à la liste, cliquez sur **Ajouter** et saisissez le nom de l'utilisateur et le mot de passe dans la fenêtre qui s'affiche.

Le profil utilisateur doit avoir les droits d'administrateur sur tous les ordinateurs qui seront utilisés pour l'installation du logiciel à distance. Pour installer le logiciel sur les ordinateurs qui font partie des domaines différents, ces domaines doivent avoir des rapports de confiance avec le domaine du Serveur d'administration.

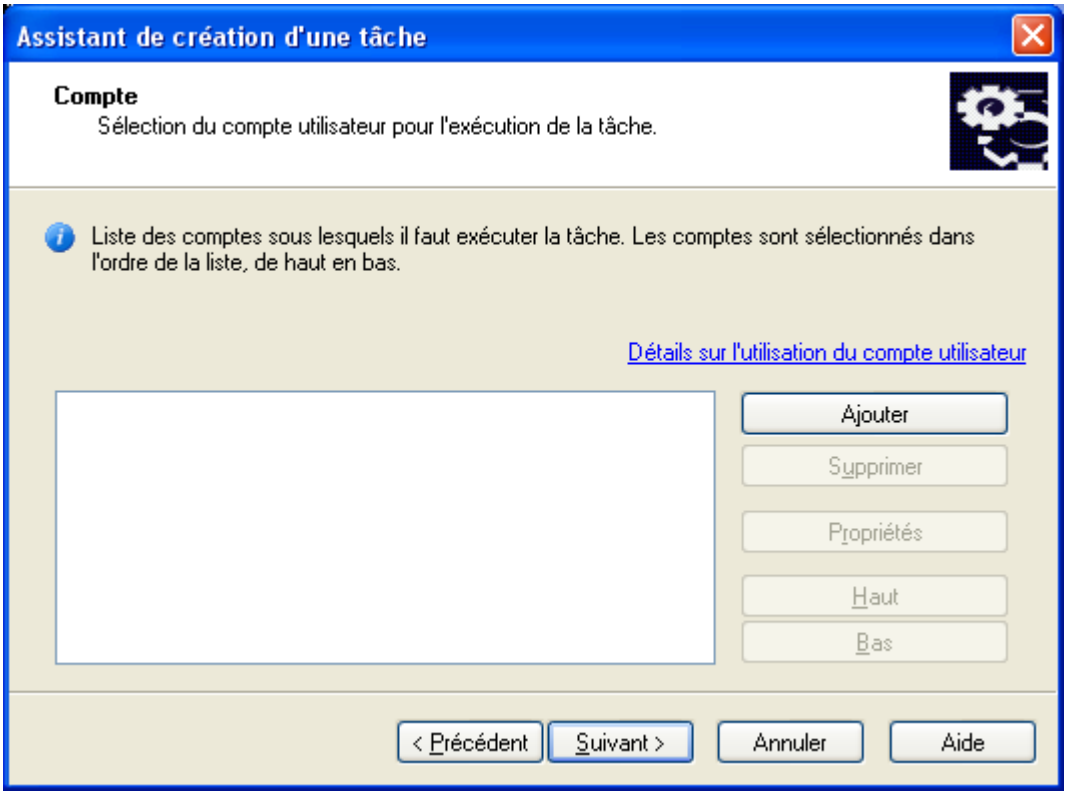


Figure 10 : création d'une tâche Sélection des comptes

12. Configurez l'exécution programmée de la tâche (cf. ill. ci-après) :
    - Dans la liste déroulante **Planification pour** programmez le démarrage de la tâche :
        - **Manuel**
        - **Toutes les N heures**.
        - **Chaque jour**
        - **Chaque semaine**
        - **Chaque mois**.
        - **Une fois** : dans ce cas, le lancement de la tâche d'installation à distance sur les ordinateurs sera réalisé seulement une fois peut importe le résultat de son exécution.
        - **Immédiatement** : démarre la tâche immédiatement après avoir terminé l'Assistant.
        - **À la fin d'une autre tâche** : dans ce cas la tâche d'installation à distance sera lancée seulement à la fin de fonctionnement de la tâche indiquée.
    - Configurez dans le groupe des champs qui correspondent au mode sélectionné les paramètres de planification (pour en savoir plus, consultez le Manuel de référence de Kaspersky Administration Kit).

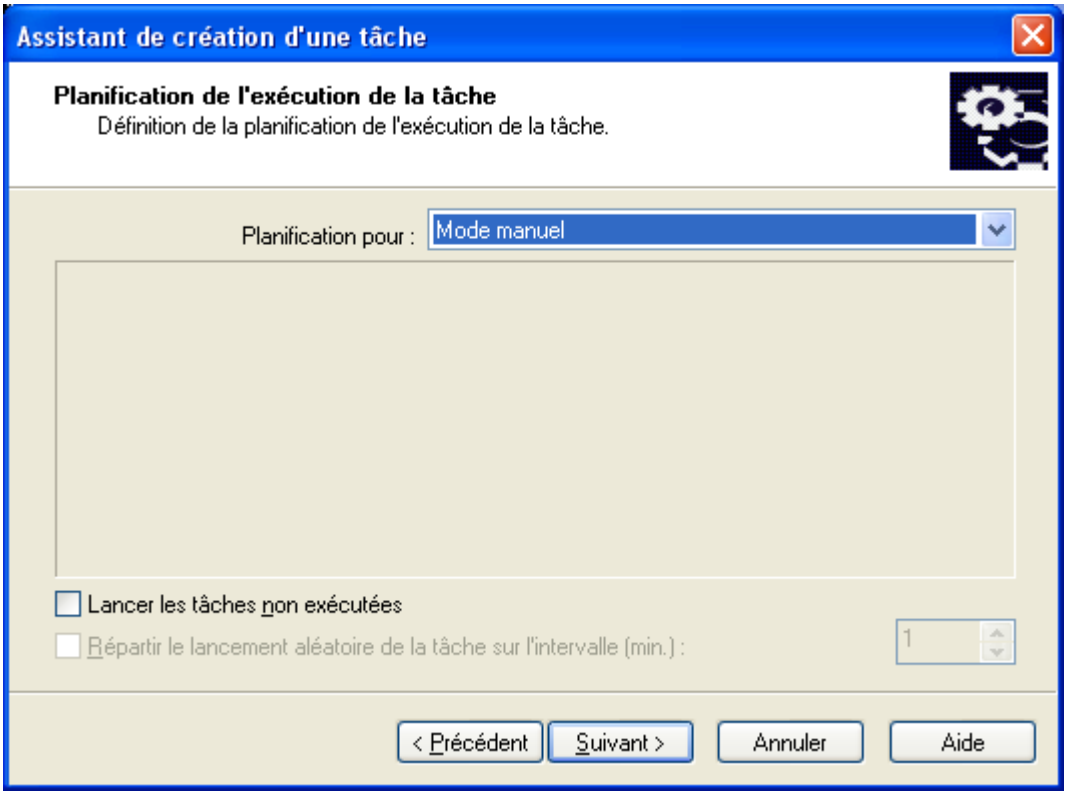


Figure 11 : création d'une tâche Configuration de l'exécution programmée de la tâche

Après la fin de l'Assistant, la tâche que vous venez de créer sera ajoutée aux dossiers **Tâches de groupe** des groupes et sous-groupes correspondants, et affichée dans l'arborescence de la console. La tâche sera lancée en fonction de sa planification, mais vous pouvez toujours lancer la tâche à la main.

- *Pour lancer la tâche d'installation à distance à la main,*

  sélectionnez l'option **Propriétés** dans le menu contextuel de la tâche d'installation à distance. Dans la fenêtre qui s'affiche sous l'onglet **Général** cliquez sur **Démarrer** (cf. ill. ci-après).

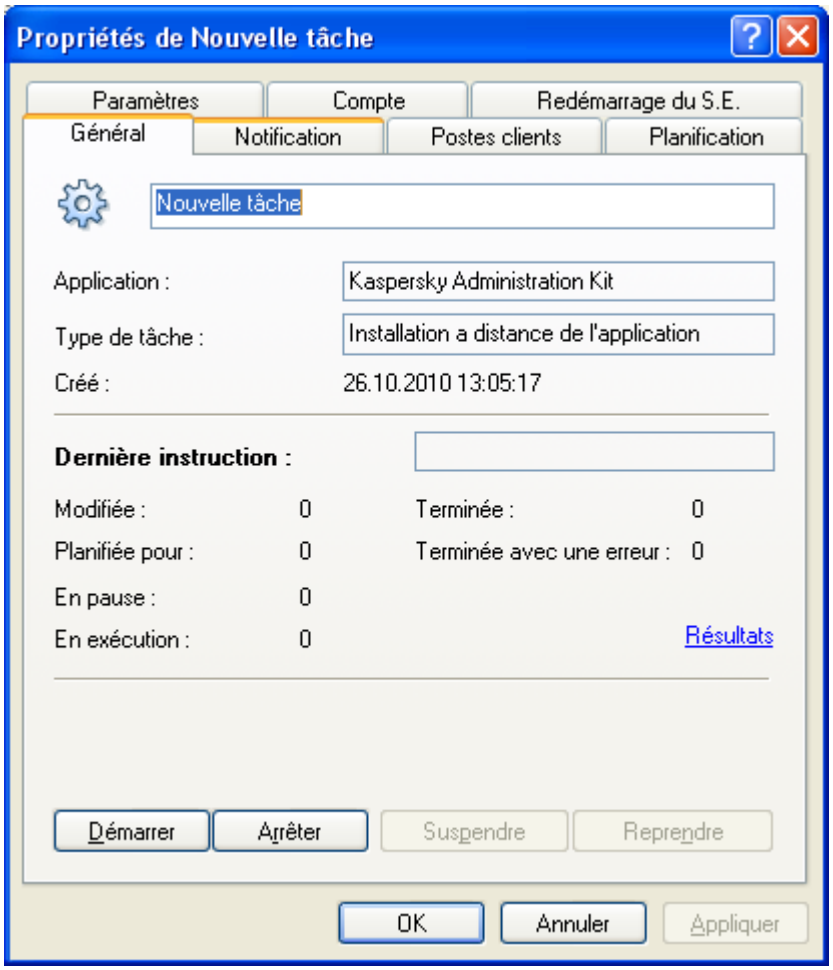


Figure 12 : lancement de l'installation de l'application

TRANSMISSION DE LA DISTRIBUTION DE L'APPLICATION VERS L'APPAREIL MOBILE VIA LE POSTE DE TRAVAIL

La transmission de l'application Kaspersky Endpoint Security 8 for Smartphone vers l'appareil mobile est assurée par l'utilitaire kmlisten.exe, installé sur le poste de travail suite à l'exécution de la tâche d'installation à distance. Au moment de la connexion de l'appareil à l'ordinateur, l'utilitaire invitera l'utilisateur à installer Kaspersky Endpoint Security 8 for Smartphone sur l'appareil mobile connecté.

Pour copier la distribution de l'application Kaspersky Endpoint Security 8 for Smartphone sur l'appareil mobile depuis le poste de travail, l'utilisateur doit procéder comme suit :

1. Connecter l'appareil au poste de travail. Si l'appareil est conforme aux spécifications système d'installation de l'application, la fenêtre **KES 8** (cf. ill. ci-après).

Figure 13: Fenêtre de l'utilitaire kmlisten.exe

2. Sélectionner dans la liste des appareils connectés un ou plusieurs appareils pour y installer l'application.
3. Cliquez sur **Installer**. L'utilitaire transmet la distribution de l'application vers les appareils sélectionnés. Le processus de l'installation de l'application sera automatiquement lancé sur les appareils mobiles sélectionnés.

La fenêtre de **KES 8** affichera l'état de transmission du paquet d'installation de l'application sur les appareils.

La fenêtre de **KES 8** s'affiche à chaque connexion de l'appareil mobile à l'ordinateur.

Pour que l'utilitaire kmlisten.exe n'invite plus à installer l'application à chaque connexion de l'appareil au poste de travail, l'utilisateur doit procéder comme suit :

dans la fenêtre **KES 8**, cochez la case **Interrompre le lancement automatique de l'application pour l'installation de Kaspersky Endpoint Security 8 for Smartphone**.

INSTALLATION DE L'APPLICATION SUR L'APPAREIL MOBILE VIA LE POSTE DE TRAVAIL

Après le téléchargement du paquet d'installation sur l'appareil mobile, l'application sera installée sur l'appareil automatiquement sans aucune intervention de la part de l'utilisateur. Pendant l'installation son état n'est pas affiché sur l'écran de l'appareil.

S'il s'agit de Symbian, l'utilisateur doit intervenir pendant l'installation de l'application. Pour en savoir plus, consultez le Guide de l'utilisateur pour Symbian.

INSTALLATION DE L'APPLICATION PAR UNE DIFFUSION DES MESSAGES ELECTRONIQUES

Si l'application ne peut pas être installée via les postes de travail d'utilisateurs, l'administrateur peut envoyer un message avec l'instruction sur le téléchargement de la distribution de l'application et sur la connexion au Serveur d'administration aux adresses électroniques d'utilisateurs.

Ce message doit contenir les informations suivantes :

- lien sur la distribution de l'application ou pièce jointe avec la distribution de l'application ;
- informations sur les paramètres de connexion de l'application au Serveur d'administration si ces paramètres ne font pas partie de la distribution de Kaspersky Endpoint Security 8 for Smartphone remise à l'administrateur.

DANS CETTE SECTION

CREATION DU MESSAGE AVEC LA DISTRIBUTION DE L'APPLICATION

Pour créer le message avec la distribution de l'application, procédez comme suit :

1. Rédigez un message pour tous les utilisateurs sur les appareils nomades sur lesquels vous avez l'intention d'installer Kaspersky Endpoint Security 8 for Smartphone.
2. Dans le champ d'objet, saisissez le texte "Distribution de l'application Kaspersky Endpoint Security 8 for Smartphone pour installer sur l'appareil mobile".
3. Insérez dans le texte du message le modèle suivant :

   Cher utilisateur de l'appareil mobile,

   Ce message contient la distribution de Kaspersky Endpoint Security 8 for Smartphone et les informations sur les paramètres de connexion de l'application au système d'administration distante.

   Pour installer Kaspersky Endpoint Security 8 for Smartphone veuillez télécharger le fichier d'installation <nom du fichier> sur votre appareil mobile. (Le fichier d'installation de l'application est joint au message. / Le fichier d'installation de l'application est accessible via <lien vers le fichier d'installation>.)

   Si vous avez reçu ce message sur votre appareil mobile, téléchargez le fichier d'installation (joint au message, / en cliquant sur le lien dans le corps du message) et enregistrez-le sur votre appareil. Si vous avez reçu ce message sur votre poste de travail, téléchargez le fichier d'installation sur l'appareil avec l'application qui assure l'échange de données entre l'appareil mobile et l'ordinateur. Ensuite, lancez le fichier d'installation que vous avez téléchargé et effectuez l'installation de l'application en suivant les instructions de l'assistant d'installation.

   Pendant l'installation l'assistant vous invitera à saisir les valeurs des paramètres suivants :

   Serveur : saisissez l'adresse <adresse du serveur d'administration> dans le champ.

   Port : saisissez le port <numéro du port du serveur d'administration> dans le champ.

   Groupe : saisissez le groupe <nom du groupe> dans le champ.

   Votre adresse élec. : saisissez l'adresse électronique de votre société.

   L'adresse de courrier électronique sert à enregistrer l'appareil dans le système d'administration à distance. N'oubliez pas qu'il est impossible de modifier l'adresse indiquée lors de l'installation de l'application.

   Si vous avez constaté des erreurs pendant l'installation de l'application, contactez l'administrateur.

   Le texte entre parenthèses divisé par une barre oblique signifie que vous devez sélectionner un des deux modes de téléchargement du fichier d'installation : depuis la pièce jointe du message ou depuis le lien et formuler les instructions appropriées dans le texte du message.

4. Remplacez le texte entre parenthèses par des valeurs appropriées des paramètres suivants :

- <nom du fichier> : nom du fichier d'installation pour le système d'exploitation installé sur l'appareil de l'utilisateur. Par exemple, si l'appareil mobile de l'utilisateur tourne sous le système d'exploitation Microsoft Windows Mobile, il faut spécifier le fichier d'installation avec l'extension CAB.
- <lien vers le fichier d'installation> : lien vers le fichier d'installation pour le système d'exploitation installé sur l'appareil de l'utilisateur. Le fichier d'installation doit être placé d'avance sur un serveur FTP- / HTTP qui peut être accédé via Internet. Si pour une raison ou une autre il est impossible de placer le fichier d'installation sur un serveur FTP- / HTTP, vous pouvez joindre le fichier d'installation à la lettre.
- <adresse du serveur d'installation> : adresse IP ou nom DNS du serveur d'administration auquel les appareils mobiles seront connectés. L'adresse du serveur doit être spécifiée dans le format qui est utilisé pour les propriétés du Serveur d'administration sous l'onglet **Général** dans le champ **Adresse**. En d'autres termes, si dans les propriétés du Serveur d'administration une adresse IP est indiquée, saisissez la même adresse IP dans le texte du message. Si dans les propriétés du Serveur d'administration un nom DNS est indiqué, saisissez le même nom DNS dans le texte du message.
- <numéro du port du serveur d'administration> : numéro du port ouvert sur le serveur d'administration pour la connexion des appareils mobiles. Le numéro de port par défaut est 13292.
- <nom du groupe> par le nom du groupe auquel seront ajoutés automatiquement les appareils mobiles après la première synchronisation avec le Serveur d'administration. Par défaut, les appareils sont ajoutés au groupe qui porte le nom KES8.

Si les paramètres de connexion des appareils mobiles au Serveur d'administration font partie de la distribution de Kaspersky Endpoint Security 8 for Smartphone qui vous a été remise, demandez dans le texte du message uniquement les adresses électroniques d'utilisateurs. Il ne faut pas spécifier les paramètres de connexion avec le Serveur d'administration.

5. Si pour une raison ou une autre vous ne pouvez pas placer le fichier d'installation sur un serveur FTP- / HTTP, joignez-le au message.
6. Envoyez le message. Une fois le message envoyé, assurez-vous qu'il a été reçu par tous les destinataires.

INSTALLATION DE L'APPLICATION SUR L'APPAREIL MOBILE APRES LA RECEPTION DU MESSAGE ELECTRONIQUE

Après la réception du message avec la distribution envoyé par l'administrateur, l'utilisateur télécharge la distribution sur son appareil avec l'une des méthodes recommandées. La distribution de l'application contient le fichier d'installation pour le système d'exploitation installé sur l'appareil de l'utilisateur. L'utilisateur ouvre le fichier d'installation qui lance automatiquement l'assistant d'installation de l'application sur l'appareil.

Pendant le processus de l'installation, l'assistant invitera l'utilisateur à saisir un code secret pour l'application et à spécifier les paramètres de connexion de l'application au système d'administration distante s'ils ne font pas partie de la distribution de Kaspersky Endpoint Security 8 for Smartphone. Une fois les valeurs appropriées des paramètres saisies, l'installation se termine automatiquement. Pour en savoir plus sur l'installation de l'application, consultez le Guide de l'utilisateur de Kaspersky Endpoint Security 8 for Smartphone.

INSTALLATION DE LA LICENCE VIA KASPERSKY ADMINISTRATION KIT

La particularité de l'installation de la licence pour l'application Kaspersky Endpoint Security 8 for Smartphone est que cette licence est transmise vers l'appareil avec la stratégie pendant la synchronisation de l'appareil avec le Serveur d'administration. Pendant les trois jours qui suivent l'installation de l'application, l'appareil établit une connexion automatique avec le serveur d'administration toutes les trois heures. Après la mise en place de la stratégie, l'appareil effectue la synchronisation avec le Serveur d'administration avec une fréquence définie dans les paramètres de réseau pendant la création de la stratégie (cf. la rubrique "Création de la stratégie" à la page 45). La fréquence par défaut est toutes les 6 heures.

Pour effectuer l'activation de l'application, l'administrateur doit créer une stratégie pour le groupe dont l'appareil fait partie et ajouter une licence à cette stratégie. Lorsque la fois prochaine l'appareil mobile établira une connexion avec le Serveur d'administration, la licence sera téléchargée sur l'appareil mobile avec la stratégie et l'application installée sur l'appareil sera activée.

Si les fonctionnalités de l'application sont limitées, elle arrête d'effectuer une synchronisation automatique avec le Serveur d'administration. Voilà pourquoi si pour une raison ou une autre l'activation de l'application n'a pas été effectuée dans les 3 qui ont suivi l'installation, l'utilisateur doit effectuer la synchronisation avec le Serveur d'administration à la main (voir le Guide de l'utilisateur de Kaspersky Endpoint Security 8 for Smartphone).

Il faut obligatoirement activer l'application dans les trois jours qui suivent l'installation de Kaspersky Endpoint Security 8 for Smartphone sur les appareils mobiles. Si l'application n'est pas activée, ses fonctionnalités seront limitées. Dans ce mode de fonctionnement, la plupart de composants de Kaspersky Endpoint Security 8 for Smartphone sont désactivés.

UTILISATION DES STRATEGIES

Tous les paramètres de fonctionnement de l'application y compris la licence, la planification des mises à jour des bases de l'application, la planification des analyses de l'appareil sont définis via la stratégie ou les paramètres locaux de l'application. Les stratégies permettent de définir les mêmes valeurs des paramètres de fonctionnement de l'application pour tous les appareils mobiles du groupe. Pour en savoir plus sur les stratégies et les groupes d'administration, consultez le Guide de l'administrateur de Kaspersky Administration Kit.

Chaque paramètre, présenté dans la stratégie, a pour attribut : le "verrouille" qui affiche, s'il est interdit de modifier le paramètre dans les stratégies du niveau intégré de la hiérarchie (pour les groupes intégrés et pour les Serveurs d'administration secondaires) et dans les paramètres locaux de l'application.

Si un paramètre de la stratégie est "verrouillé", après l'application de la stratégie pour les appareils mobiles ils vont utiliser les valeurs définies par la stratégie. Dans ce cas, l'utilisateur de l'appareil mobile ne pourra pas modifier ces valeurs. Pour les paramètres non "verrouillés", l'appareil mobile utilisera les valeurs locales définies par défaut ou par l'utilisateur lui-même.

Les informations relatives aux paramètres de l'application définis dans les stratégies sont enregistrées sur le Serveur d'administration et diffusées sur les appareils mobiles lors de la synchronisation. Dans ce cas, dans les données du Serveur d'administration sont à leur tour ajoutées les modifications locales effectuées sur les appareils mobiles et autorisées par la stratégie.

Vous pouvez modifier les paramètres du fonctionnement de l'application sur un appareil mobile spécifique à l'aide des paramètres locaux de l'application (cf. la rubrique "Configuration des paramètres locaux de l'application" à la page 59), si la stratégie actuelle autorise leur modification.

DANS CETTE SECTION

CREATION D'UNE STRATEGIE

➧ *Pour créer une stratégie, procédez comme suit :*

1. Connectez-vous au serveur d'administration.
2. Dans l'arborescence de la console, sélectionnez le groupe pour lequel vous souhaitez créer une stratégie.
3. Sélectionnez le sous-dossier **Stratégie**, qui fait partie du groupe.
4. Ouvrez le menu contextuel et sélectionnez l'option **Créer** → **Stratégie**, ou cliquez sur le lien **Créer une nouvelle stratégie** dans la barre des tâches. Cette action lance un Assistant. Suivez les instructions de l'Assistant.
5. Spécifiez le nom de la stratégie et sélectionnez **Kaspersky Endpoint Security 8 for Smartphone** en tant qu'application pour laquelle cette stratégie est créée.

   La saisie du nom se fait d'une manière standard. Si vous spécifiez un nom de la stratégie qui existe déjà, ce nom sera automatiquement suivi d'un **(1)**.

   Les applications sont sélectionnées dans la liste déroulante (cf. ill. ci-après). La liste déroulante inclut toutes les applications de la société qui possèdent un plug-in de console installé sur le poste administrateur.

   Vous ne pouvez créer la stratégie pour l'application Kaspersky Endpoint Security 8 for Smartphone que si le

plug-in de gestion de cette application est installé sur le poste de travail de l'administrateur. Si le plug-in n'est pas installé, le nom de l'application ne sera pas affiché dans la liste des applications.

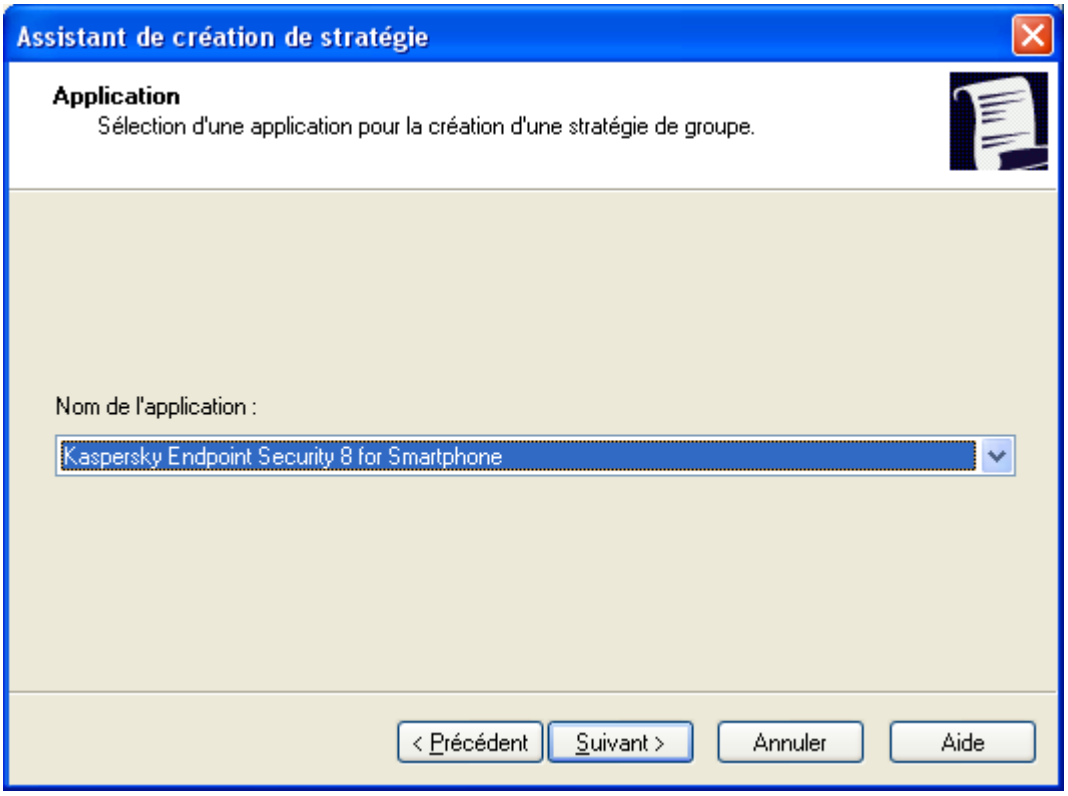


Figure 14 : sélection de l'application pour la création d'une stratégie.

6. Spécifiez l'état de la stratégie (cf. ill. ci-après). Pour ce faire, choisissez une des options suivantes :

   - **Stratégie active**. Dans ce cas, la stratégie créée est enregistrée sur le Serveur d'administration et sera utilisée pour l'application en tant que stratégie active.
   - **Stratégie inactive**. Dans ce cas, la stratégie créée est enregistrée sur le Serveur d'administration en tant que stratégie de sauvegarde et peut être activée par l'événement. Le cas échéant, la stratégie inactive peut être activée (pour en savoir plus sur les états des stratégies, consultez le Manuel de référence de Kaspersky Administration Kit).

Il est possible de créer de nombreuses stratégies pour une application, mais une seule d'entre elles peut être celle active. En cas de création d'une nouvelle stratégie active, la stratégie précédente devient inactive automatiquement.

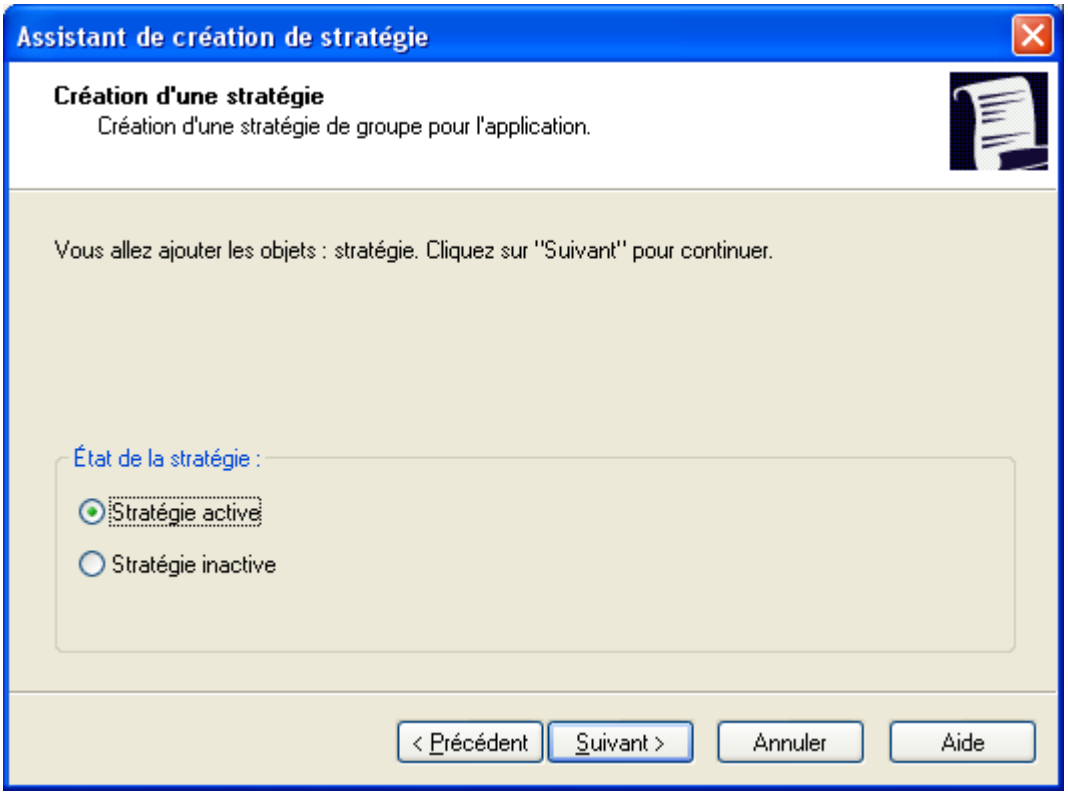


Figure 15 : activation de la stratégie

7. Définissez les paramètres de l'analyse à la demande (cf. la rubrique "Analyse à la demande" à la page 15). Pendant la création de la stratégie, vous pouvez configurer les paramètres suivants (cf. ill. ci-après) :

   - activer/désactiver l'analyse des fichiers exécutables ;
   - activer/désactiver l'analyse des archives ;
   - activer/désactiver la réparation des objets infectés ;
   - configurer l'analyse programmée de tout le système de fichier de l'appareil.

   Kaspersky Endpoint Security 8 for Smartphone analyse par défaut tous les fichiers stockés sur l'appareil et sur la carte mémoire. En cas de détection d'un objet infecté, l'application tente de le réparer. S'il est impossible de réparer l'objet, l'application le place en quarantaine. Les paramètres sont décrits dans la section " Paramètres de la fonction Analyse à la demande " (cf. section " Paramètres de la fonction Analyse à la demande " à la page 60).

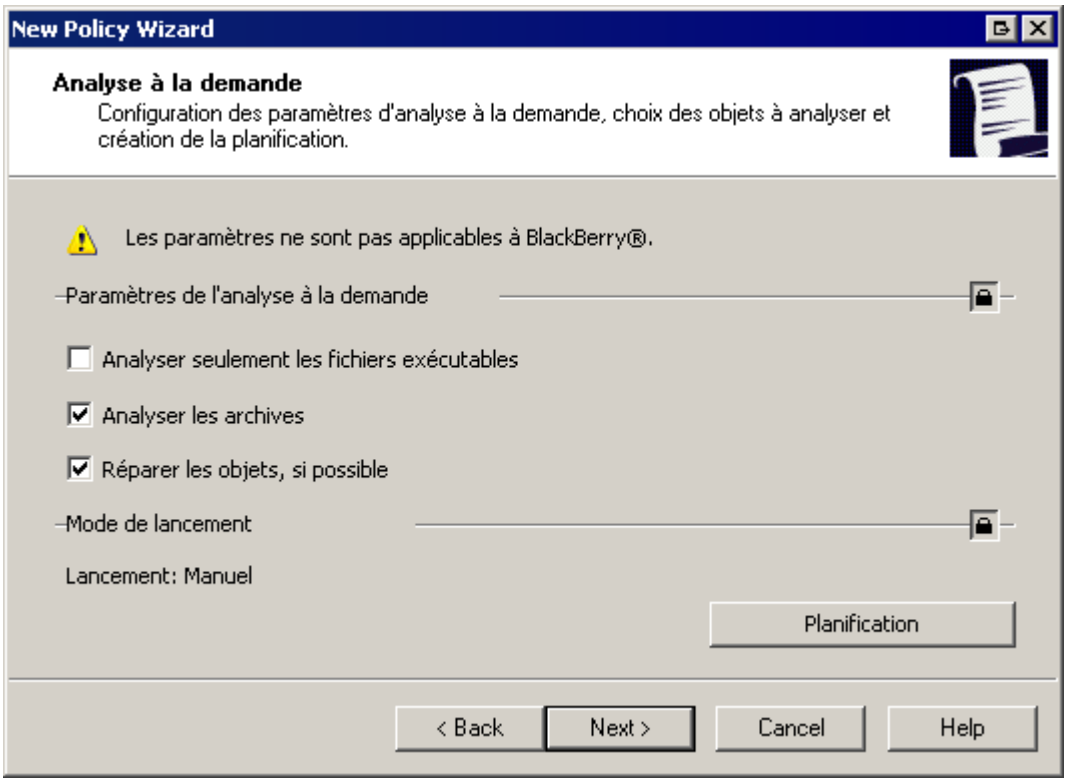


Figure 16 : configuration des paramètres du composant Analyse à la demande

8. Définissez les paramètres du composant Protection (à la page 14). Pendant la création de la stratégie, vous pouvez configurer les paramètres suivants (cf. ill. ci-après) :

   - activer/désactiver le composant Protection sur les appareils mobiles d'utilisateurs ;
   - activer/désactiver l'analyse des fichiers exécutables ;
   - sélectionner l'action sur les objets infectés.

   Par défaut, le composant Protection est activé et analyse tous les types de fichiers auxquels l'utilisateur de l'appareil souhaite accéder. En cas de détection d'un objet infecté, l'application tente de le réparer. Si la réparation s'avère impossible, l'application place l'objet dans un répertoire de quarantaine. Les paramètres sont décrits dans la section " Paramètres de la fonction Protection " (cf. section " Paramètres de la fonction Protection " à la page 63).

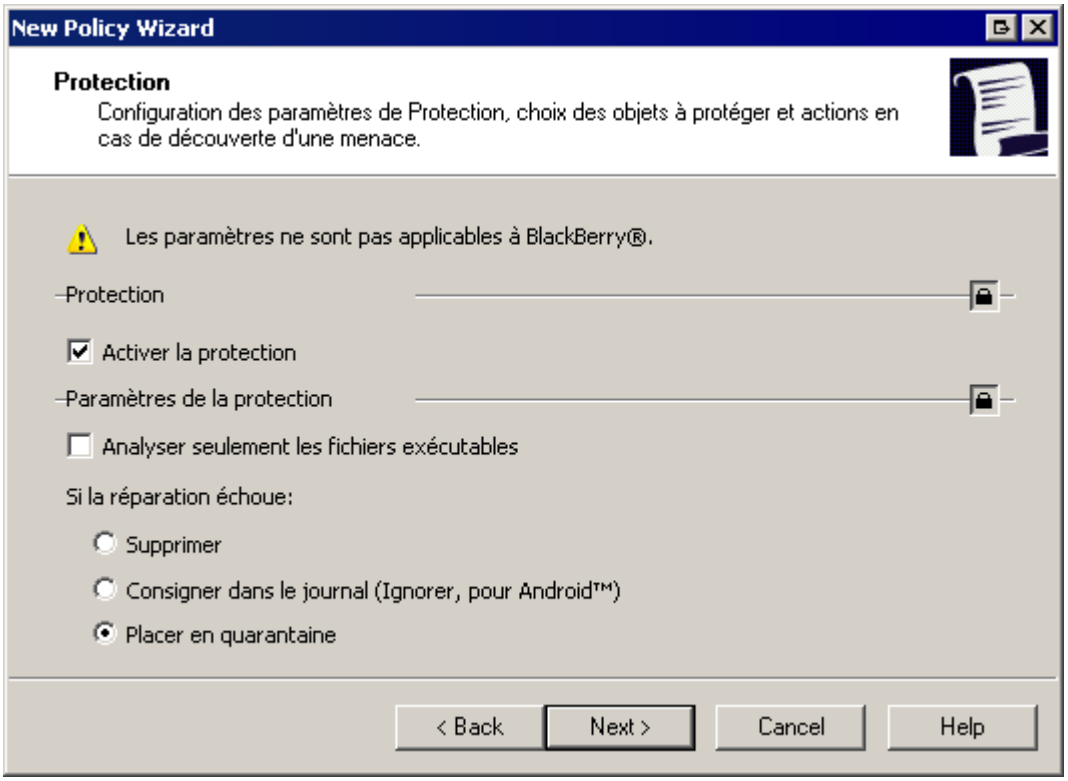


Figure 17 : configuration des paramètres du composant Protection

9. Configurez les paramètres de la mise à jour des bases de l'application : sélectionnez la source des mises à jour et configurez la planification des mises à jour (cf. ill. ci-après). Spécifiez s'il faut effectuer la mise à jour lorsque les appareils d'utilisateurs sont en itinérance. La source de mise à jour par défaut est les serveurs de mises à jour de Kaspersky Lab. Le lancement des mises à jour est effectué par l'utilisateur de l'appareil mobile à la main. La mise à jour en itinérance n'est pas effectuée. Les paramètres sont décrits dans la section " Paramètres de la fonction Mise à jour " (cf. section " Paramètres de la fonction Mise à jour " à la page 65).

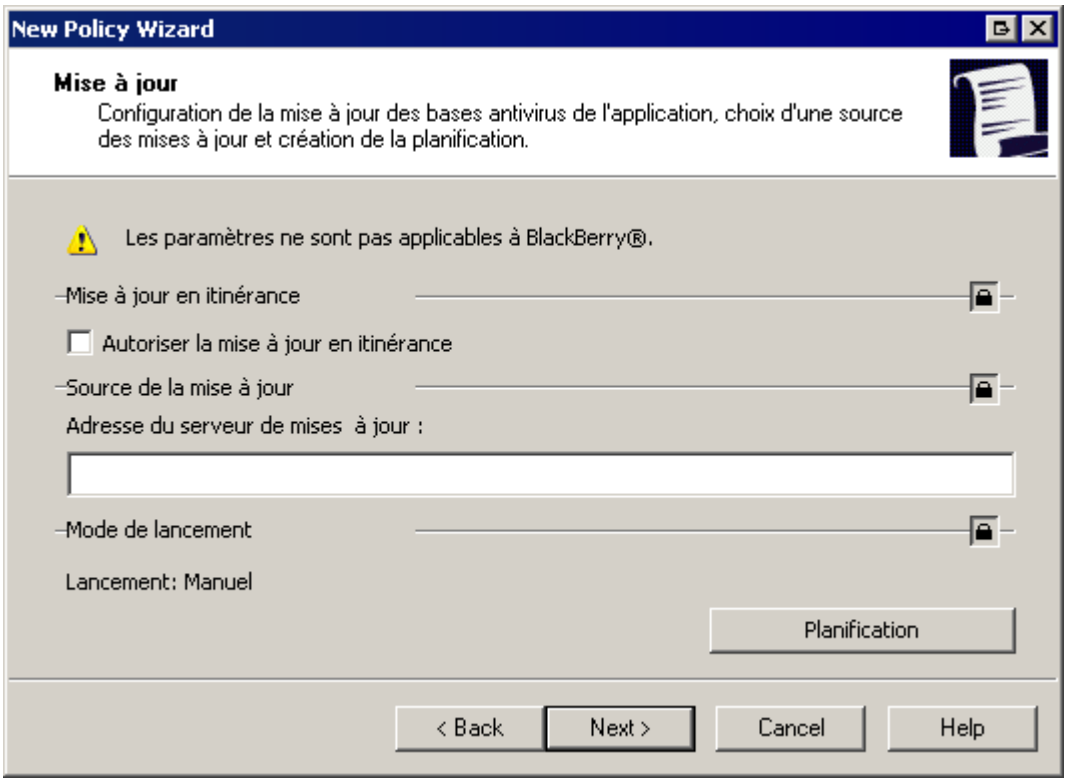


Figure 18 : sélection de la source des mises à jour

10. Définissez les paramètres du composant Antivol (à la page 16). Spécifiez les fonctions du composant qui seront accessibles sur les appareils d'utilisateurs et configurez les paramètres des fonctions sélectionnées (cf. ill. ci-après). Par défaut, toutes les fonctions du composant Antivol sont désactivées. Les paramètres sont décrits dans la section " Paramètres du composant Antivol " (cf. section " Paramètres du composant Antivol " à la page 66).

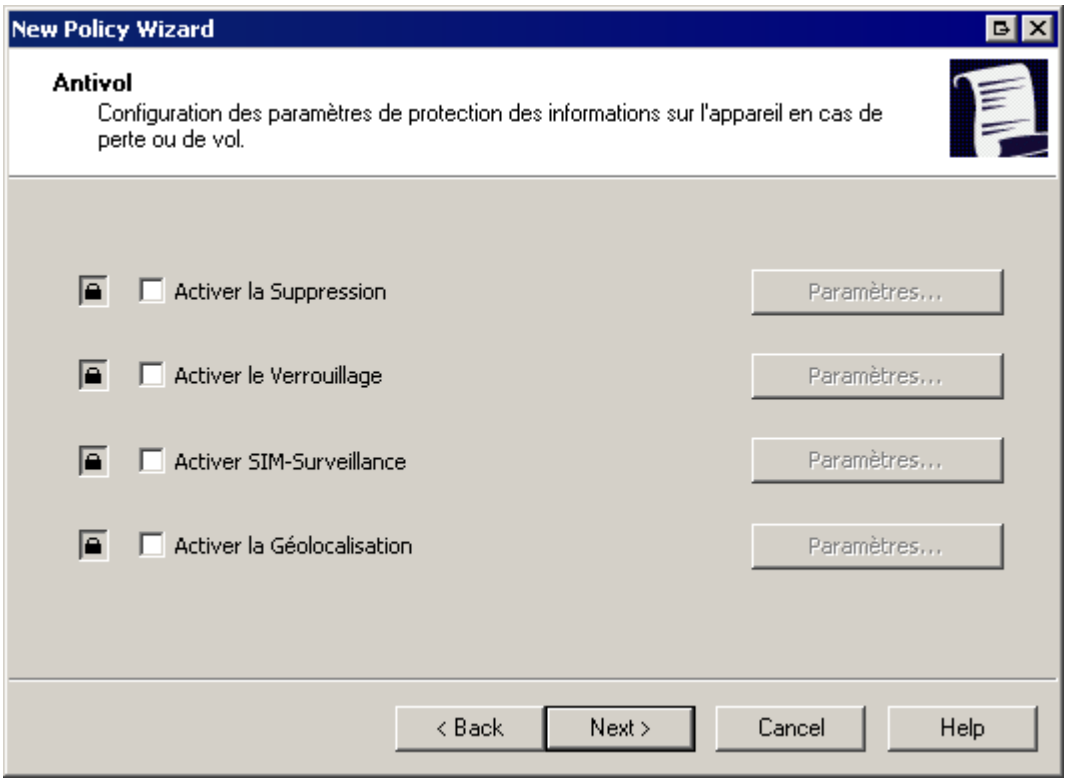


Figure 19 : configuration des paramètres du composant Antivol

11. Définissez les paramètres de synchronisation des appareils mobiles avec le Serveur d'administration (cf. ill. ci-après) et le mode de fonctionnement du composant Pare-feu (à la page 18). Par défaut, l'appareil mobile fait une tentative de connexion au Serveur d'administration toutes les 6 heures. Par défaut, le composant Pare-feu est désactivé. Les paramètres sont décrits dans la section " Paramètres du composant Pare-feu " (cf. section " Paramètres du composant Pare-feu " à la page 71).

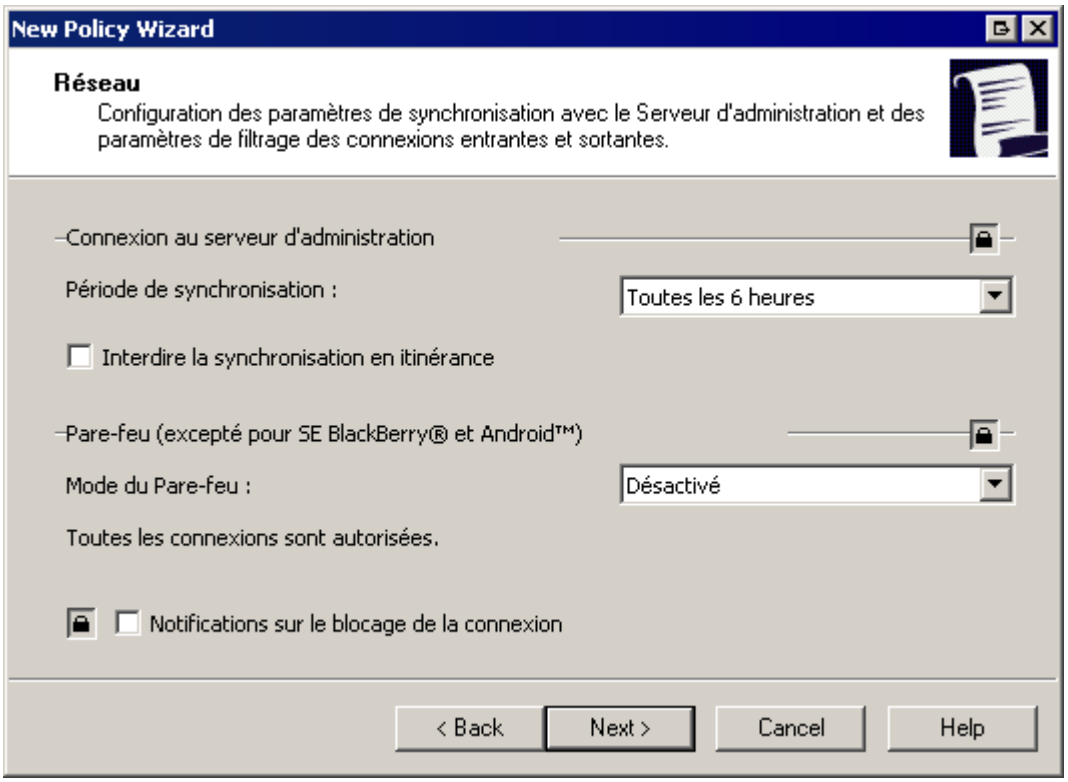


Figure 20 : configuration du réseau

12. Définissez les paramètres des composants Anti-Spam (à la page 17), Contacts personnels (à la page 17) et Chiffrement (à la page 18). Spécifiez les composants qui seront utilisables sur les appareils mobiles d'utilisateurs et configurez les paramètres du composant Chiffrement (cf. ill. ci-après). Par défaut, l'utilisateur est autorisé à utiliser les composants Anti-Spam et Contacts personnels. Les paramètres des composants Anti-Spam et Contacts personnels doivent être configurés par les utilisateurs des appareils mobiles. Les paramètres sont décrits dans les sections " Paramètres des composants Anti-Spam et Contacts personnels " (cf. section " Paramètres des composants Anti-Spam et Contacts personnels " à la page 74) et " Paramètres du composant Chiffrement " (cf. section " Paramètres du composant Chiffrement " à la page. 75).

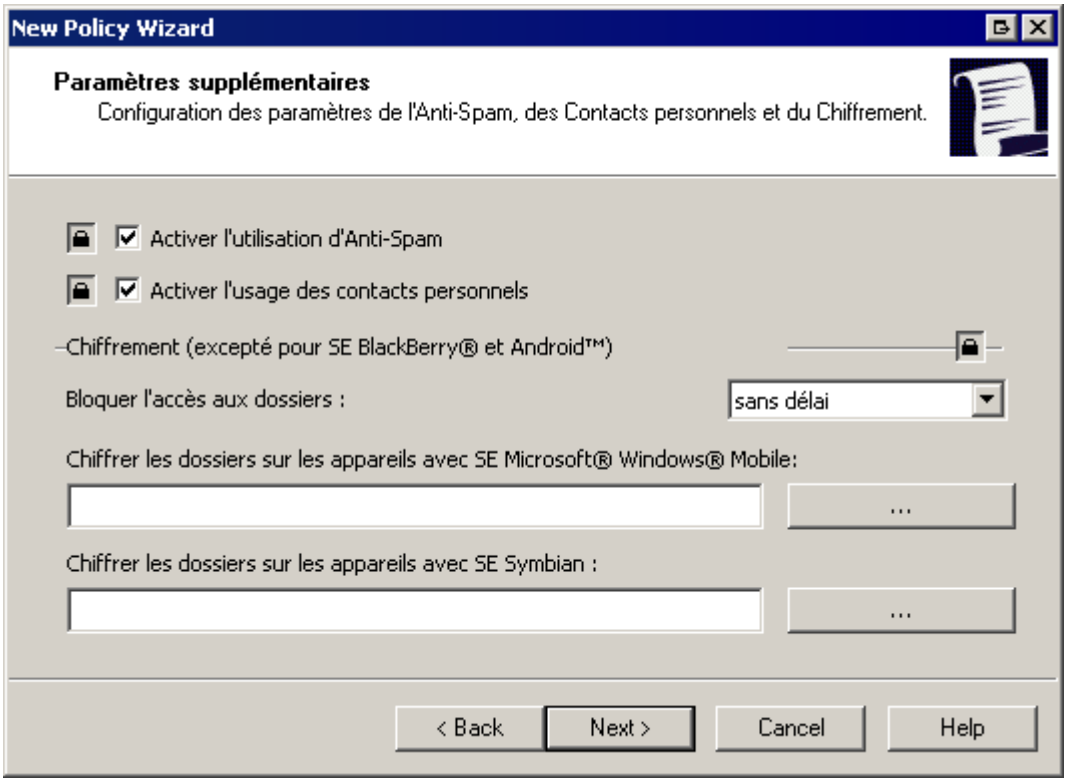


Figure 21 : configuration des paramètres complémentaires

13. Spécifiez la licence qui sera installée sur les appareils mobiles pour activer l'application (cf. ill. ci-après).

Il faut obligatoirement activer l'application dans les trois jours qui suivent l'installation de Kaspersky Endpoint Security 8 for Smartphone sur les appareils mobiles. Si l'application n'est pas activée, ses fonctionnalités seront limitées automatiquement. Dans ce mode de fonctionnement, la plupart de composants de Kaspersky Endpoint Security 8 for Smartphone sont désactivés.

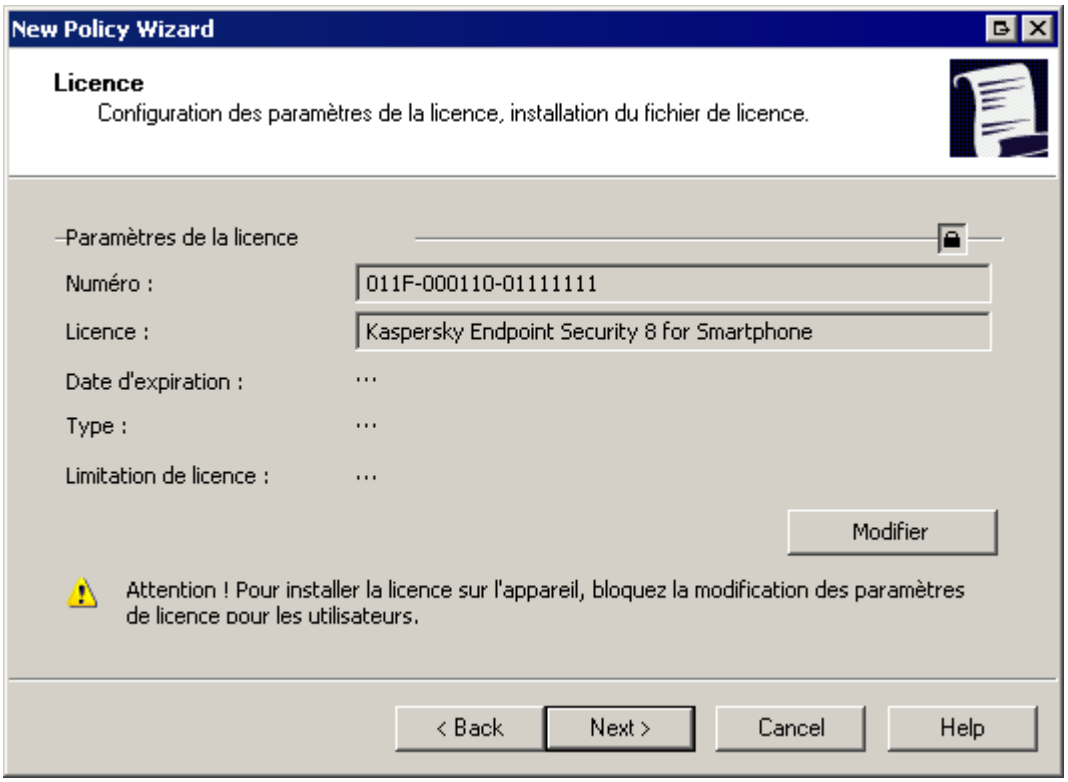


Figure 22 : sélection du fichier de licence pour l'activation de la licence

Cliquez sur **Modifier** et sélectionnez dans la fenêtre qui s'affiche le fichier de licence pour installer la licence. Ensuite, la fenêtre de l'assistant affiche les informations sur la licence :

- numéro de la licence ;
- nom de la licence ;
- date de fin de validité de la licence ;
- type de la licence installée (par exemple, commerciale ou évaluation) ;
- restrictions définies dans la licence.

Assurez-vous que le "cadenas" qui s'affiche sur le bouton dans le coin supérieur droit est fermé – . Si le "cadenas" est ouvert, l'installation de la licence sur les appareils mobiles ne sera pas effectuée.

14. Cliquez sur **Terminer** pour fermer l'assistant de création de la stratégie.

Après la fermeture de l'assistant, la stratégie pour Kaspersky Endpoint Security 8 for Smartphone sera ajoutée au dossier **Stratégie** du groupe d'administration approprié et affichée dans la barre des tâches.

La stratégie sera diffusée sur les appareils mobiles pendant leur synchronisation avec le Serveur d'administration immédiatement après l'ajout de l'appareil mobile dans le groupe d'administration du noeud **Ordinateurs administrés** (cf. la rubrique "**Déplacement des appareils dans le groupe Ordinateurs administrés**" à la page 55).

CONFIGURATION DES PARAMETRES DE LA STRATEGIE

Après la création de la stratégie, vous pouvez modifier les paramètres de l'application via les propriétés de la stratégie. Pendant la modification des paramètres, vous pouvez utiliser le bouton pour autoriser / interdire la modification des paramètres sur l'appareil mobile.

Pour apporter des modifications à une stratégie, procédez comme suit :

1. Connectez-vous au Serveur d'administration.
2. Sélectionnez dans l'arborescence de la console dans le dossier **Ordinateurs administrés** le groupe d'administration dont les appareils mobiles font partie.
3. Sélectionnez le dossier **Stratégies** qui fait partie du groupe. Toutes les stratégies créées pour le groupe seront affichées dans la barre des résultats.
4. Sélectionnez dans la liste des stratégies la stratégie pour Kaspersky Endpoint Security 8 for Smartphone dont les paramètres vous souhaitez modifier.
5. Sélectionnez dans le menu contextuel de la stratégie l'option **Propriétés**. La fenêtre de configuration de la stratégie s'ouvre et présente plusieurs onglets.
6. Définissez les valeurs requises pour les paramètres des composants de l'application sous les onglets **Analyse** (cf. section " **Paramètres de la fonction Analyse à la demande** " à la page 60), **Protection** (cf. section " **Paramètres de la fonction Protection** " à la page 63), **Mise à jour** (cf. section " **Paramètres de la fonction Mise à jour** " à la page 65), **Antivol** (cf. section " **Paramètres du composant Antivol** " à la page 66), **Réseau** (cf. section " **Paramètres de synchronisation des appareils avec le Serveur d'administration** " à la page 73), **Avancé** et **Licence**. Les onglets **Général** et **Evénements** sont typiques pour l'application Kaspersky Administration Kit (pour en savoir plus, consultez le Guide de l'Administrateur de Kaspersky Administration Kit). Les autres onglets contiennent les paramètres de l'application Kaspersky Endpoint Security 8 for Smartphone.
7. Cliquez sur **Appliquer** ou sur **OK**.

MISE EN PLACE DE LA STRATEGIE

Pendant la synchronisation des appareils mobiles avec le Serveur d'administration, les paramètres de l'application définis dans la stratégie sont transmis vers tous les appareils du groupe. La licence pour activer l'application est copiée sur les appareils mobiles en même temps que les paramètres de l'application.

Si le paramètre dans la stratégie est "verrouillé" l'utilisateur ne pourra pas modifier la valeur de ce paramètre sur l'appareil mobile. L'utilisateur est libre de redéfinir tous les autres paramètres du fonctionnement de l'application.

Les paramètres modifiés par l'utilisateur sont transmis vers le Serveur d'administration à la prochaine synchronisation et sont enregistrés sur le Serveur d'administration dans les paramètres locaux de l'application (cf. la rubrique "Configuration des paramètres locaux de l'application" à la page 59).

DEPLACEMENT DES APPAREILS DANS LE GROUPE ORDINATEURS ADMINISTRES

Pendant la première synchronisation des appareils mobiles avec le Serveur d'administration, les appareils sont automatiquement mis dans le groupe du noeud **Ordinateurs non répartis** (par défaut, ce groupe porte le nom KES8). Pendant que les appareils se trouvent dans ce groupe, la gestion centralisée des paramètres des applications de Kaspersky Endpoint Security 8 for Smartphone installées sur ces appareils est impossible.

Pour pouvoir gérer les applications de Kaspersky Endpoint Security 8 for Smartphone installé sur les appareils mobiles à l'aide des stratégies, l'administrateur doit déplacer les appareils depuis le groupe du noeud **Ordinateurs non répartis** dans le groupe déjà créé **Ordinateurs administrés** (cf. la rubrique "**Création de groupes**" à la page 29).

L'administrateur peut déplacer les appareils mobiles dans le groupe du noeud **Ordinateurs administrés** à la main ou configurer le déplacement automatique des appareils dans le groupe indiqué.

DANS CETTE SECTION

DEPLACEMENT MANUEL DE L'APPAREIL DANS LE GROUPE

*Pour déplacer manuellement les appareils mobiles dans le groupe du noeud **Ordinateurs administrés**, procédez comme suit :*

1. Connectez-vous au Serveur d'administration.
2. Sélectionnez dans l'arborescence de la console le noeud **Ordinateurs non répartis**.
3. Sélectionnez le groupe où les appareils mobiles ont été ajoutés automatiquement pendant la synchronisation avec le Serveur d'administration (par défaut, il s'agit de KES8).
4. Sélectionnez dans le groupe l'appareil qu'il faut déplacer dans le groupe du noeud **Ordinateurs administrés**.
5. Ouvrez le menu contextuel et sélectionnez l'option **Déplacer dans le groupe**. La fenêtre **Sélectionnez le groupe** s'affiche (cf. ill. ci-après).

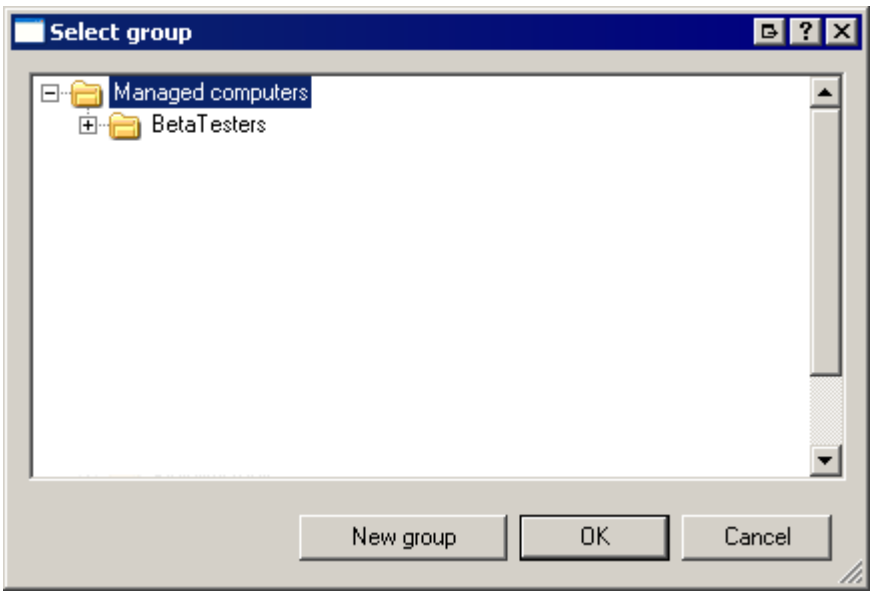


Figure 23 : sélection du groupe

6. Ouvrez le noeud **Ordinateurs administrés**, sélectionnez le groupe où il faudra déplacer l'appareil. Vous pouvez sélectionner le groupe que vous avez créé pendant la préparation à l'installation (cf. la rubrique "Création de groupes" à la page 29) ou créer un nouveau groupe.

   Pour créer un nouveau groupe, sélectionnez dans le nœud **Ordinateurs administrés** un groupe pour y créer le groupe et cliquez sur **Créer un groupe**. Saisissez ensuite le nom du groupe créé.

7. Cliquez sur le bouton **OK**. L'appareil mobile est déplacé dans le groupe sélectionné.

CONFIGURATION DU DEPLACEMENT AUTOMATIQUE DES APPAREILS DANS LE GROUPE

*Pour configurer le déplacement automatique des appareils dans le groupe du nœud **Ordinateurs administrés**, procédez comme suit :*

1. Sélectionnez dans l'arborescence de la console le Serveur d'administration auquel les appareils mobiles sont connectés.
2. Ouvrez le menu contextuel du serveur et sélectionnez l'option **Propriétés**. La fenêtre de configuration des paramètres du Serveur d'administration s'affiche.
3. Ouvrez l'onglet **Déplacement des ordinateurs** (cf. ill. ci-après).

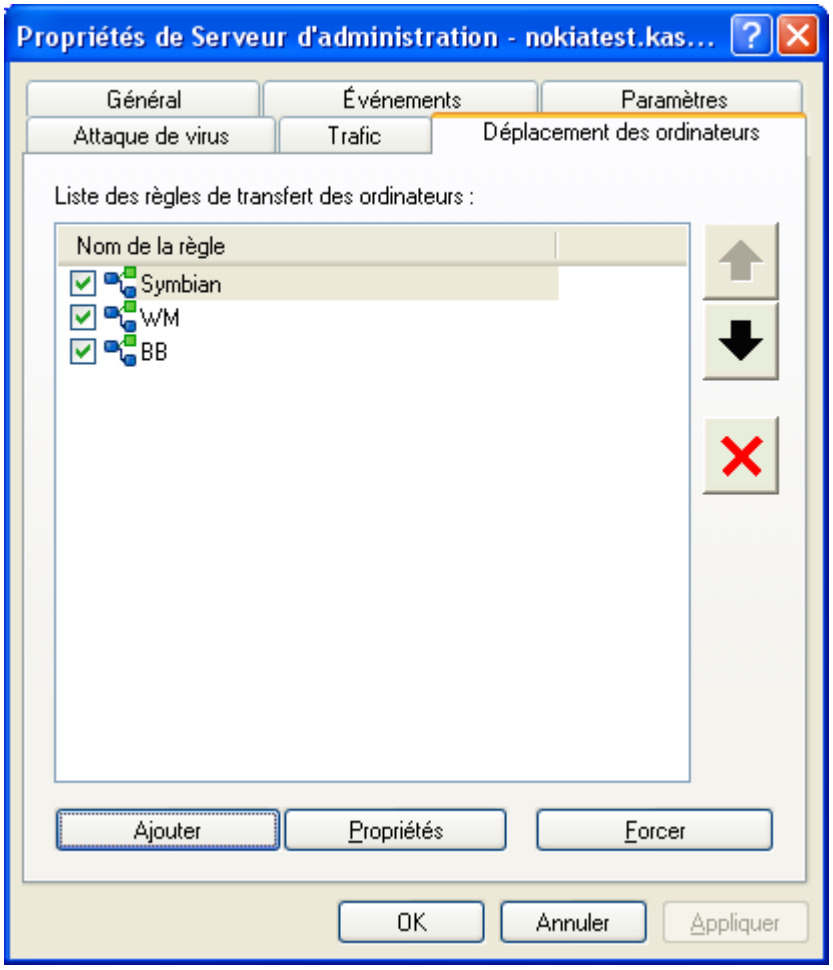


Figure 24 : fenêtre de configuration des paramètres du serveur d'administration

4. Créez une règle pour le déplacement des appareils mobiles dans le groupe. Pour ce faire, cliquez sur **Ajouter**. La fenêtre **Nouvelle règle** s'affiche (cf. ill. ci-après).

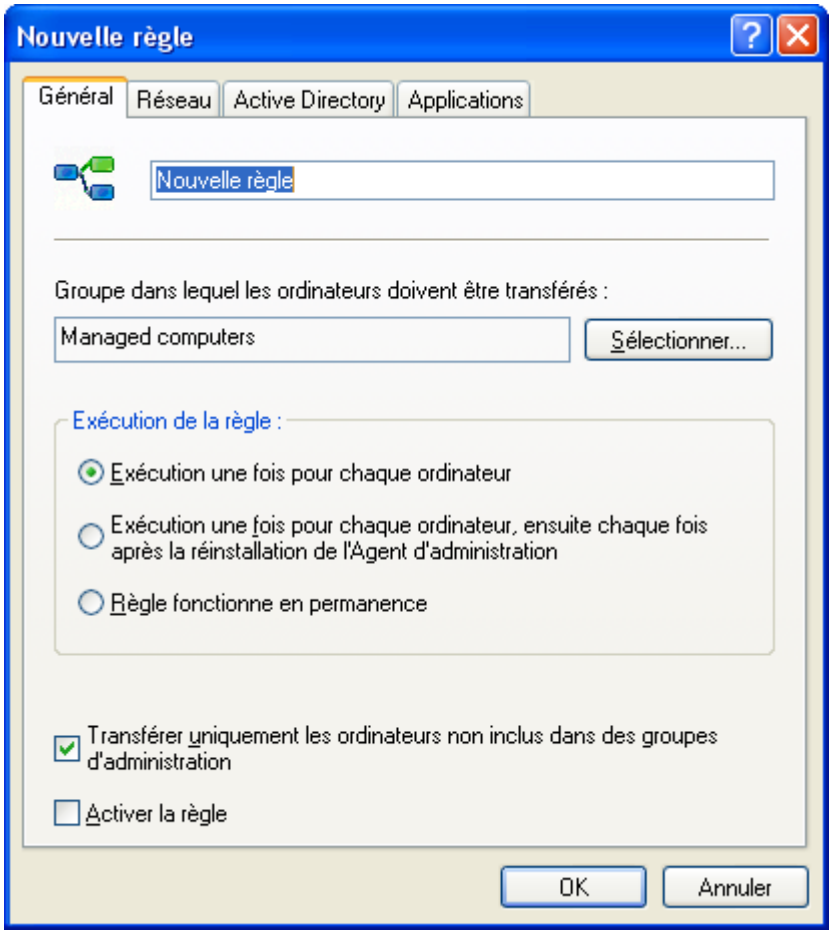


Figure 25 : paramètres généraux de déplacement d'appareils dans le groupe

5. Ouvrez l'onglet **Général** et procédez comme suit :

   - Saisissez le nom de la règle.
   - Spécifiez le groupe où il faudra déplacer les appareils mobiles. Pour ce faire, cliquez sur **Sélectionner** à droite du champ **Groupe dans lequel les ordinateurs doivent être transférés** et sélectionnez le groupe dans la fenêtre qui s'affiche.
   - Dans le groupe **Exécution de la règle**, sélectionnez **Exécution une fois pour chaque ordinateur**.
   - Cochez la case **Transférer uniquement les ordinateurs non inclus dans des groupes d'administration**, si les appareils faisant déjà partie de groupes d'administration ne doivent pas être déplacés dans un autre groupe après l'application de la règle.
   - Cochez la case **Activer la règle** pour activer l'application de la règle.

6. Ouvrez l'onglet **Applications** (cf. ill. ci-après) et sélectionnez le type des systèmes d'exploitation qui seront déplacés dans le groupe indiqué : Windows Mobile, Symbian, BlackBerry ou Android.

Si vous voulez placer tous les appareils dans le même groupe quel que soit le type du système d'exploitation installé, créez plusieurs règles en y indiquant le même groupe pour le placement des appareils.

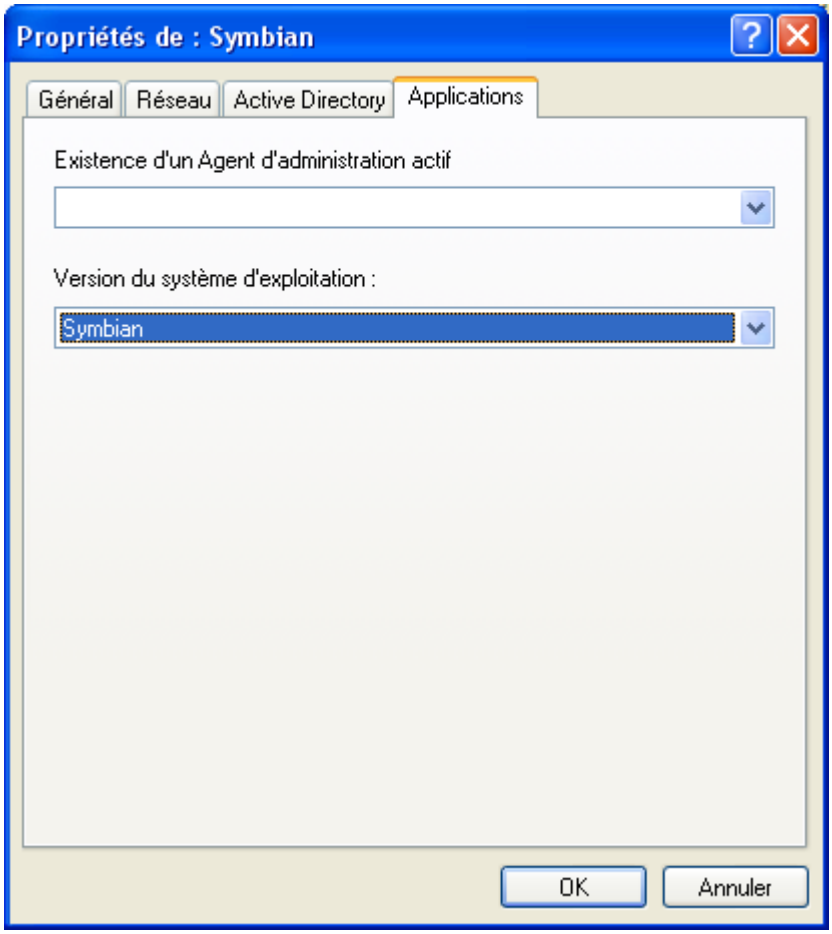


Figure 26 : sélection du système d'exploitation de l'appareil

7. Cliquez sur le bouton **OK**. La règle est ajoutée sur la liste des règles pour le déplacement des ordinateurs (v. l'onglet **Déplacement des ordinateurs** dans la fenêtre de configuration des paramètres du Serveur d'administration).

Suite à l'application de la règle, tous les ordinateurs qui n'ont pas été encore répartis seront déplacés depuis le groupe **Ordinateurs non répartis** vers le groupe que vous avez indiqué.

CONFIGURATION DES PARAMETRES LOCAUX DE L'APPLICATION

Le système d'administration de Kaspersky Administration Kit permet de gérer à distance les paramètres locaux de l'application Kaspersky Endpoint Security 8 for Smartphone sur les appareils mobiles via la Console d'administration. Les paramètres locaux de l'application permettent d'installer sur l'appareil des valeurs personnalisées des paramètres différentes des valeurs des paramètres définies dans la stratégie. Si dans la stratégie a été installée une licence qui prévoit un nombre inférieur d'appareils par rapport au nombre d'appareils dans le groupe, les paramètres locaux de l'application permettent d'installer une autre licence pour les appareils qui non pas été couvertes par la licence initiale.

Si un paramètre de la stratégie a été "verrouillé", la valeur du paramètre définie dans la stratégie ne peut être modifiée ni dans les paramètres locaux de l'application ni sur l'appareil mobile. La valeur de ce paramètre ne peut être modifiée que via la stratégie.

Si un paramètre de la stratégie a été "déverrouillé", l'application utilisera une des valeurs suivantes :

- la valeur par défaut si une autre valeur pour le paramètre n'a pas été définie par l'administrateur dans les paramètres locaux de l'application ou par l'utilisateur sur l'appareil mobile ;
- la valeur locale du paramètre défini par l'administrateur dans les paramètres locaux de l'application ;
- la valeur définie par l'utilisateur sur son appareil mobile.

Les valeurs des paramètres définies par l'administrateur via la console dans les paramètres locaux de l'application sont transmises vers l'appareil mobile pendant la synchronisation de l'appareil avec le Serveur d'administration et sont enregistrées sur l'appareil en tant que paramètres actifs de l'application. Si l'utilisateur définit sur son appareil mobile d'autres valeurs des paramètres, à la prochaine synchronisation de l'appareil avec le Serveur d'administration les nouvelles valeurs des paramètres seront transmises sur le serveur et enregistrées dans les paramètres locaux de l'application à la place des valeurs qui ont été installées par l'administrateur.

Pour configurer les paramètres locaux de l'application, procédez comme suit :

1. Connectez-vous au serveur d'administration.
2. Sélectionnez dans l'arborescence de la console le noeud **Ordinateurs administrés** et ouvrez le groupe avec les appareils mobiles où est installée l'application Kaspersky Endpoint Security 8 for Smartphone.
3. Sélectionnez l'appareil mobile dont les paramètres locaux de l'application vous allez modifier.
4. Ouvrez le menu contextuel de l'appareil et sélectionnez l'option **Propriétés**. La fenêtre **Propriétés : <nom de l'appareil>** avec plusieurs onglets s'affiche.
5. Sélectionnez l'onglet **Applications**. Il propose un tableau qui reprend la liste des applications de Kaspersky Lab installées sur l'appareil mobile, ainsi que de brèves informations sur chacune d'elles.
6. Sélectionnez l'application Kaspersky Endpoint Security 8 for Smartphone et cliquez sur **Propriétés**. La fenêtre **Paramètres de l'application Kaspersky Endpoint Security 8 for Smartphone** s'affiche.
7. **Analyser**, **Protection**, **Mise à jour**, **Antivol**, **Réseau**, **Avancé**, **Licence** (cf. la rubrique "**Description des paramètres de l'application Kaspersky Endpoint Security 8 for Smartphone**" à la page 60).
8. Cliquez sur le bouton **OK**. Les valeurs des paramètres locaux seront enregistrées sur le Serveur d'administration et transmises sur l'appareil mobile à la prochaine synchronisation de l'appareil avec le Serveur d'administration.

DESCRIPTION DES PARAMETRES DE L'APPLICATION KASPERSKY ENDPOINT SECURITY 8 FOR SMARTPHONE

L'administrateur peut configurer à distance les paramètres de fonctionnement de Kaspersky Endpoint Security 8 for Smartphone pour les composants Analyser, Protection, Antivol, Pare-feu, Anti-Spam, Contacts personnels et Chiffrement via les propriétés de la stratégie ou via les propriétés de l'appareil mobile sélectionné dans la Console d'administration.

De plus, l'administrateur doit obligatoirement configurer les paramètres de connexion des appareils au Serveur d'administration et les paramètres de mise à jour des bases de l'application ainsi qu'effectuer l'installation de la licence. Sinon, les applications installées sur les appareils mobiles ne pourront pas assurer un échange de données avec le Serveur d'administration et leurs fonctionnalités seront limitées.

Si dans les paramètres locaux de l'application un paramètre ne peut pas être modifié, la modification de ce paramètre est interdite dans la stratégie (le paramètre est suivi de l'icône).

Voici une description détaillée des onglets de la fenêtre **Propriétés** et des éléments de l'interface qui permettent à l'administrateur de configurer les paramètres de fonctionnement de l'application.

PARAMETRES DE LA FONCTION ANALYSE A LA DEMANDE

L'analyse à la demande permet d'identifier et de neutraliser les objets malveillants (cf. la rubrique "Analyse à la demande" à la page 15).

Les paramètres définis par l'administrateur sont utilisés pour l'analyse complète ou partielle de l'appareil pour détecter des objets malveillants éventuels. Dans les paramètres de l'analyse à la demande (cf. ill. ci-après), l'administrateur peut spécifier les types de fichiers à analyser, sélectionner l'action à appliquer si un objet infecté est détecté et configurer l'analyse programmée pour tout le système de fichiers de l'appareil. La configuration du lancement de l'analyse partielle programmée via le système d'administration distante n'est pas prévue. L'analyse partielle programmée peut être configurée par l'utilisateur directement depuis l'application installée sur l'appareil mobile.

L'analyse à la demande n'est pas utilisée sur les appareils tournant sous le système d'exploitation BlackBerry.

DANS CETTE SECTION

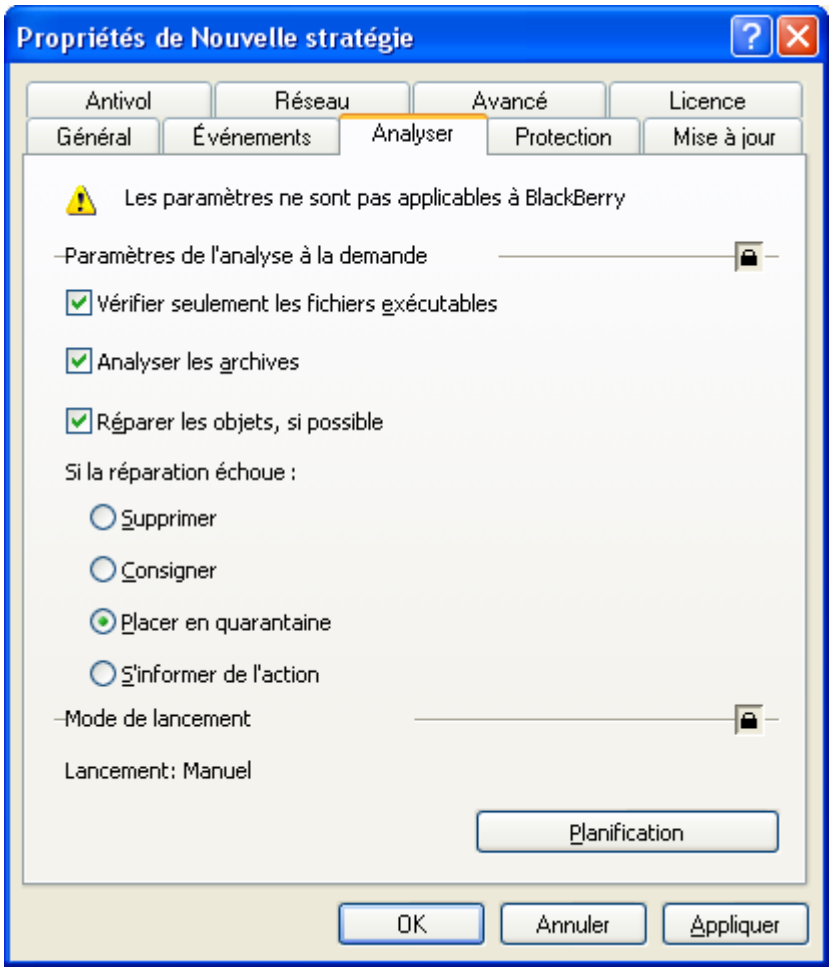


Figure 27 : configuration des paramètres de la fonction Analyse à la demande

La case **Vérifier seulement les fichiers exécutables**. Si la case est cochée, l'application analyse uniquement les fichiers exécutables des formats suivants : EXE, DLL, MDL, APP, RDL, PRT, PXT, LDD, PDD, CLASS, SO, ELF.

La case **Analyser les archives**. Si la case est cochée, l'application analyse tous les fichiers y compris le contenu des archives. L'application peut analyser les types d'archives suivants en fonction du système d'exploitation :

- sous Microsoft Windows Mobile : ZIP, JAR, JAD et CAB ;
- sous Symbian : ZIP, JAR, JAD, SIS et SISX ;
- sous Android : ZIP, JAR, JAD, SIS, SISX, CAB et APK.

Si les cases **Vérifier seulement les fichiers exécutables** et **Analyser les archives** ne sont pas cochées, l'application analyse tous les fichiers sauf les fichiers dans les archives.

La case **Réparer les objets, si possible**. Si la case est cochée, l'application répare les objets malveillants réparables. Si la réparation est impossible, l'application exécute l'action définie pour les objets infectés dans la liste **Si la réparation échoue**. Si la case n'est pas cochée, en cas de détection d'un objet malveillant l'application exécute l'action définie dans la liste **Action après découverte d'une menace**.

La liste **Si la réparation échoue** / **Action après découverte d'une menace** permet de sélectionner l'action que l'application exécutera en cas de détection d'un objet malveillant ou si la réparation est impossible :

- **Supprimer**. Supprime physiquement les objets malveillants sans notifier l'utilisateur.
- **Consigner dans le journal (Ignorer, pour Android**). Ignore les objets malveillants, mais consigne les informations relatives à leur découverte dans le journal de l'application et bloque les tentatives d'accès à l'objet (par exemple, copie ou ouverture).

  Si l'appareil tourne sous Android, l'application exécutera l'action **Ignorer** : les objets malveillants seront ignorés et ne seront pas supprimés de l'appareil.
- **Placer en quarantaine.** Bloque l'objet, déplace l'objet infecté dans un dossier spécifique – celui de quarantaine.
- **Confirmer l'action.** En cas de détection de l'objet malveillant, notifie l'utilisateur et propose de sélectionner l'action à exécuter sur l'objet découvert.

Vous pouvez sélectionner les actions après découverte d'une menace uniquement pendant la configuration des paramètres de la stratégie (cf. la rubrique "Configuration des paramètres de la stratégie" à la page 54) et des paramètres locaux de la stratégie (cf. la rubrique "Configuration des paramètres locaux de l'application" à la page 59). La configuration de ce paramètre n'est pas prévue pendant la création de la stratégie (cf. la rubrique "Création de la stratégie" à la page 45).

Le bouton **Planification**. Affiche la fenêtre pour programmer l'analyse complète du système de fichiers de l'appareil. Vous avez le choix parmi les options suivantes :

- **Manuel** L'analyse sera lancée par l'utilisateur à la main.
- **Chaque jour** L'analyse sera lancée automatiquement chaque jour. Spécifiez dans le groupe des champs **Heure de lancement** l'heure de lancement de l'analyse. L'heure est spécifiée pour une journée de 24h au format HH:MM.
- **Chaque semaine** L'analyse sera lancée automatiquement une fois par semaine le jour sélectionné. Sélectionnez dans la liste déroulante le jour de la semaine pour lancer l'analyse et spécifiez dans le groupe des champs **Heure de lancement** l'heure de lancement de l'analyse. L'heure est spécifiée pour une journée de 24h au format HH:MM.

PARAMETRES DE LA FONCTION PROTECTION

La Protection aide à éviter l'infection du système de fichiers de l'appareil mobile (cf. la rubrique "Protection" à la page 14). L'administrateur peut spécifier dans les paramètres de la protection les types de fichiers à analyser, sélectionner l'action à exécuter en cas de détection d'un objet infecté (cf. ill. ci-après).

La Protection est lancée par défaut au démarrage du système d'exploitation de l'appareil. Elle se trouve en permanence dans la mémoire vive de l'appareil et analyse tous les fichiers ouverts, enregistrés ou exécutés.

La Protection n'est pas utilisée sur les appareils tournant sous le système d'exploitation BlackBerry.

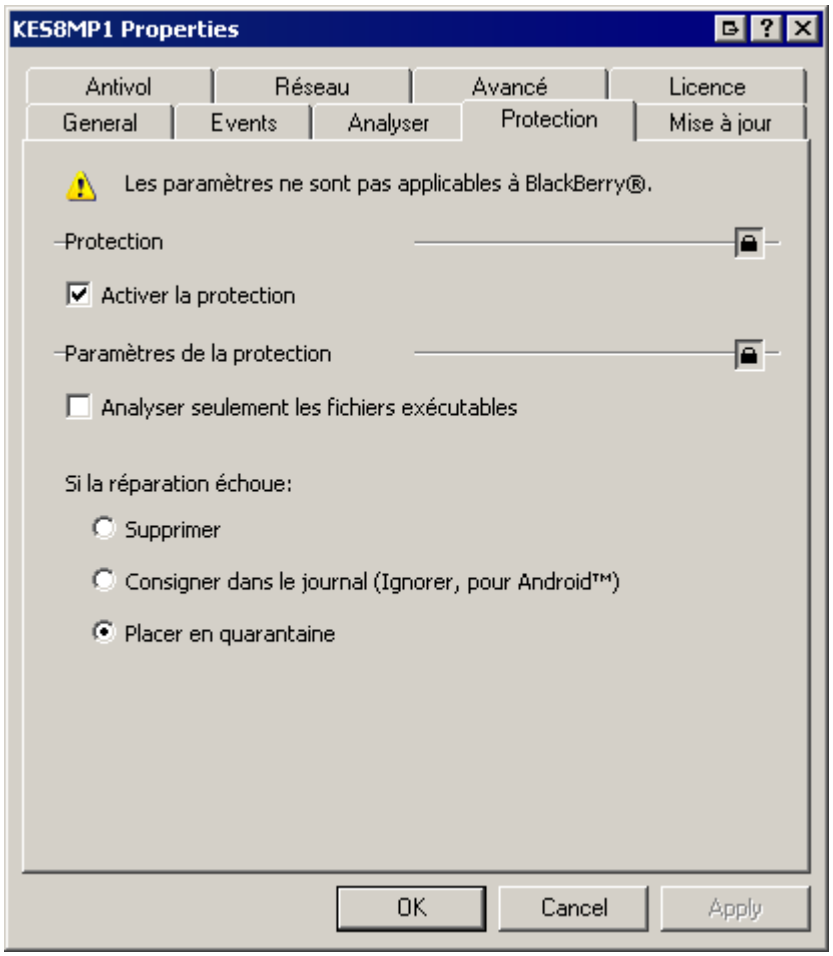


Figure 28 : configuration des paramètres de la fonction Protection

La case **Activer la protection**. Si la case est cochée, l'application analyse tous les fichiers ouverts, exécutés ou enregistrés. Si la case est décochée, la Protection est désactivée. La Protection est activée par défaut.

Le groupe **Paramètres de la protection** permet de spécifier les types de fichiers à analyser et de sélectionner l'action à exécuter en cas de détection d'un objet infecté.

La case **Vérifier seulement les fichiers exécutables**. Si la case est cochée, l'application analyse uniquement les fichiers exécutables des formats suivants : EXE, MDL, APP, DLL, RDL, PRT, PXT, LDD, PDD, CLASS. Si la case est décochée, Kaspersky Anti-Virus analyse les fichiers de tous les types.

La liste **Si la réparation échoue** permet de sélectionner l'action que l'application exécutera en cas de détection d'un objet infecté :

- **Supprimer**. Supprime physiquement les objets malveillants sans notifier l'utilisateur.
- **Consigner dans le journal (Ignorer, pour Android)**. Ignore les objets malveillants, mais consigne les informations relatives à leur découverte dans le journal de l'application et bloque les tentatives d'accès à l'objet (par exemple, copie ou ouverture).

Si l'appareil tourne sous Android, l'application exécutera l'action **Ignorer** : les objets malveillants seront ignorés et ne seront pas supprimés de l'appareil.

- **Placer en quarantaine.** Place les objets malveillants en quarantaine.

PARAMETRES DE LA FONCTION MISE A JOUR

La mise à jour des bases antivirus assure la fiabilité du système de protection des appareils mobiles contre les virus (cf. la rubrique "Mise à jour" à la page 16).

L'administrateur peut spécifier la source de mises à jour et créer la planification que l'application utilisera pour lancer la mise à jour.

La source de mise à jour par défaut est les serveurs de mises à jour de Kaspersky Lab. Le lancement de la mise à jour est effectué par l'utilisateur de l'appareil mobile à la main (cf. ill. ci-après).

La mise à jour des bases antivirus n'est pas utilisée sur les appareils tournant sous le système d'exploitation BlackBerry.

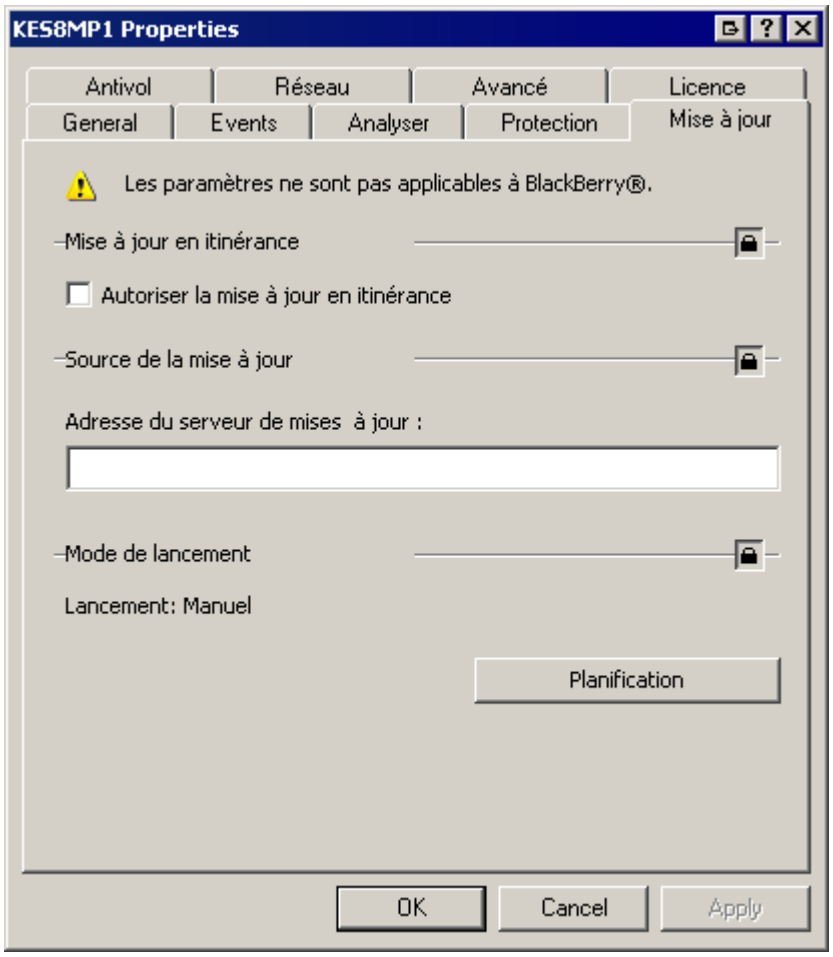


Figure 29 : configuration des paramètres de la fonction Mise à jour

La case **Autoriser la mise à jour en itinérance**. Si la case est cochée, la mise à jour programmée des bases de l'application est effectuée également lorsque l'appareil est en itinérance. L'utilisateur peut lancer la mise à jour des bases antivirus à la main quelle que soit la valeur du paramètre. Celle-ci est décochée par défaut.

L'autorisation de la mise à jour en itinérance n'est pas prise en charge par Android.

Dans le groupe **Source de la mise à jour**, il faut saisir l'adresse du serveur pour copier les mises à jour. Pour effectuer les mises à jour depuis les serveurs de mises à jour de Kaspersky Lab, dans le champ **Adresse du serveur de mises à jour** saisissez `KLServeurs`.

Si vous utilisez un autre serveur pour mettre à jour les bases de l'application, spécifiez dans le groupe **Source de la mise à jour** un serveur HTTP, un dossier local ou un dossier réseau. Par exemple, http://domain.com/index/.

La structure des dossiers dans la source de la mise à jour doit être identique à celle du serveur de mise à jour de Kaspersky Lab.

Le bouton **Planification**. Affiche la fenêtre pour programmer les mises à jour de l'application. Vous avez le choix parmi les options suivantes :

- **Manuel** La mise à jour des bases de l'application sera lancée par l'utilisateur à la main.
- **Chaque jour** La mise à jour des bases de l'application sera lancée automatiquement chaque jour. Spécifiez dans le groupe des champs **Heure de lancement** l'heure de lancement de la mise à jour.
- **Chaque semaine** La mise à jour des bases de l'application sera lancée automatiquement une fois par semaine le jour sélectionné. Sélectionnez dans la liste déroulante le jour de la semaine pour lancer la mise à jour et spécifiez dans le groupe des champs **Heure de lancement** l'heure de lancement de la mise à jour.

Le fait de créer ou de ne pas créer une planification par l'administrateur ne peut en aucune manière limiter la possibilité de l'utilisateur de lancer la mise à jour à la main.

PARAMETRES DU COMPOSANT ANTIVOL

Le composant Antivol assure la protection des données stockées sur les appareils mobiles d'utilisateurs contre l'accès non autorisé (cf. la rubrique "Antivol" à la page 16). L'administrateur peut activer ou désactiver l'utilisation des fonctions du composant Antivol sur les appareils mobiles d'utilisateurs et configurer les paramètres de ces fonctions (cf. ill. ci-après).

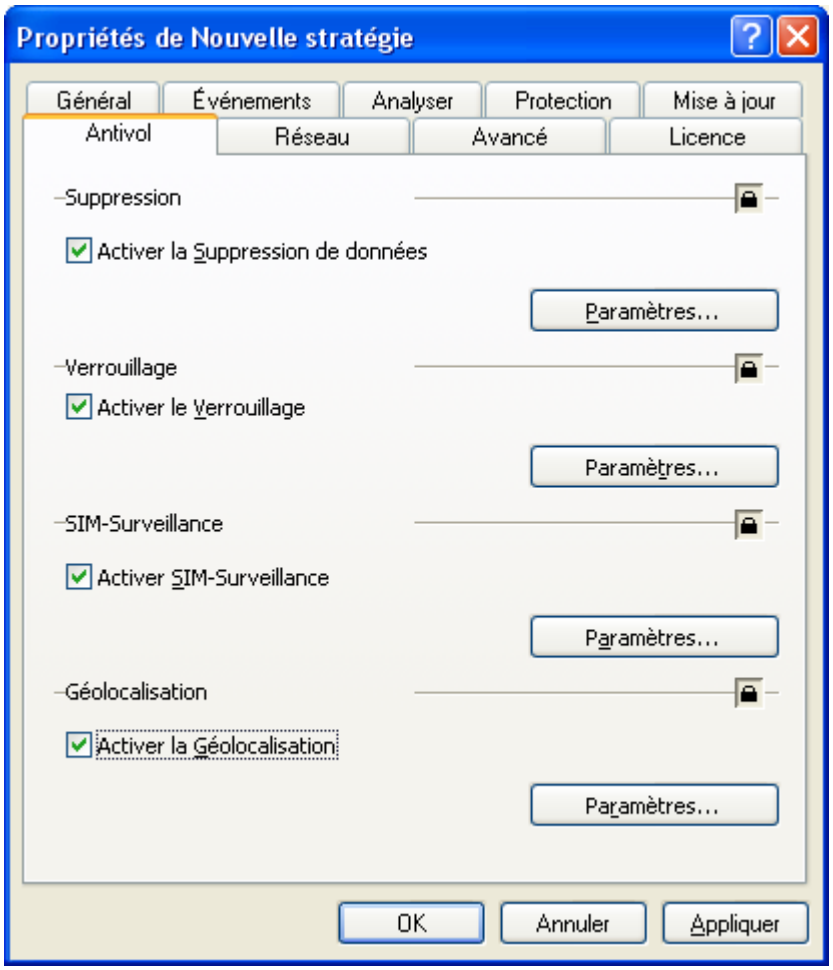


Figure 30 : configuration des paramètres du composant Antivol

La case **Activer la Suppression de données**. Si la case est cochée, la fonction de suppression des données à distance et la fonction de sélection des données à supprimer seront activées. Par défaut, la fonction Suppression est désactivée. Le bouton **Paramètres** à droite de la case ouvre la fenêtre **Paramètres de suppression des données** où vous pouvez configurer les paramètres de la fonction (cf. la rubrique "Paramètres de la fonction Suppression" à la page 68).

La case **Activer le Verrouillage**. Si la case est cochée, la possibilité de bloquer à distance l'accès à l'appareil et aux données qui y sont stockées est activée. La fonction Verrouillage est désactivée par défaut. Le bouton **Paramètres** à droite de la case ouvre la fenêtre où vous pouvez configurer les paramètres de la fonction (cf. la rubrique "Paramètres de la fonction Verrouillage" à la page 70).

Pour que la fonction Verrouillage fonctionne sur les appareils dotés d'Android version 2.2 et ultérieure, l'application Kaspersky Endpoint Security 8 for Smartphone doit être installée comme écran principal par défaut.

Si l'application n'est pas installée en tant qu'écran d'accueil par défaut sur les appareils tournant sous Android version 2.2 ou ultérieure, Kaspersky Endpoint Security 8 for Smartphone exécutera les actions dans les conditions suivantes :

- Si les paramètres de l'application sont verrouillés, la fonction Verrouillage est activée après leur transfert sur l'appareil. Il ne sera pas possible de garantir la protection de l'appareil lors du déclenchement de la fonction. Lors de la synchronisation avec Kaspersky Administration Kit, l'application enverra l'événement **Impossible de verrouiller l'appareil**. À chaque lancement de l'application ou lors de la synchronisation de l'appareil avec Kaspersky Administration Kit, l'application proposera à l'utilisateur d'installer Kaspersky Endpoint Security 8 for Smartphone en tant qu'écran d'accueil par défaut.

  Quand l'utilisateur installe l'application en tant qu'écran d'accueil par défaut, lors de la synchronisation suivante de l'appareil avec Kaspersky Administration Kit, l'application envoie l'événement **Verrouillage activé**.

- Si la modification des paramètres de l'application est autorisée, la fonction Verrouillage n'est pas activée après leur transfert sur l'appareil. Lors de la synchronisation de l'appareil avec Kaspersky Administration Kit, l'application envoie l'événement **Verrouillage désactivé**.

La case **Activer SIM-Surveillance**. Si la case est cochée, Kaspersky Endpoint Security 8 for Smartphone bloque l'appareil mobile en cas de remplacement de la carte SIM ou de mise sous tension sans cette carte. L'utilisateur peut spécifier un numéro de téléphone et / ou une adresse électronique pour envoyer le nouveau numéro de téléphone et activer le verrouillage de l'appareil en cas de remplacement de la carte SIM. Pour configurer cette fonction, il faut spécifier le numéro de téléphone et / ou l'adresse électronique pour y envoyer le numéro de téléphone actuel en cas de remplacement de la carte SIM de l'appareil. Par défaut, la fonction SIM-Surveillance est désactivée. Le bouton **Paramètres** à droite de la case ouvre la fenêtre **Paramètres SIM-surveillance** où vous pouvez configurer les paramètres de la fonction (cf. la rubrique "Paramètres de la fonction SIM-surveillance" à la page 70).

La case **Activer la Géolocalisation**. Si la case est cochée, Kaspersky Endpoint Security 8 for Smartphone permet de déterminer les coordonnées géographiques de l'appareil et de les recevoir via SMS envoyé à l'appareil à l'origine de la demande ou à l'adresse électronique définie. Pour configurer cette fonction, il faut spécifier l'adresse électronique où l'application enverra les coordonnées géographiques de l'appareil après la réception d'une instruction SMS. Par défaut, l'application envoie les coordonnées de l'appareil par SMS au numéro de téléphone qui a émis l'instruction SMS spéciale. Par défaut, la fonction Géolocalisation est désactivée. Le bouton **Paramètres** à droite de la case ouvre la fenêtre où vous pouvez configurer les paramètres de la fonction Géolocalisation.

PARAMETRES DE LA FONCTION SUPPRESSION

La configuration des paramètres de la fonction Suppression est effectuée dans la fenêtre **Paramètres de suppression des données** (cf. ill. ci-après).

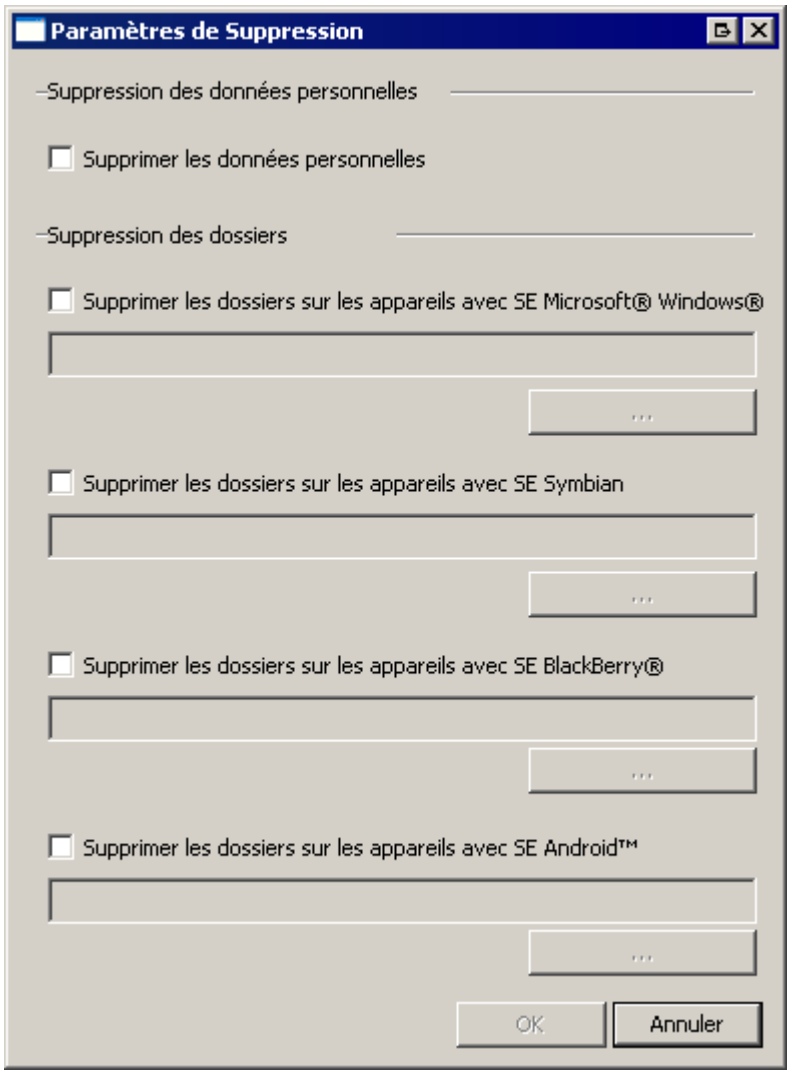


Figure 31 : configuration des paramètres de la fonction Suppression

La case **Supprimer les données personnelles**. L'application permet de supprimer les informations suivantes stockées sur les appareils tournants sous Microsoft Windows Mobile et Symbian : entrées des Contacts et sur la carte SIM, SMS, galerie, calendrier, paramètres de connexion à Internet. L'application supprime les informations personnelles suivantes stockées sur les appareils tournant sous BlackBerry : entrées des Contacts, calendrier, messages électroniques, journal des appels. Sur les appareils tournant sous Android, l'application supprime les données personnelles suivantes : entrées dans le répertoire téléphonique et sur la carte SIM, SMS, journal des appels, calendrier, paramètres de connexion à Internet, comptes utilisateur, à l'exception du compte Google™. La fonction est activée lorsque l'appareil reçoit l'instruction SMS spéciale.

Si cette case est cochée, les données personnelles seront supprimées à la réception d'un SMS spécial. Si cette case n'est pas cochée, les données personnelles ne seront pas supprimées à la réception d'un SMS spécial.

Par défaut, la case **Supprimer les données personnelles** est cochée.

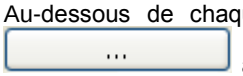
Le groupe **Suppression des dossiers** (cf. ill. ci-après). L'application permet de configurer la suppression de dossiers sur l'appareil mobile en cas de réception de l'instruction SMS spéciale.

Pendant la configuration des paramètres de la stratégie, les paramètres de suppression de dossiers sont définis pour chacun des systèmes d'exploitation et le groupe **Suppression des dossiers** contient les cases suivantes :

- **Supprimer les dossiers sur les appareils avec SE Microsoft Windows Mobile**. La suppression des dossiers définis par l'administrateur ou l'utilisateur sur les appareils tournant sous Microsoft Windows Mobile.

- **Supprimer les dossiers sur les appareils avec SE Symbian**. La suppression des dossiers définis par l'administrateur ou l'utilisateur sur les appareils tournant sous Symbian.
- **Supprimer les dossiers sur les appareils avec SE BlackBerry**. La suppression des dossiers définis par l'administrateur ou l'utilisateur sur les appareils tournant sous BlackBerry.
- **Supprimer les dossiers sur les appareils avec SE Android**. La suppression des dossiers définis par l'administrateur ou l'utilisateur sur les appareils tournant sous Android.

Si la case est cochée, après la réception de l'instruction SMS spéciale l'application supprime de l'appareil mobile les dossiers définis par l'administrateur et les dossiers définis par l'utilisateur. Si la case est décochée, les dossiers ne seront pas supprimés.

Au-dessous de chaque case, il y a un champ pour créer la liste des dossiers à supprimer. Le bouton 

à droite du champ affiche la fenêtre où l'administrateur peut créer une liste des dossiers à supprimer. Dans ce cas, vous pouvez spécifier les dossiers stockés dans la mémoire de l'appareil ou sur une carte mémoire. Par défaut, la liste des dossiers à supprimer est vide.

Pour créer la liste des dossiers, l'administrateur peut utiliser les macros suivantes :

- Pour les appareils mobiles tournant sous Microsoft Windows Mobile :
  - %DOCS% : dossier **Mes documents** (le nom exact dépend de la localisation de l'appareil) ;
  - %CARD% : toutes les cartes mémoire accessibles dans le système.
- Pour les appareils mobiles tournant sous Symbian :
  - %DOCS% : dossier **C:\Data** ;
  - %CARD% : toutes les cartes mémoire accessibles dans le système.
- Pour les appareils mobiles tournant sous SE BlackBerry :
  - %DOCS% : dossier **\store\home\user\documents** ;
  - %CARD% : carte mémoire (**\SDCard**).
- Pour les appareils tournant sous Android, la macro %CARD% désigne la carte mémoire (**\SDCard**).

Pendant la configuration des paramètres locaux de l'application via la Console d'administration dans la fenêtre **Paramètres de suppression des données** figurent les paramètres qui définissent la suppression des données sur un appareil spécifique, alors, le groupe **Suppression des dossiers** contient une seule case **Supprimer les dossiers** et un champ pour créer la liste des dossiers à supprimer (cf. ill. ci-après). Dans ce cas, la liste des dossiers à supprimer est accessible uniquement à la consultation. L'administrateur ne peut modifier la liste des dossiers à supprimer que dans les paramètres de la stratégie.

Attention ! Pour annuler la suppression des dossiers définis, l'administrateur doit supprimer tout le texte dans le champ de saisie sous la case **Supprimer les dossiers sur les appareils avec SE Microsoft Windows Mobile** / **Supprimer les dossiers sur les appareils avec SE Symbian** / **Supprimer les dossiers sur les appareils avec SE BlackBerry** / **Supprimer les dossiers sur les appareils avec SE Android** et assurer la transmission des paramètres sur les appareils mobiles d'utilisateurs. Pour ce faire, dans la fenêtre de configuration des paramètres de la stratégie sous l'onglet **Antivol** le groupe **Suppression** doit être "verrouillé".

PARAMETRES DE LA FONCTION VERROUILLAGE

La configuration des paramètres de la fonction Verrouillage est effectuée dans la fenêtre **Paramètres de verrouillage** (cf. ill. ci-après).

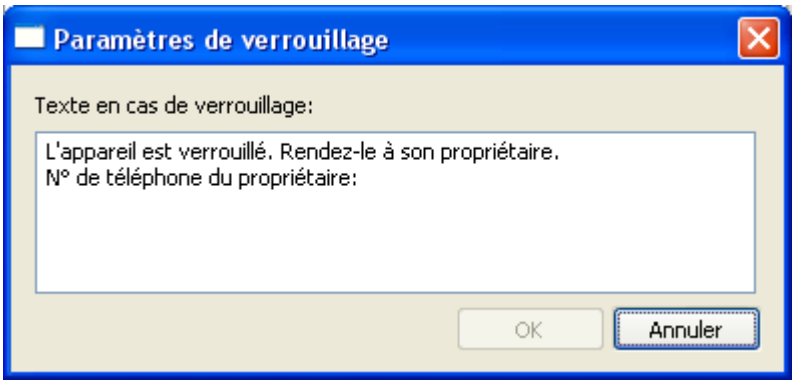


Figure 32 : configuration des paramètres de la fonction Verrouillage

Texte en cas de verrouillage. Le texte du message qui apparaîtra sur l'écran de l'appareil verrouillé. Un texte standard est saisi par défaut.

PARAMETRES DE LA FONCTION SIM-SURVEILLANCE

La configuration des paramètres de la fonction SIM-Surveillance est effectuée dans la fenêtre **Paramètres de SIM-surveillance** (cf. ill. ci-après).

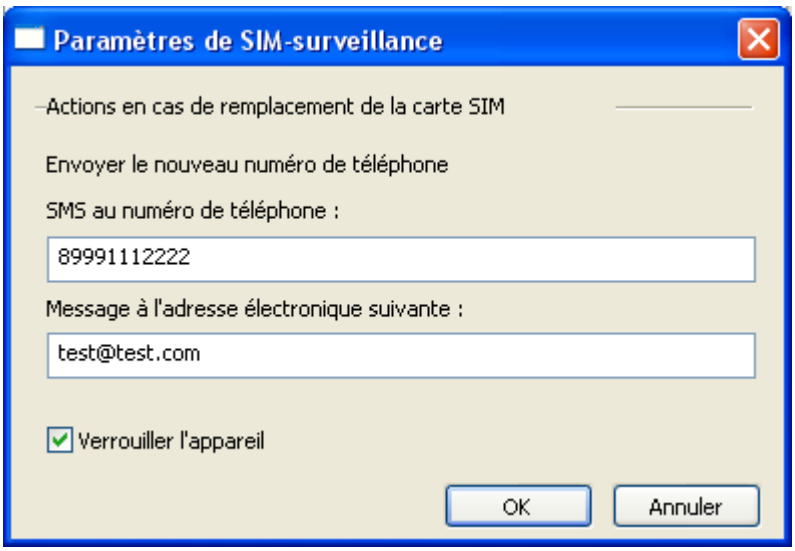


Figure 33 : configuration des paramètres de la fonction SIM-Surveillance

SMS au numéro de téléphone. Ce champ sert à saisir le numéro où l'application enverra un SMS avec le nouveau numéro de téléphone en cas de remplacement de la carte SIM. Ces numéros peuvent commencer par un chiffre ou par le signe "+" et ne peuvent contenir que des chiffres. Il est conseillé de saisir le numéro au format utilisé par votre opérateur de téléphonie mobile.

Message à l'adresse électronique suivante. Ce champ sert à saisir l'adresse électronique où l'application enverra un message avec le nouveau numéro de téléphone en cas de remplacement de la carte SIM.

Verrouiller l'appareil. Bloque l'appareil en cas de remplacement de la carte SIM ou de mise sous tension sans cette carte. Si cette case est cochée, SIM-Surveillance pourra bloquer l'appareil en cas de remplacement de la carte SIM. Pour déverrouiller l'appareil, l'utilisateur de l'appareil devra saisir le code secret de l'application. Si cette case n'est pas cochée, SIM-Surveillance ne pourra pas bloquer l'appareil au remplacement de la carte SIM. Vous pouvez également saisir le texte qui s'affichera à l'écran de l'appareil verrouillé. Un texte standard est saisi par défaut.

PARAMETRES DE LA FONCTION GEOLOCALISATION

La configuration des paramètres de la fonction Géolocalisation est effectuée dans la fenêtre Géolocalisation (cf. ill. ci-après).

Figure 34 : configuration des paramètres de la fonction Géolocalisation

Message à l'adresse électronique suivante. L'adresse électronique où l'application enverra les coordonnées géographiques de l'appareil après la réception d'une instruction SMS. Par défaut, l'application envoie les coordonnées de l'appareil par SMS au numéro de téléphone qui a émis l'instruction SMS spéciale.

PARAMETRES DU COMPOSANT PARE-FEU

Le Pare-feu contrôle connexions réseau sur les appareils mobiles d'utilisateurs (cf. la rubrique "Pare-feu" à la page 18). L'administrateur peut définir pour le composant Pare-feu un niveau de protection qui sera installé sur les appareils mobiles d'utilisateur. Paramètres du composant Pare-feu figurent sous l'onglet **Réseau** (cf. ill. ci-après).

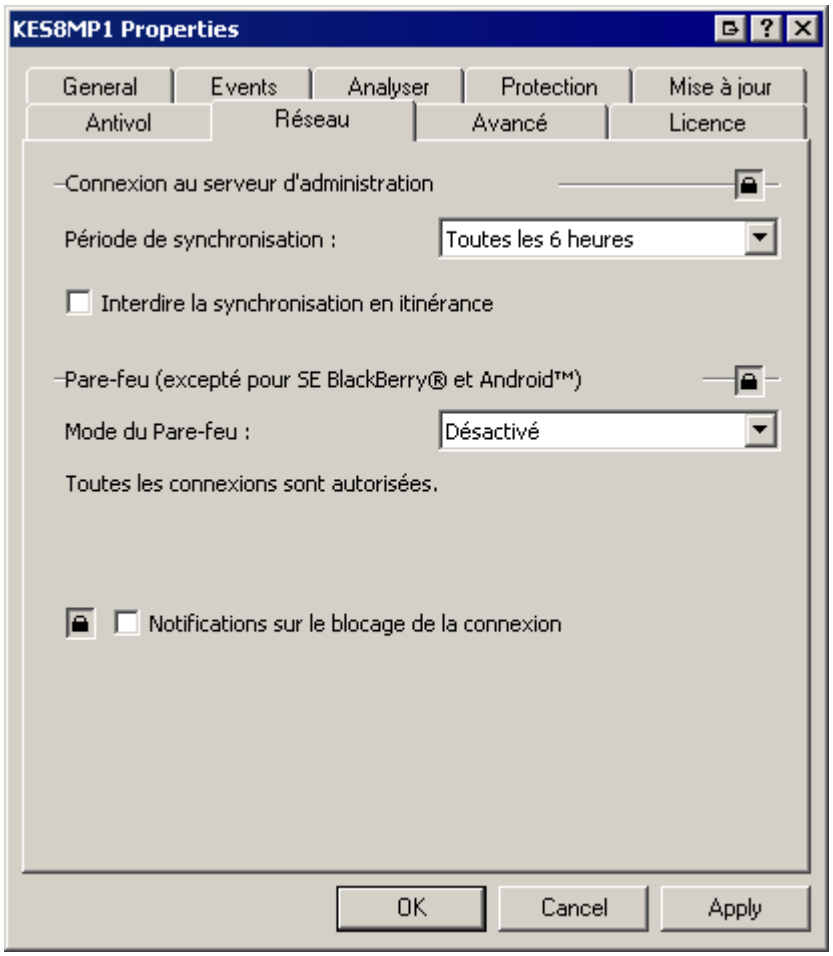


Figure35 : Configuration des paramètres du composant Pare-feu et des paramètres de synchronisation avec le Serveur d'administration

Le composant Pare-feu est utilisé sur les appareils tournant sous BlackBerry et Android.

Le groupe **Pare-feu (excepté pour SE BlackBerry et Android**) permet de configurer les paramètres du composant Pare-feu :

- La liste déroulante **Mode du Pare-feu** permet de sélectionner un des modes suivants :
  - **Désactivé** : autorisation de la moindre activité de réseau. Le Pare-feu est désactivé.
  - **Protection minimum** : bloque uniquement les connexions entrantes. Les connexions sortantes sont autorisées.
  - **Protection maximum** : bloque toutes les connexions entrantes. L'utilisateur peut recevoir les messages électroniques, surfer sur le Web et télécharger les fichiers. Les connexions sortantes peuvent être réalisées uniquement via les ports SSH, HTTP, HTTPS, IMAP, SMTP, POP3.
  - **Tout bloquer** : bloque toute activité de réseau, sauf la mise à jour des bases antivirus et la connexion au Serveur d'administration.

  Par défaut, le Pare-feu n'est pas activé et la valeur du paramètre **Mode du Pare-feu** est **Désactivé**.
- La case **Notifications sur le blocage de la connexion**. Si la case est cochée, l'application notifie l'utilisateur sur le blocage de la connexion. Si la case est décochée, l'application bloque la connexion selon le mode sélectionné sans notifier l'utilisateur.

  Par défaut, les notifications du Pare-feu sont désactivées.

PARAMETRES DE SYNCHRONISATION DES APPAREILS AVEC LE SERVEUR D'ADMINISTRATION

La synchronisation des appareils mobiles avec le Serveur d'administration assure la gestion des appareils mobiles via Kaspersky Administration Kit (cf. la rubrique "Conception de la gestion de l'application via Kaspersky Administration Kit" à la page 23). L'administrateur peut définir les paramètres de synchronisation des appareils avec le Serveur d'administration sous l'onglet **Réseau** (cf. ill. ci-après).

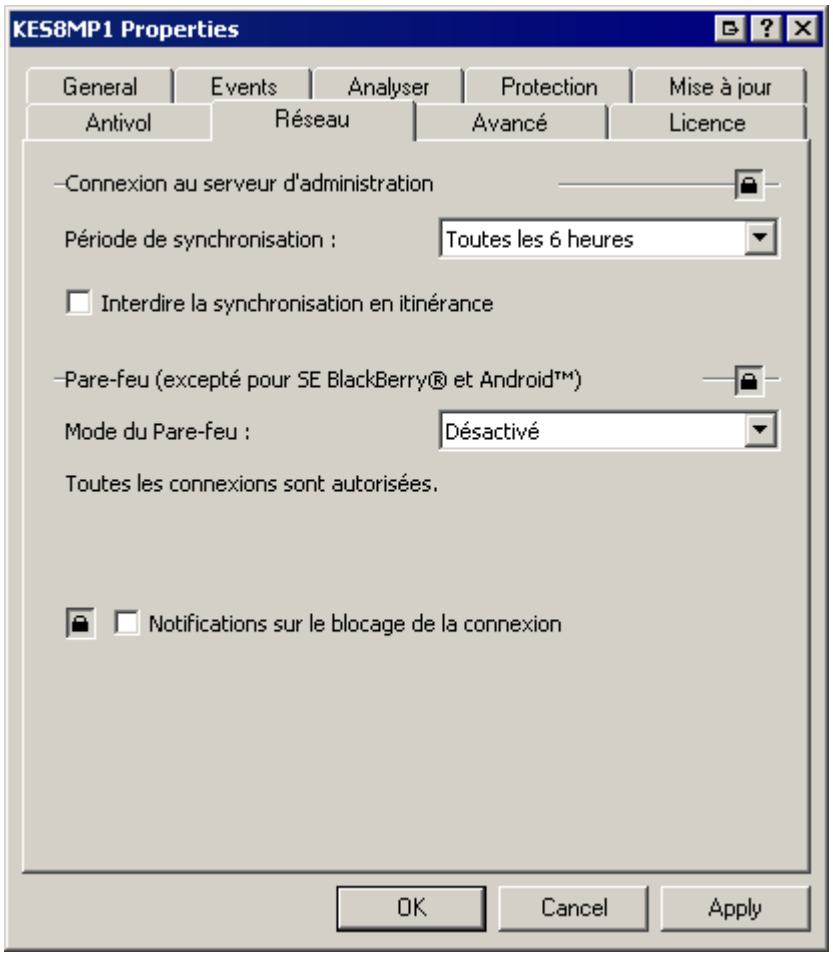


Figure36 : Configuration des paramètres du composant Pare-feu et des paramètres de synchronisation avec le Serveur d'administration

Le groupe **Connexion au serveur d'administration** permet de configurer les paramètres de synchronisation suivants :

- **Période de synchronisation**. Le texte dans ce champ indique la fréquence de la synchronisation des appareils mobiles avec le Serveur d'administration.

  Par défaut, la synchronisation est effectuée toutes les 6 heures.

- La case **Interdire la synchronisation en itinérance**. Si la case est cochée, la synchronisation automatique avec le Serveur d'administration sera interdite lorsque l'appareil est en itinérance. Dans ce cas, l'utilisateur pourra toujours effectuer la synchronisation à la main.

  Par défaut, la synchronisation automatique des appareils mobiles avec le Serveur d'administration est autorisée et la case est décochée.

  L'interdiction de la synchronisation en itinérance n'est pas prise en charge par Android.

PARAMETRES DES COMPOSANTS ANTI-SPAM ET CONTACTS PERSONNELS

Le composant Anti-Spam empêche la réception d'appels et de SMS non sollicités sur la base des listes noire et blanche créées par l'utilisateur (cf. la rubrique "Anti-Spam" à la page 17). Le composant Contacts personnels dissimule les informations confidentielles de l'utilisateur : entrées des Contacts, SMS entrants, sortants et transmis et entrées du journal des appels (cf. la rubrique "Contacts personnels" à la page 17).

L'administrateur peut définir la disponibilité des composants Anti-Spam et Contacts personnels pour les utilisateurs des appareils mobiles sous l'onglet **Avancé** (cf. ill. ci-après). Si l'utilisation des composants est autorisée, la configuration des paramètres pour ces composants est effectuée par l'utilisateur.

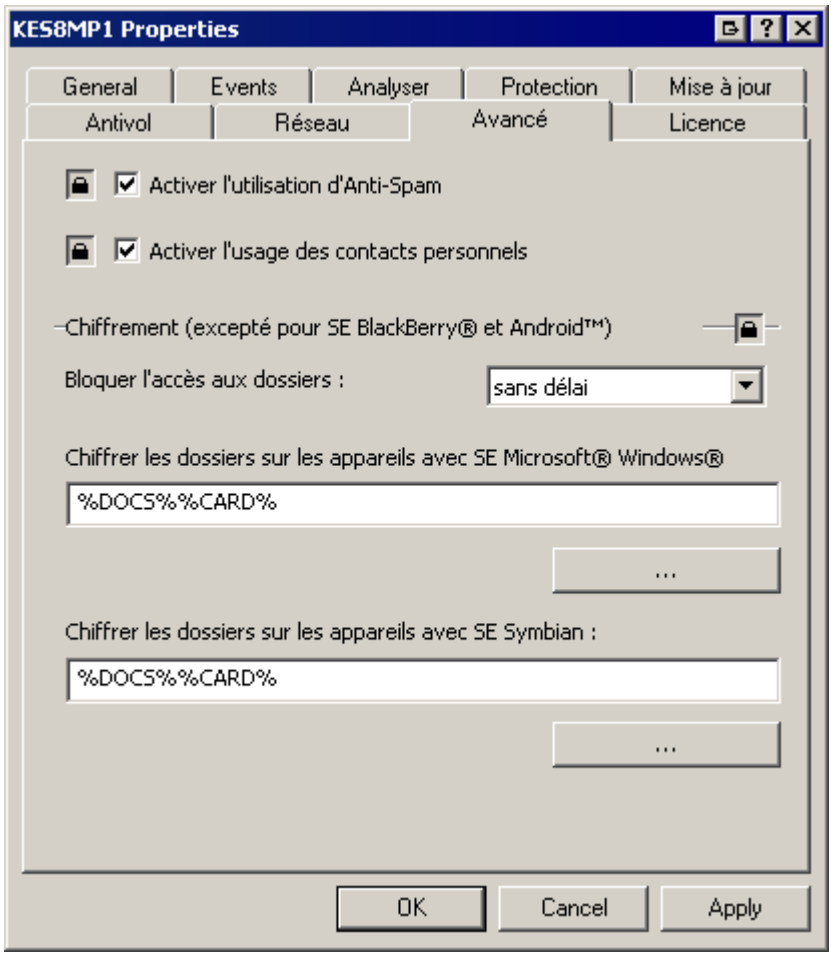


Figure 37 : Configuration des paramètres des composants Anti-Spam, Contacts personnels et Chiffrement

Les paramètres des composants Anti-Spam et Contacts personnels figurent sur l'onglet **Avancé** :

- La case **Activer l'utilisation de l'Antide l'Anti-Spam**. Si la case est cochée, l'utilisateur peut utiliser le composant Anti-Spam sur son appareil mobile et configurer ses paramètres. Si l'utilisation de l'Antide l'Anti-Spam est interdite, l'accès au composant sur l'appareil est bloqué.

  Par défaut, l'utilisation du composant Anti-Spam est autorisée.

- La case **Activer l'utilisation des contacts personnels**. Si la case est cochée, l'utilisateur peut utiliser le composant Contacts personnels sur son appareil mobile et configurer ses paramètres. Si l'utilisation des Contacts personnels est interdite, l'accès au composant sur l'appareil est bloqué.

  Par défaut, l'utilisation du composant Contacts personnels est autorisée.

  Le composant Contacts personnels n'est pas pris en charge par BlackBerry.

PARAMETRES DU COMPOSANT CHIFFREMENT

Le composant Chiffrement chiffre les informations de la liste des dossiers pour le chiffrement que vous avez créée (cf. la rubrique "Chiffrement" à la page 18).

L'administrateur peut spécifier la période à l'issue de laquelle après le passage de l'appareil en mode d'économie d'énergie l'accès aux données chiffrées sera interdit et définir les dossiers ainsi chiffrés. La configuration des paramètres de chiffrement est effectuée sous l'onglet **Avancé** (cf. ill. ci-après).

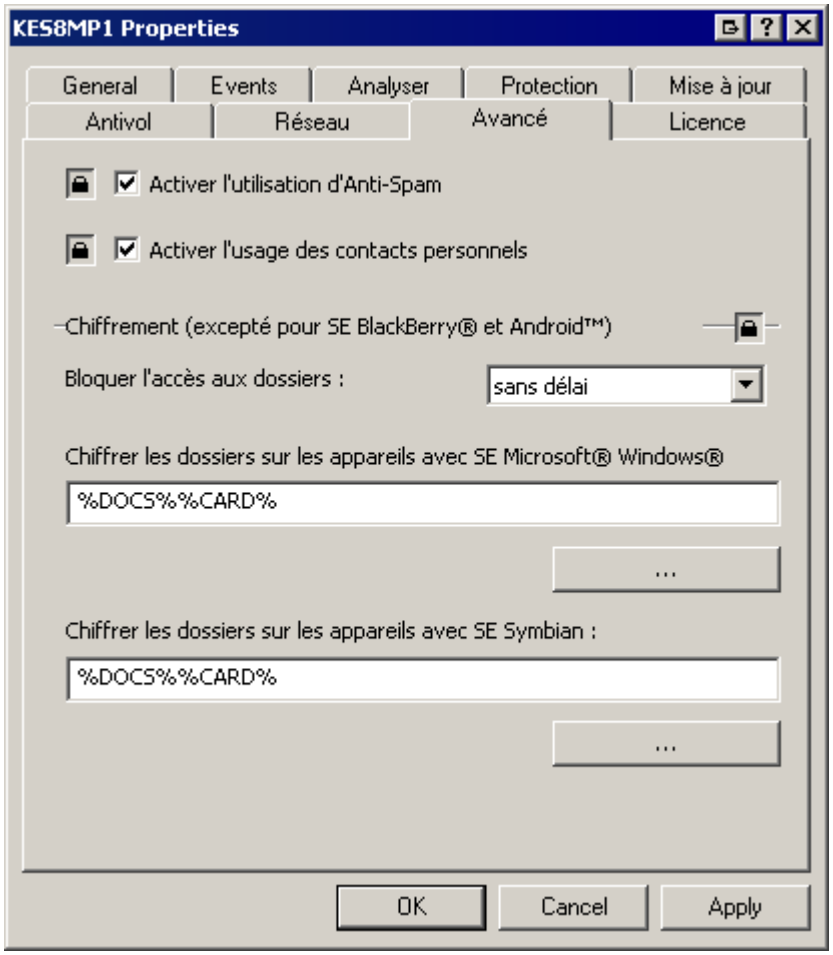


Figure 38 : Configuration des paramètres des composants Anti-Spam, Contacts personnels et Chiffrement

Le composant Chiffrement n'est pas pris en charge par les appareils mobiles tournant sous SE BlackBerry et Android.

Le groupe **Chiffrement (excepté pour SE BlackBerry et Android)** permet de configurer les paramètres du composant Chiffrement :

- **Bloquer l'accès aux dossiers**. Sélectionnez dans la liste la période à l'issue de laquelle l'accès aux dossiers chiffrés utilisés sera interdit. La fonction est activée au moment de passage de l'appareil en mode d'économie d'énergie.

  Par défaut, l'accès aux dossiers chiffrés utilisés est bloqué directement après le passage de l'appareil en mode économie énergétique. La valeur sélectionnée pour le paramètre **Bloquer l'accès aux dossiers** est **sans délai**.

- **Chiffrer les dossiers sur les appareils avec SE Microsoft Windows Mobile**. Le champ contient la liste des dossiers pour le chiffrement sélectionnés par l'administrateur pour les appareils tournant sous Microsoft Windows Mobile. Le bouton ... à droite du champ affiche la fenêtre où l'administrateur peut créer une liste des dossiers pour le chiffrement.

- **Chiffrer les dossiers sur les appareils avec SE Symbian**. Le champ contient la liste des dossiers pour le chiffrement sélectionnés par l'administrateur pour les appareils tournant sous Microsoft Windows Mobile. Le

bouton  à droite du champ affiche la fenêtre où l'administrateur peut créer une liste des dossiers pour le chiffrement.

Pour créer la liste des dossiers, l'administrateur peut utiliser les macros suivantes :

- Pour les appareils mobiles tournant sous Microsoft Windows Mobile :
  - %DOCS% : dossier **Mes documents** (le nom exact dépend de la localisation de l'appareil) ;
  - %CARD% : toutes les cartes mémoire accessibles dans le système.
- Pour les appareils mobiles tournant sous Symbian :
  - %DOCS% : dossier **C:\Data** ;
  - %CARD% : toutes les cartes mémoire accessibles dans le système.

L'utilisateur ne peut pas annuler le chiffrement des dossiers définis par l'administrateur. Il peut cependant spécifier les dossiers à chiffrer sur sont appareil mobile via l'interface locale de l'application. Si l'administrateur n'a pas défini les dossiers à chiffrer, l'application ne chiffrera que les dossiers spécifiés par l'utilisateur.

Pendant la modification des paramètres locaux de l'application via le Console d'administration la liste des dossiers pour le chiffrement est accessible uniquement à la consultation. L'administrateur ne peut modifier la liste des dossiers pour le chiffrement que dans les paramètres de la stratégie.

Pour annuler le chiffrement des dossiers définis, l'administrateur doit supprimer tout le texte dans le champ de saisie sous la case **Chiffrer les dossiers sur les appareils avec SE Microsoft Windows Mobile/Chiffrer les dossiers sur les appareils avec SE Symbian** et assurer la transmission des paramètres sur les appareils mobiles d'utilisateurs. Pour ce faire, dans la fenêtre de configuration des paramètres de la stratégie sous l'onglet **Avancé** le groupe **Chiffrement (excepté pour SE BlackBerry et Android)** doit être "verrouillé" (cf. ill. ci-après).

SUPPRESSION DE L'APPLICATION

La suppression de l'application de l'appareil mobile est effectuée par l'utilisateur à la main.

Pour SE Microsoft Windows Mobile et Symbian avant la suppression de l'application, la dissimulation des informations confidentielles sur l'appareil sera désactivée automatiquement et les informations chiffrées seront déchiffrées en mode automatique. Sous BlackBerry et Android, l'utilisateur doit désactiver manuellement le masquage des données confidentielles avant de supprimer l'application de l'appareil.

Pour en savoir plus sur la procédure de suppression de l'application, consultez le Guide de l'utilisateur de Kaspersky Endpoint Security 8 for Smartphone.

DEPLOIEMENT DE L'APPLICATION VIA MS SCMDM

Cette section décrit la procédure de déploiement de Kaspersky Endpoint Security 8 for Smartphone via Mobile Device Manager.

DANS CETTE SECTION

CONCEPTION DE LA GESTION DE L'APPLICATION VIA MDM

L'administration des paramètres de Kaspersky Endpoint Security 8 for Smartphone via le serveur MDM est assurée par le fichier de modèle d'administration endpoint8_fr.adm. Il fait partie de la distribution de l'application (cf. la rubrique "Procédure de déploiement de l'application via MDM" à la page 79). Le modèle d'administration prévoit pour chacun des composants de l'application (cf. la rubrique "Présentation des composants de Kaspersky Endpoint Security 8 for Smartphone" à la page 14) un ensemble de stratégies qui assurent la configuration des paramètres pour le composant en question. Par défaut, aucune stratégie n'est définie à l'installation du modèle ce qui permet à l'utilisateur de personnaliser les paramètres de l'application.

Le composant Anti-Virus (cf. la rubrique "Anti-Virus Fichier" à la page 14) propose les stratégies suivantes :

- **Protection**. Cette stratégie assure la configuration de la protection des appareils mobiles contre les objets malveillants (cf. la rubrique "Protection" à la page 14).
- **Analyse à la demande.** Cette stratégie assure la configuration de l'analyse des appareils mobiles à la recherche d'éventuels objets malveillants (cf. la rubrique "Analyse à la demande" à la page 15).
- **Analyse programmée**. Cette stratégie assure l'exécution programmée de l'analyse des appareils mobiles.
- **Mise à jour selon planification**. Cette stratégie assure l'exécution automatique de la mise à jour programmée des bases de l'application (cf. la rubrique "Mise à jour" à la page 16).
- **Interdiction de la mise à jour en itinérance**. Cette stratégie permet d'interdire la mise à jour automatique des bases de l'application si les appareils mobiles d'utilisateurs sont en itinérance.
- **Source de la mise à jour**. Cette stratégie permet de sélectionner la source de notifications pour télécharger le paquet de mises à jour sur les appareils mobiles.

Le composant Antivol (à la page 16) propose les stratégies suivantes :

- **Verrouillage**. Cette stratégie assure la configuration de la fonction Verrouillage (à la page 16).
- **Affichage du texte en cas de verrouillage de l'appareil**. Cette stratégie permet de sélectionner le texte qui sera affiché à l'écran des appareils mobiles verrouillés.
- **Suppression**. Cette stratégie assure la configuration de la fonction Suppression (à la page 17).
- **Liste des dossiers à supprimer.** Cette stratégie permet de créer une liste de dossiers sur les appareils mobiles pour une suppression à distance.
- **Géolocalisation**. Cette stratégie assure la configuration de la fonction Géolocalisation (à la page 17).
- **SIM-Surveillance**. Cette stratégie assure la configuration de la fonction SIM-Surveillance (à la page 17).

Le composant Anti-Spam (à la page 17) propose la stratégie **Interdiction de l'utilisation de l'Antide l'Anti-Spam**, qui permet d'interdire ou d'autoriser son activation à l'utilisateur. Si l'activation de l'Antide l'Anti-Spam est autorisée, l'utilisateur prend soin de configurer les paramètres de fonctionnement de ce composant sur l'appareil mobile.

Le composant Contacts personnels (à la page 17) propose la stratégie **Interdiction de l'utilisation de Contacts personnels**, qui permet d'interdire ou d'autoriser son activation à l'utilisateur. Si l'activation de Contacts personnels est autorisée, l'utilisateur prend soin de configurer les paramètres de fonctionnement de ce composant sur l'appareil mobile.

Le composant Chiffrement (à la page 18) propose les stratégies suivantes :

- **Interdiction de l'accès aux données chiffrées**. Cette stratégie permet de verrouiller l'accès aux données chiffrées.
- **Liste des dossiers pour le chiffrement.** Cette stratégie permet de créer une liste des dossiers à chiffrer.

Le composant Pare-feu (à la page 18) propose les stratégies suivantes :

- **Mode du Pare-feu.** Cette stratégie assure la configuration du niveau de sécurité du Pare-feu.
- **Notification du Pare-feu**. Cette stratégie permet d'activer ou de désactiver la notification de l'utilisateur sur le blocage des connexions interdites.

L'installation de la licence sur les appareils mobiles d'utilisateurs est exécutée via le modèle d'administration à l'aide de la stratégie **Licence**.

Les stratégies permettent à l'administrateur de configurer les paramètres de Kaspersky Endpoint Security 8 for Smartphone avant d'installer l'application et de modifier les valeurs des paramètres après l'installation de l'application.

Attention ! La période de synchronisation des appareils mobiles avec le serveur MDM peut être différente de la période de la mise en place des stratégies.

PROCEDURE DU DEPLOIEMENT DE L'APPLICATION VIA MDM

La distribution de Kaspersky Endpoint Security 8 for Smartphone contient une archive auto-extractible KES8_forMicrosoftMDM_fr.exe avec des fichiers suivants qui assurent l'installation de l'application sur les appareils mobiles :

- endpoint_MDM_Afaria_8_0_x_xx_fr.cab : fichier d'installation de l'application pour le système d'exploitation Microsoft Windows Mobile ;
- endpoint8_fr.adm : fichier du modèle d'administration avec les paramètres des stratégies pour les gérer ;
- endpoint8_ca.cer : fichier de certification du centre de certification ;
- endpoint8_cert.cer : fichier de certification qui sert de signature pour le fichier d'installation de l'application ;
- kes2mdm.exe : utilitaire pour convertir le fichier de licence de l'application ;
- kl.pbv, licensing.dll, oper.pbv : ensemble de fichiers qui assurent le fonctionnement de l'utilitaire kes2mdm.exe.

Le déploiement de Kaspersky Endpoint Security 8 for Smartphone est effectué selon la procédure standard de déploiement du logiciel via Mobile Device Manager. D'abord, il faut créer un objet de stratégie de groupe pour enregistrer les paramètres de l'application et gérer les appareils mobiles. L'objet de stratégie est créé pour le groupe d'appareils enregistrés Active Directory® où il faut installer l'application. Ensuite, le modèle d'administration est installé dans l'objet de stratégie créé. Une fois le modèle installé, il faut configurer tous les paramètres requis de l'application et installer la licence. Pour diffuser l'application sur les appareils mobiles d'utilisateurs, il faut créer un paquet d'installation dans la console Mobile Device Manager Software Distribution. Le paquet d'installation sera copié sur l'appareil mobile lors de sa synchronisation avec le serveur MDM. Une fois copiée, l'application sera installée automatiquement sur les appareils mobiles sans intervention d'utilisateur.

Ainsi, l'installation de Kaspersky Endpoint Security 8 for Smartphone via Mobile Device Manager comprend les étapes suivantes :

1. Installation du modèle d'administration pour la gestion dans l'objet de stratégie de groupe.
2. Configuration des paramètres de l'application.
3. Installation de la licence à l'aide de l'utilitaire de conversion du fichier de licence.
4. Création d'un paquet d'installation de l'application et la diffusion de ce paquet sur les appareils mobiles d'utilisateurs.
5. Installation de l'application sur les appareils mobiles.

PREPARATION AU DEPLOIEMENT DE L'APPLICATION VIA MDM

Avant de déployer Kaspersky Endpoint Security 8 for Smartphone via Mobile Device Manager, l'administrateur doit s'assurer que les conditions suivantes sont satisfaites :

1. Microsoft System Center Mobile Device Manager est déployé et configuré dans le réseau.
2. Tous les appareils mobiles d'utilisateurs font partie du réseau et sont enregistrés dans le domaine.
3. Windows Server Update Services 3.0 SP1 est installé et configuré sur le serveur MDM.

DANS CETTE SECTION

SUR LE MODELE D'ADMINISTRATION

Le modèle d'administration pour la gestion de Kaspersky Endpoint Security 8 for Smartphone permet de configurer les stratégies de la gestion de l'application. C'est un fichier texte qui contient tous les paramètres requis de l'application. Ce fichier endpoint8_fr.adm fait partie de la distribution de l'application.

Pendant le déploiement de Kaspersky Endpoint Security 8 for Smartphone via Mobile Device Manager, il faut ajouter le modèle d'administration de l'application à l'objet de stratégie de groupe qui a été créé dans la console de gestion. Le modèle est installé sur le poste de travail de l'administrateur qui a l'autorisation de gérer les stratégies dans le contrôleur de domaine.

Attention ! La langue de modèle doit correspondre à celle du système d'exploitation installée sur le poste de travail de l'administrateur.

Vous pouvez configurer les stratégies pour tous les composants de l'application (cf. la rubrique "Configuration du modèle d'administration" à la page 81).

INSTALLATION DU MODELE D'ADMINISTRATION

Pour installer le modèle d'administration de Kaspersky Endpoint Security 8 for Smartphone, procédez comme suit :

1. Créez l'objet de stratégie de groupe dans la console de gestion (MMC).
2. Dans l'arborescence de la console, sélectionnez dans le nœud de l'objet créé le nœud **Configuration de l'ordinateur**, puis créez le groupe **Modèles d'administration**.
3. Sélectionnez dans le menu contextuel l'option **Ajout et suppression de modèles**.
4. Dans la fenêtre **Ajout et suppression de modèles** qui s'ouvre, cliquez sur **Ajouter**.
5. Sélectionnez dans la fenêtre qui s'ouvre le fichier de modèle endpoint8_fr.adm, enregistré sur le poste de travail de l'administrateur.
6. Dans la fenêtre **Ajout et suppression de modèles**, cliquez sur **Fermer**.

   Le groupe **Modèles d'administration** sera enrichi du groupe **Paramètres de Kaspersky Endpoint Security 8 for Smartphone** qui contient les groupes de paramètres pour chacun des composants de l'application (cf. ill. ci-après).

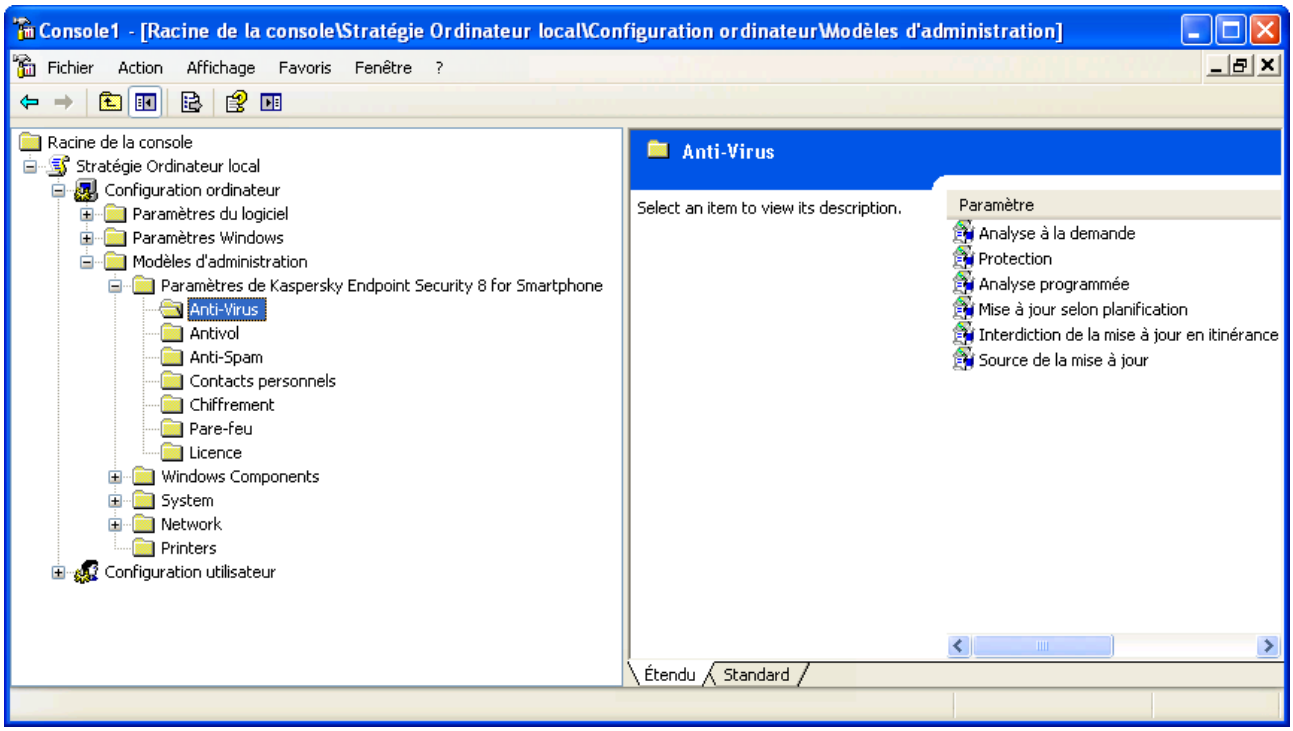


Figure 39 : modèle d'administration

CONFIGURATION DU MODELE D'ADMINISTRATION

Tous les paramètres de fonctionnement de Kaspersky Endpoint Security 8 for Smartphone, activation de la licence comprise, sont définis via les stratégies. Les informations relatives aux paramètres de l'application définis dans les stratégies sont enregistrées sur le serveur MDM et diffusées sur les appareils mobiles lors de la synchronisation.

Pour configurer le modèle d'administration, procédez comme suit :

1. Dans l'arborescence de la console de gestion, sélectionnez l'objet de stratégie de groupe, dont les paramètres de Kaspersky Endpoint Security 8 for Smartphone vous souhaitez configurer.
2. Sélectionnez le nœud **Configuration de l'ordinateur**.
3. Sélectionnez le dossier **Modèles d'administration**, ensuite le dossier **Paramètres de Kaspersky Endpoint Security 8 for Smartphone**.
4. Sélectionnez le dossier avec le nom du composant de l'application, dont les paramètres vous souhaitez configurer (cf. la rubrique "Présentation des composants de Kaspersky Endpoint Security 8 for Smartphone" à la page 14).

   La partie droite de la fenêtre de console affichera les stratégies qui assurent la configuration du composant sélectionné (cf. la rubrique "Conception de la gestion de l'application via MDM" à la page 78).

Les sections suivantes présentent les procédures détaillées pour configurer les stratégies de chacun des composants de l'application.

DANS CETTE SECTION

CONFIGURATION DE LA STRATEGIE PROTECTION

Pour configurer la stratégie Protection, procédez comme suit :

1. Dans l'arborescence de la console de gestion, sélectionnez le dossier **Anti-Virus**.
2. Dans la partie droite de la fenêtre de console de gestion, sélectionnez la stratégie **Protection**.
3. Dans le menu contextuel de la stratégie, sélectionnez l'option **Propriétés**.

   La fenêtre **Propriétés de Protection** s'affiche (cf. ill. ci-après).

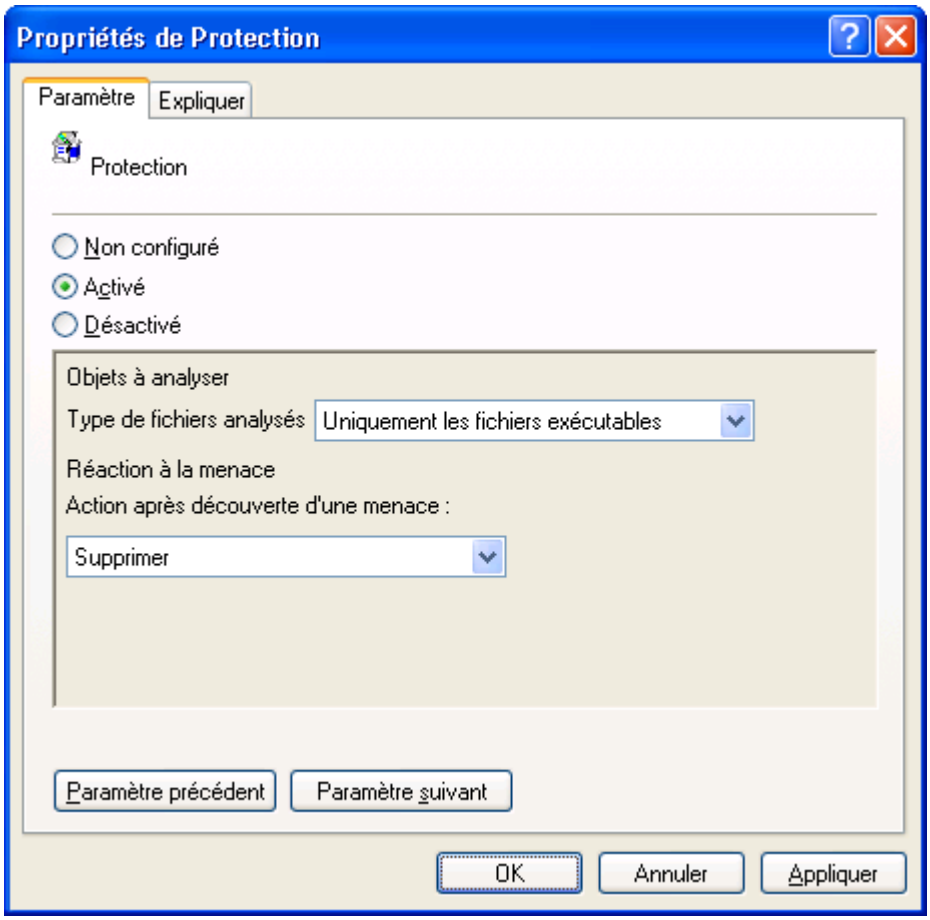


*Figure 40 : fenêtre **Propriétés: Protection***

4. Sous l'onglet **Paramètre**, sélectionnez une des options suivantes :

   - **Non configuré**. Le Composant / la fonction sont activés sur l'appareil mobile de l'utilisateur. Les paramètres définis par la stratégie peuvent être modifiés par l'utilisateur sur l'appareil mobile.

     Dans ce cas, le composant / la fonction utilisent les paramètres définis par l'utilisateur.

   - **Activé**. Le Composant / la fonction sont activés sur l'appareil mobile de l'utilisateur. Paramètres définis par la stratégie ne peuvent pas être modifiés par l'utilisateur sur l'appareil mobile. Dans ce cas, un verrou est affiché dans le coin supérieur gauche de l'écran de l'appareil.

     Le composant / la fonction utilisent les paramètres définis par la stratégie. En sélectionnant cette option, vous pouvez toujours configurer les paramètres de la stratégie.

   - **Désactivé**. Le Composant / la fonction définis par la stratégie sont désactivés sur l'appareil mobile de l'utilisateur. Impossible de modifier les paramètres. Dans ce cas, un verrou est affiché dans le coin supérieur gauche de l'écran de l'appareil.

5. Dans la liste déroulante **Type de fichiers analysés**, sélectionnez le type de fichiers à analyser par Kaspersky Endpoint Security 8 for Smartphone. Valeurs possibles :
   - **Tous les fichiers**. L'application analyse les fichiers de tous les types.
   - **Uniquement les fichiers exécutables**. L'application analyse uniquement les fichiers exécutables des formats suivants : EXE, DLL, SIS, MDL, APP, RDL, PRT, PXT, LDD, PDD, CLASS.
6. Dans la liste déroulante **Action après découverte d'une menace**, sélectionnez l'action à effectuer en cas de découverte d'un objet malveillant. Valeurs possibles :
   - **Supprimer**. Les objets malveillants sont supprimés sans notification de l'utilisateur.
   - **Consigner**. Les objets malveillants ne sont pas modifiés, mais les informations relatives à leur découverte sont consignées dans le journal de l'application. Les requêtes envoyées à l'objet (par exemple, tentative de copie ou d'ouverture) seront bloquées.
   - **Placer en quarantaine.** Les objets infectés détectés sont placés en quarantaine.

CONFIGURATION DE LA STRATEGIE ANALYSE A LA DEMANDE

Pour configurer la stratégie Analyse à la demande, procédez comme suit :

1. Dans l'arborescence de la console de gestion, sélectionnez le dossier **Anti-Virus**.
2. Dans la partie droite de la fenêtre de console de gestion, sélectionnez la stratégie **Analyse à la demande**.
3. Dans le menu contextuel de la stratégie, sélectionnez l'option **Propriétés**.

   La fenêtre **Propriétés de Analyse à la demande** s'affiche (cf. ill. ci-après).

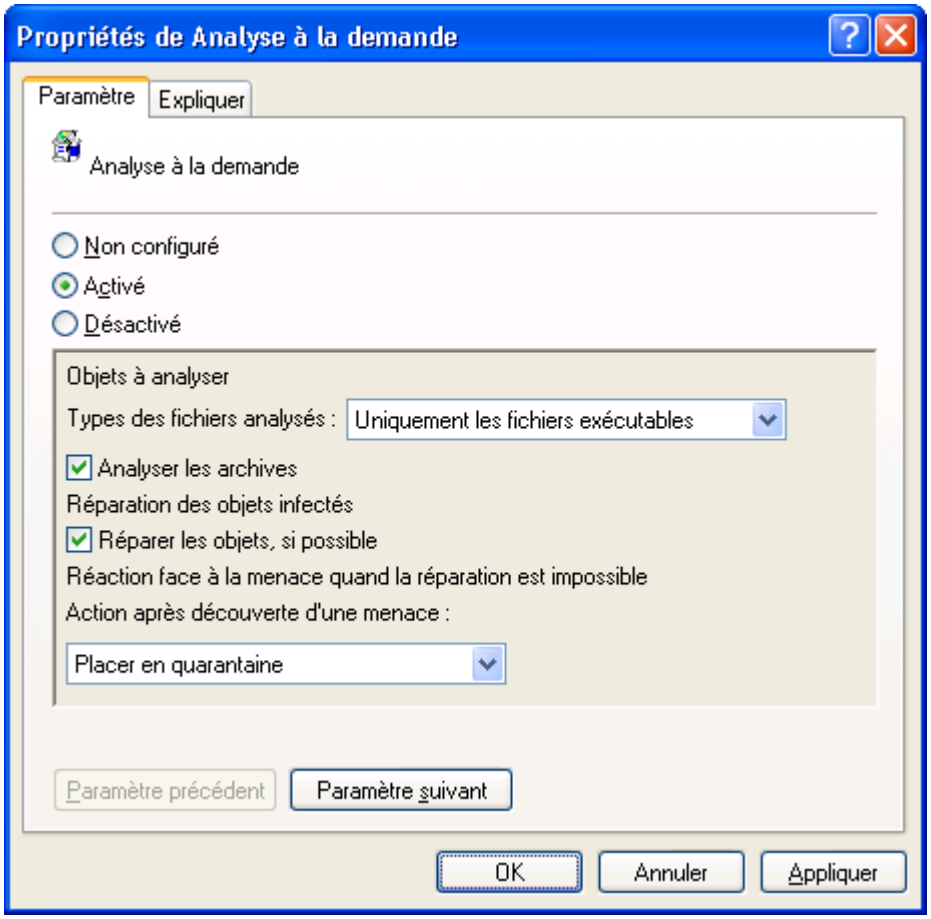


*Figure 41 : fenêtre **Propriétés : analyse à la demande***

4. Sous l'onglet **Paramètre**, sélectionnez une des options suivantes :

   - **Non configuré**. Le Composant / la fonction sont activés sur l'appareil mobile de l'utilisateur. Les paramètres définis par la stratégie peuvent être modifiés par l'utilisateur sur l'appareil mobile.

     Dans ce cas, le composant / la fonction utilisent les paramètres définis par l'utilisateur.

   - **Activé**. Le Composant / la fonction sont activés sur l'appareil mobile de l'utilisateur. Paramètres définis par la stratégie ne peuvent pas être modifiés par l'utilisateur sur l'appareil mobile. Dans ce cas, un verrou est affiché dans le coin supérieur gauche de l'écran de l'appareil.

     Le composant / la fonction utilisent les paramètres définis par la stratégie. En sélectionnant cette option, vous pouvez toujours configurer les paramètres de la stratégie.

5. Dans la liste déroulante **Types de fichiers analysés**, sélectionnez le type de fichiers à analyser par Kaspersky Endpoint Security 8 for Smartphone. Valeurs possibles :

   - **Tous les fichiers**. L'application analyse les fichiers de tous les types.
   - **Uniquement les fichiers exécutables**. L'application analyse uniquement les fichiers exécutables des formats suivants : EXE, DLL, SIS, MDL, APP, RDL, PRT, PXT, LDD, PDD, CLASS. Dans ce cas, les archives ne sont ni décompactées, ni analysées.

6. Cochez la case **Analyser les archives**, pour que Kaspersky Endpoint Security 8 for Smartphone analyse les fichiers archivés. L'application analyse les archives des formats suivants : ZIP, JAR, JAD, SIS и SISX.

   Si la case **Analyser les archives** n'est pas cochée et si dans la liste déroulante **Types de fichiers analysés** l'option **Tous les fichiers** est sélectionnée, l'application va analyser tous les fichiers sauf les fichiers archivés.

7. Cochez la case **Réparer les objets, si possible** pour permettre à l'application de réparer les objets malveillants. Si la réparation est impossible, l'application exécute l'action sélectionnée dans la liste déroulante **Action après découverte d'une menace**.

8. Dans la liste déroulante **Action après découverte d'une menace**, sélectionnez l'action à effectuer en cas de découverte d'un objet malveillant. Valeurs possibles :

   - **Supprimer**. Les objets malveillants sont supprimés sans notification de l'utilisateur.
   - **Consigner**. Les objets malveillants ne sont pas modifiés, mais les informations relatives à leur découverte sont consignées dans le journal de l'application. Les requêtes envoyées à l'objet (par exemple, tentative de copie ou d'ouverture) seront bloquées.
   - **Placer en quarantaine.** Les objets infectés détectés sont placés en quarantaine. Cette action est sélectionnée par défaut.
   - **Confirmer l'action.** Quand un objet malveillant est découvert, une notification proposant plusieurs actions à choisir s'affiche :
     - **Ignorer**.
     - **Placer en quarantaine.**
     - **Supprimer**.
     - **Tenter de réparer**.

CONFIGURATION DE LA STRATEGIE ANALYSE PROGRAMMEE

Pour configurer la stratégie Analyse programmée, procédez comme suit :

1. Dans l'arborescence de la console de gestion, sélectionnez le dossier **Anti-Virus**.
2. Dans la partie droite de la fenêtre de console de gestion, sélectionnez la stratégie **Analyse programmée**.
3. Dans le menu contextuel de la stratégie, sélectionnez l'option **Propriétés**.

   La fenêtre **Propriétés de Analyse programmée** s'affiche (cf. ill. ci-après).

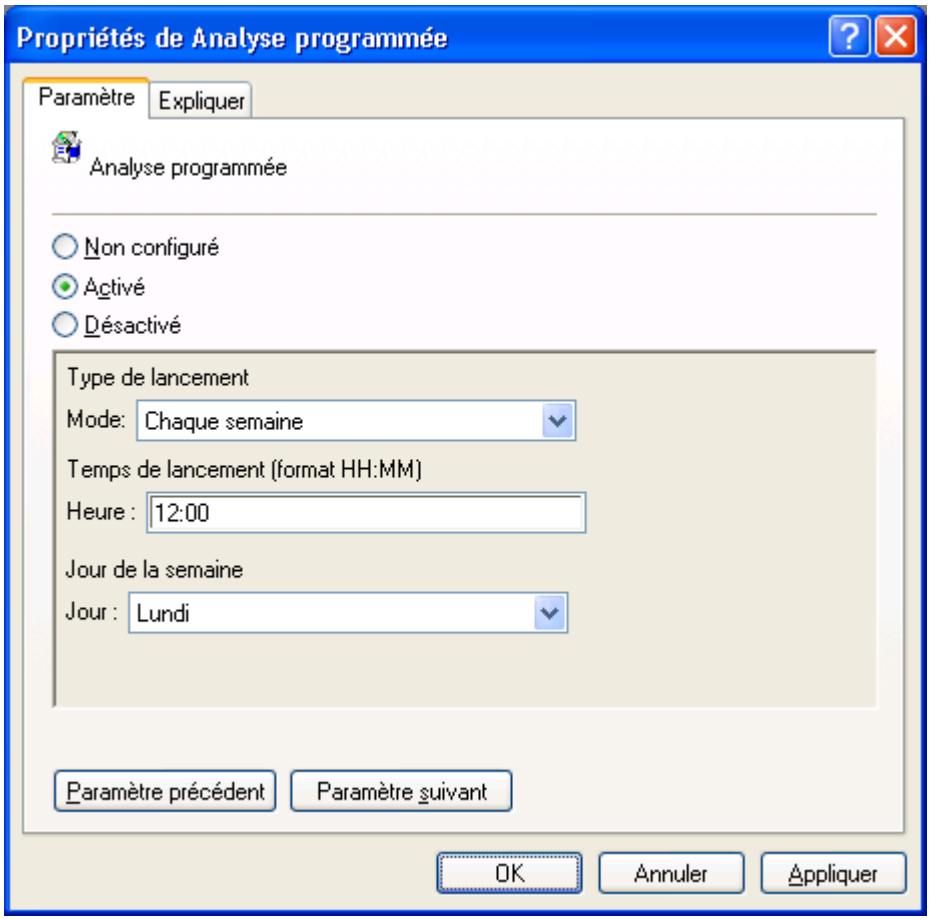


*Figure 42 : fenêtre **Propriétés : Analyse programmée***

4. Sous l'onglet **Paramètre**, sélectionnez une des options suivantes :

   - **Non configuré**. Le Composant / la fonction sont activés sur l'appareil mobile de l'utilisateur. Les paramètres définis par la stratégie peuvent être modifiés par l'utilisateur sur l'appareil mobile.

     Dans ce cas, le composant / la fonction utilisent les paramètres définis par l'utilisateur.

   - **Activé**. Le Composant / la fonction sont activés sur l'appareil mobile de l'utilisateur. Paramètres définis par la stratégie ne peuvent pas être modifiés par l'utilisateur sur l'appareil mobile. Dans ce cas, un verrou est affiché dans le coin supérieur gauche de l'écran de l'appareil.

     Le composant / la fonction utilisent les paramètres définis par la stratégie. En sélectionnant cette option, vous pouvez toujours configurer les paramètres de la stratégie.

5. Dans la liste déroulante **Mode**, sélectionnez le mode de lancement de l'analyse à la demande. Valeurs possibles :
   - **Manuel** L'utilisateur peut lancer l'analyse à la main en temps voulu.
   - **Chaque jour** L'analyse sera exécutée tous les jours en temps voulu. Dans le champ qui suit (**Heure**), sélectionnez l'heure de lancement au format HH:MM.
   - **Chaque semaine** L'analyse sera exécutée une fois par semaine le jour que vous avez sélectionné et en temps voulu. Dans la liste déroulante qui suit (**Jour**), sélectionnez le jour de la semaine, dans le champ **Heure** sélectionnez l'heure de lancement au format HH:MM.

CONFIGURATION DE LA STRATEGIE MISE A JOUR SELON PLANIFICATION

Pour configurer la stratégie Mise à jour selon planification, procédez comme suit :

1. Dans l'arborescence de la console de gestion, sélectionnez le dossier **Anti-Virus**.
2. Dans la partie droite de la fenêtre de console de gestion, sélectionnez la stratégie **Mise à jour selon planification**.
3. Dans le menu contextuel de la stratégie, sélectionnez l'option **Propriétés**.

   La fenêtre **Propriétés de Mise à jour selon planification** s'affiche (cf. ill. ci-après).

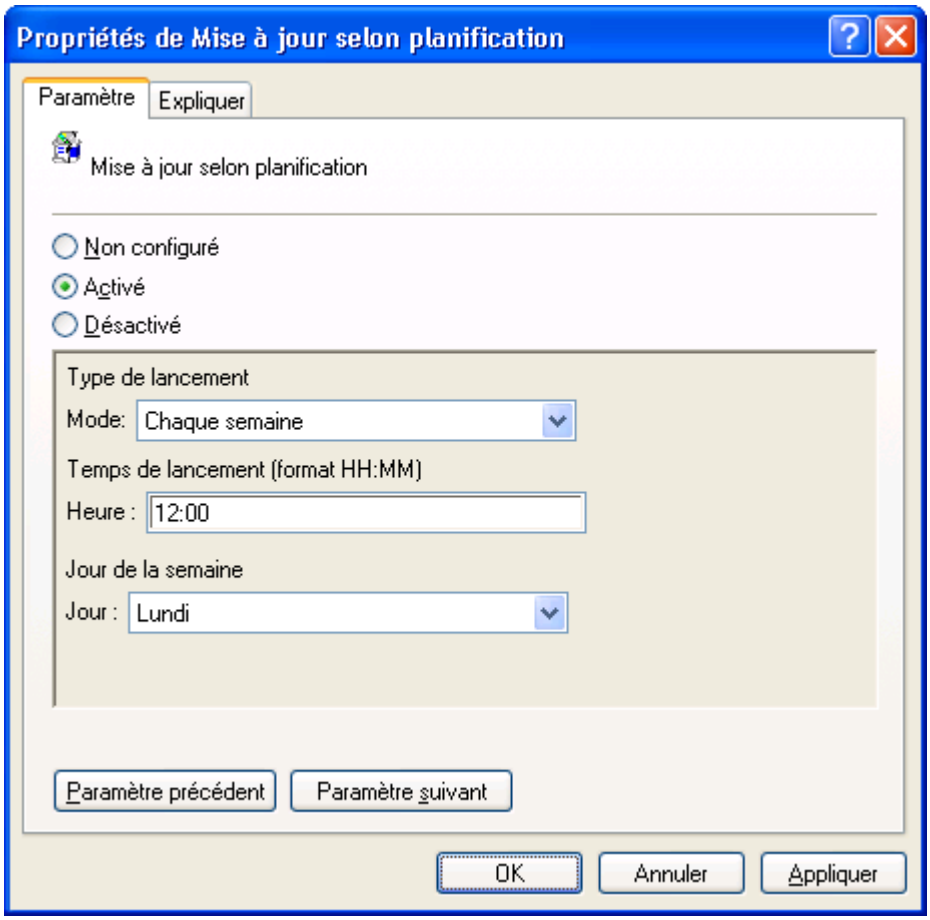


*Figure 43: fenêtre **Propriétés : Mise à jour selon planification***

4. Sous l'onglet **Paramètre**, sélectionnez une des options suivantes :
   - **Non configuré**. Le Composant / la fonction sont activés sur l'appareil mobile de l'utilisateur. Les paramètres définis par la stratégie peuvent être modifiés par l'utilisateur sur l'appareil mobile.

     Dans ce cas, le composant / la fonction utilisent les paramètres définis par l'utilisateur.
   - **Activé**. Le Composant / la fonction sont activés sur l'appareil mobile de l'utilisateur. Paramètres définis par la stratégie ne peuvent pas être modifiés par l'utilisateur sur l'appareil mobile. Dans ce cas, un verrou est affiché dans le coin supérieur gauche de l'écran de l'appareil.

Le composant / la fonction utilisent les paramètres définis par la stratégie. En sélectionnant cette option, vous pouvez toujours configurer les paramètres de la stratégie.

5. Dans la liste déroulante **Mode**, sélectionnez le mode de lancement de la mise à jour des bases de l'application. Valeurs possibles :

   - **Manuel** L'utilisateur peut lancer la mise à jour des bases à la main en temps voulu.
   - **Chaque jour** La mise à jour des bases de l'application sera effectuée tous les jours en temps voulu. Dans le champ qui suit (**Heure**), sélectionnez l'heure de lancement pour une journée de 24h au format (HH:MM).
   - **Chaque semaine** La mise à jour des bases de l'application sera exécutée une fois par semaine le jour que vous avez sélectionné et en temps voulu. Dans la liste déroulante qui suit (**Jour**), sélectionnez le jour de la semaine, dans le champ **Heure** sélectionnez l'heure de lancement pour une journée de 24h au format (HH:MM).

CONFIGURATION DE LA STRATEGIE INTERDICTION DE LA MISE A JOUR EN ITINERANCE

Pour configurer la stratégie Interdiction de la mise à jour en itinérance, procédez comme suit :

1. Dans l'arborescence de la console de gestion, sélectionnez le dossier **Anti-Virus**.
2. Dans la partie droite de la fenêtre de console de gestion, sélectionnez la stratégie **Interdiction de la mise à jour en itinérance**.
3. Dans le menu contextuel de la stratégie, sélectionnez l'option **Propriétés**.

   La fenêtre **Propriétés de Interdiction de la mise à jour en itinérance** s'affiche (cf. ill. ci-après).

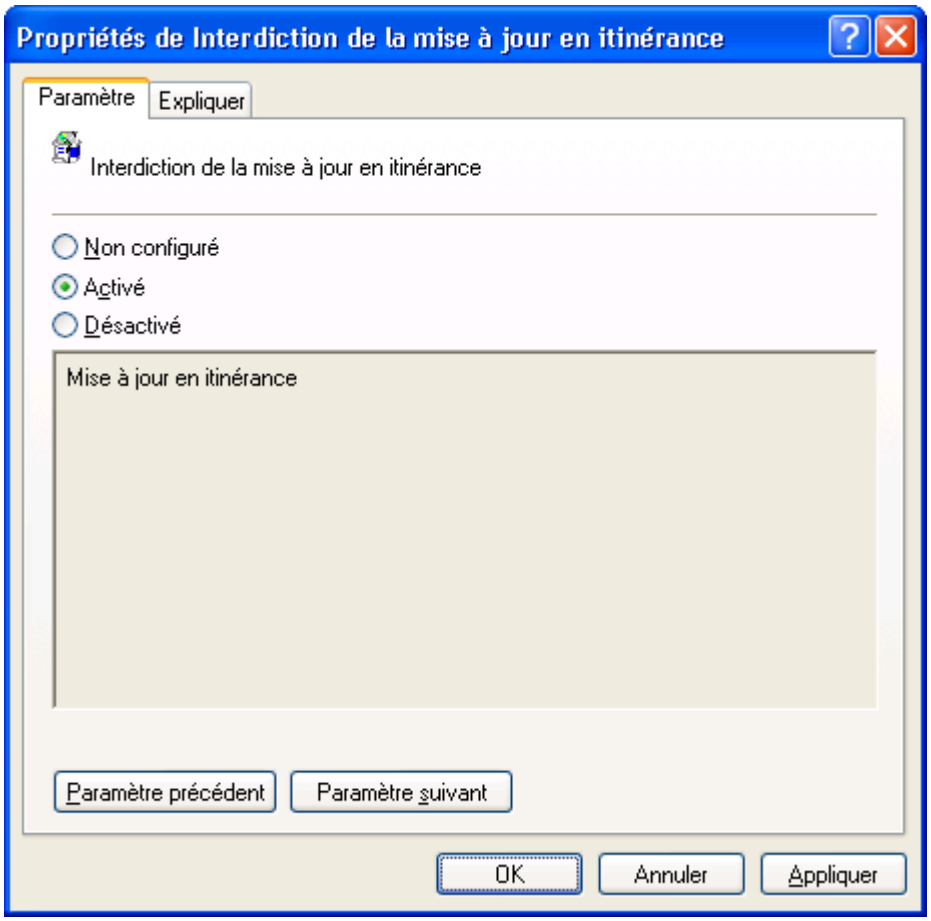


*Figure 44: Fenêtre **Propriétés : interdiction de la mise à jour en itinérance***

Pour interdire la mise à jour automatique des bases de l'application lorsque l'appareil mobile de l'utilisateur est en itinérance, sous l'onglet **Paramètre** sélectionnez l'option **Activé**.

Pour autoriser la mise à jour automatique des bases de l'application lorsque l'appareil mobile de l'utilisateur est en itinérance, sous l'onglet **Paramètre** sélectionnez l'option **Désactivé**.

Pour laisser l'utilisateur configurer l'interdiction de la mise à jour en itinérance, sous l'onglet **Paramètre**, sélectionnez l'option **Non configuré**.

CONFIGURATION DE LA STRATEGIE SOURCE DE MISES A JOUR

Pour configurer la stratégie Source de la mise à jour, procédez comme suit :

1. Dans l'arborescence de la console d'administration, sélectionnez le dossier **Antivirus**.
2. Dans la partie droite de la fenêtre de console de gestion, sélectionnez la stratégie **Source de la mise à jour**.
3. Dans le menu contextuel de la stratégie, sélectionnez l'option **Propriétés**.

   La fenêtre **Propriétés de Source de la mise à jour** s'affiche (cf. ill. ci-après).

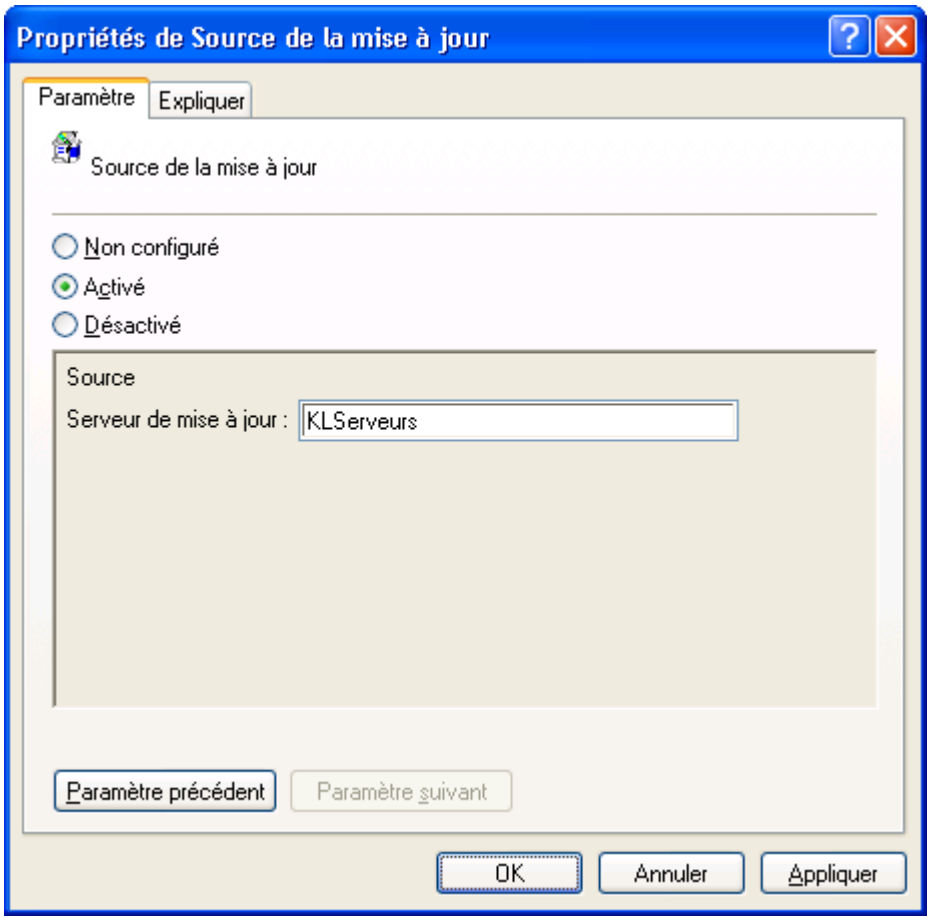


*Figure 45 : fenêtre **Propriétés : Source de la mise à jour***

4. Sous l'onglet **Paramètre**, sélectionnez une des options suivantes :

   - **Non configuré**. Le Composant / la fonction sont activés sur l'appareil mobile de l'utilisateur. Les paramètres définis par la stratégie peuvent être modifiés par l'utilisateur sur l'appareil mobile.

     Dans ce cas, le composant / la fonction utilisent les paramètres définis par l'utilisateur.

   - **Activé**. Le Composant / la fonction sont activés sur l'appareil mobile de l'utilisateur. Paramètres définis par la stratégie ne peuvent pas être modifiés par l'utilisateur sur l'appareil mobile. Dans ce cas, un verrou est affiché dans le coin supérieur gauche de l'écran de l'appareil.

     Le composant / la fonction utilisent les paramètres définis par la stratégie. En sélectionnant cette option, vous pouvez toujours configurer les paramètres de la stratégie.

5. Dans le champ **Serveur de mise à jour**, spécifiez l'adresse de la source de notifications des bases de l'application pour télécharger les mises à jour sur les appareils mobiles.

Pour télécharger les mises à jour des bases de l'application depuis les serveurs de mises à jour de Kaspersky Lab, saisissez dans ce champ l'adresse suivante : KL Servers.

Pour télécharger les mises à jour des bases de l'application depuis un autre serveur de mises à jour, spécifiez un serveur HTTP, un serveur local ou un répertoire réseau. Par exemple, http://domain.com/index/.

La structure des dossiers dans la source de la mise à jour doit être identique à celle du serveur de mise à jour Kaspersky Lab.

CONFIGURATION DE LA STRATEGIE VERROUILLAGE

Pour configurer la stratégie Verrouillage, procédez comme suit :

1. Dans l'arborescence de la console de gestion, sélectionnez le dossier **Antivol**
2. Dans la partie droite de la fenêtre de console de gestion, sélectionnez la stratégie **Verrouillage**.
3. Dans le menu contextuel de la stratégie, sélectionnez l'option **Propriétés**.

   La fenêtre **Propriétés de Verrouillage** s'affiche (cf. ill. ci-après).

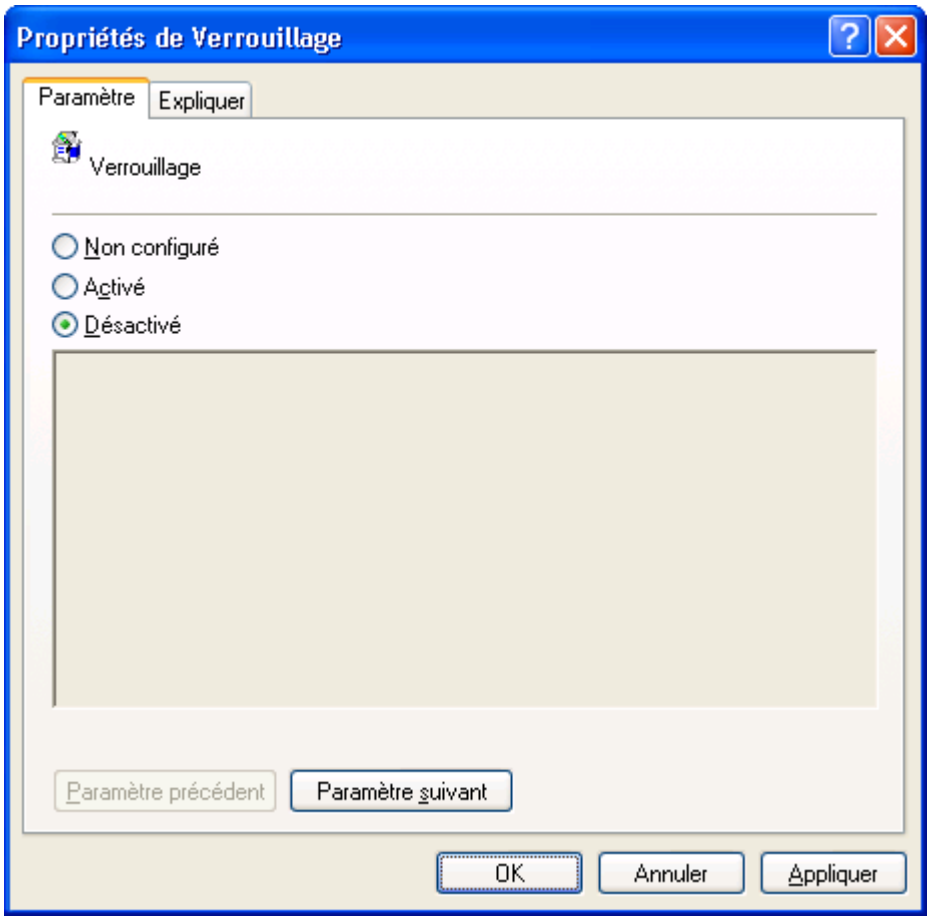


*Figure 46 : fenêtre **Propriétés : Verrouillage***

4. Pour activer la possibilité de verrouiller l'appareil mobile de l'utilisateur à distance, sélectionnez sous l'onglet **Paramètre** l'option **Activé**.

   Pour désactiver la fonction Verrouillage, sélectionnez sous l'onglet **Paramètre** l'option **Désactivé**.

   Pour laisser l'utilisateur activer ou désactiver la fonction Verrouillage, sélectionnez sous l'onglet **Paramètre** l'option **Non configuré**.

CONFIGURATION DE LA STRATEGIE AFFICHAGE DU TEXTE EN CAS DE VERROUILLAGE DE L'APPAREIL

Pour configurer la stratégie Affichage du texte en cas de verrouillage de l'appareil, procédez comme suit :

1. Dans l'arborescence de la console de gestion, sélectionnez le dossier **Antivol**.
2. Dans la partie droite de la fenêtre de console de gestion, sélectionnez la stratégie **Affichage du texte en cas de verrouillage de l'appareil**.
3. Dans le menu contextuel de la stratégie, sélectionnez l'option **Propriétés**.

   La fenêtre **Propriétés de Affichage du texte en cas de verrouillage de l'appareil** s'affiche (cf. ill. ci-après).

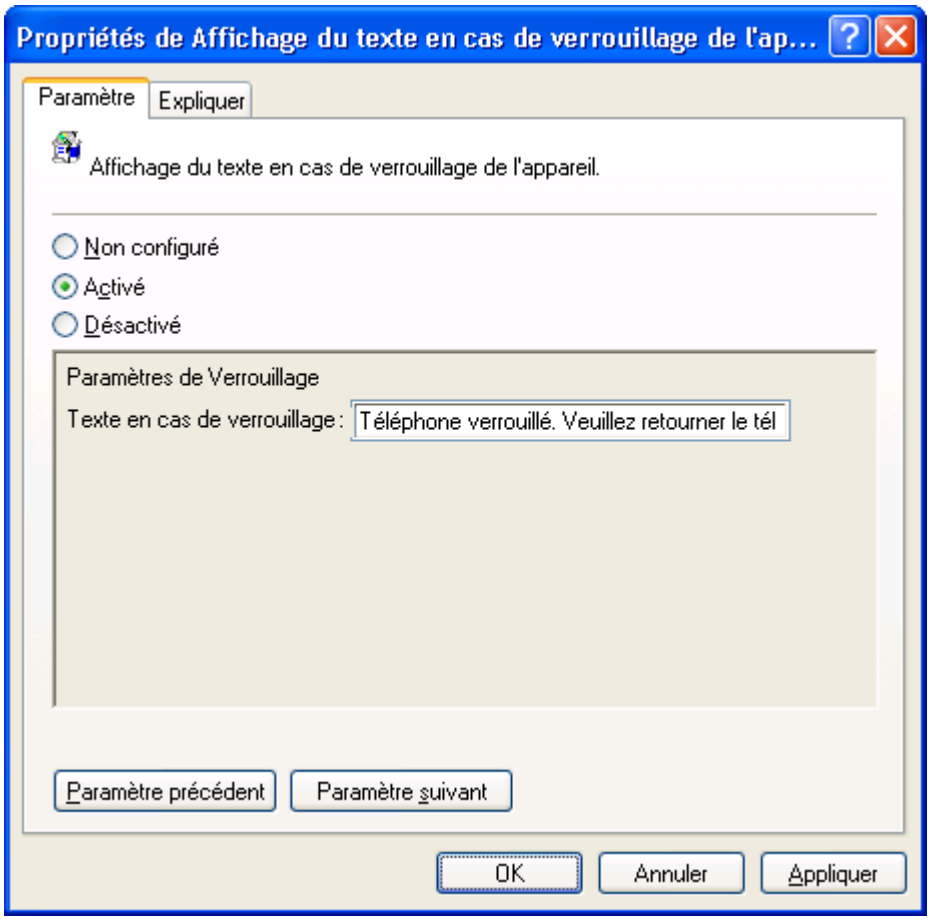


*Figure 47 : La fenêtre **Propriétés de Affichage du texte en cas de verrouillage de l'appareil***

4. Sous l'onglet **Paramètre**, sélectionnez une des options suivantes :

   - **Non configuré**. Le Composant / la fonction sont activés sur l'appareil mobile de l'utilisateur. Les paramètres définis par la stratégie peuvent être modifiés par l'utilisateur sur l'appareil mobile.

     Dans ce cas, le composant / la fonction utilisent les paramètres définis par l'utilisateur.

   - **Activé**. Le Composant / la fonction sont activés sur l'appareil mobile de l'utilisateur. Paramètres définis par la stratégie ne peuvent pas être modifiés par l'utilisateur sur l'appareil mobile. Dans ce cas, un verrou est affiché dans le coin supérieur gauche de l'écran de l'appareil.

     Le composant / la fonction utilisent les paramètres définis par la stratégie. En sélectionnant cette option, vous pouvez toujours configurer les paramètres de la stratégie.

5. Dans le champ **Texte en cas de verrouillage**, saisissez le texte qui apparaîtra sur l'écran de l'appareil verrouillé.

CONFIGURATION DE LA STRATEGIE SUPPRESSION

Pour configurer la stratégie Suppression, procédez comme suit :

1. Dans l'arborescence de la console de gestion, sélectionnez le dossier **Antivol**
2. Dans la partie droite de la fenêtre de console de gestion, sélectionnez la stratégie **Suppression**.
3. Dans le menu contextuel de la stratégie, sélectionnez l'option **Propriétés**.

   La fenêtre **Propriétés de Suppression** s'affiche (cf. ill. ci-après).

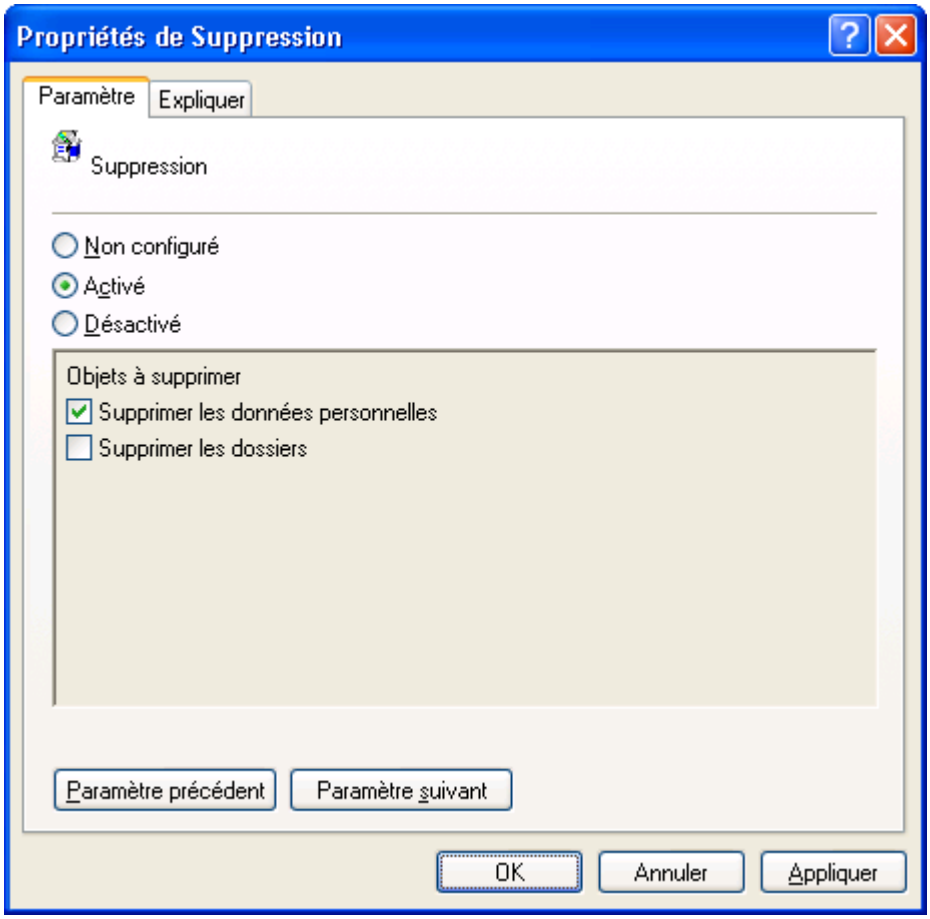


*Figure 48 : fenêtre **Propriétés : Suppression***

4. Sous l'onglet **Paramètre**, sélectionnez une des options suivantes :

   - **Non configuré**. Le Composant / la fonction sont activés sur l'appareil mobile de l'utilisateur. Les paramètres définis par la stratégie peuvent être modifiés par l'utilisateur sur l'appareil mobile.

     Dans ce cas, le composant / la fonction utilisent les paramètres définis par l'utilisateur.

   - **Activé**. Le Composant / la fonction sont activés sur l'appareil mobile de l'utilisateur. Paramètres définis par la stratégie ne peuvent pas être modifiés par l'utilisateur sur l'appareil mobile. Dans ce cas, un verrou est affiché dans le coin supérieur gauche de l'écran de l'appareil.

     Le composant / la fonction utilisent les paramètres définis par la stratégie. En sélectionnant cette option, vous pouvez toujours configurer les paramètres de la stratégie.

     Attention ! En activant la stratégie Suppression, spécifiez au moins un paramètre de cette stratégie.

   - **Désactivé**. Le Composant / la fonction définis par la stratégie sont désactivés sur l'appareil mobile de l'utilisateur. Impossible de modifier les paramètres. Dans ce cas, un verrou est affiché dans le coin supérieur gauche de l'écran de l'appareil.

5. Cochez la case **Supprimer les données personnelles** pour autoriser Kaspersky Endpoint Security 8 for Smartphone à supprimer toutes les données personnelles (par exemple, contacts, SMS, galerie) stockées sur l'appareil mobile à la réception de l'instruction de l'utilisateur.
6. Cochez la case **Supprimer les dossiers**, pour autoriser Kaspersky Endpoint Security 8 for Smartphone à supprimer les dossiers sélectionnés stockés sur l'appareil mobile de l'utilisateur.

CONFIGURATION DE LA STRATEGIE LISTE DES DOSSIERS A SUPPRIMER

Pour configurer la stratégie Liste des dossiers à supprimer, procédez comme suit :

1. Dans l'arborescence de la console de gestion, sélectionnez le dossier **Antivol**
2. Dans la partie droite de la fenêtre de console de gestion, sélectionnez la stratégie **Liste des dossiers à supprimer**.
3. Dans le menu contextuel de la stratégie, sélectionnez l'option **Propriétés**.

   La fenêtre **Propriétés de Liste des dossiers à supprimer** s'affiche (cf. ill. ci-après).

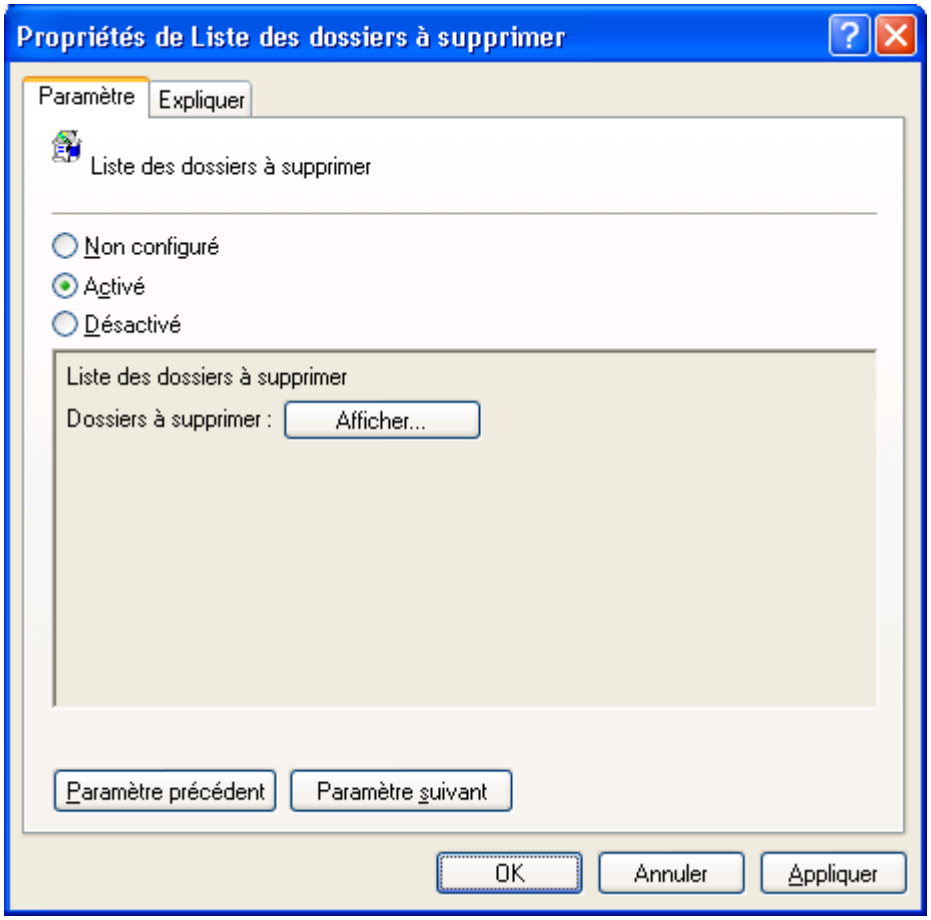


*Figure 49 : fenêtre **Propriétés : Liste des dossiers à supprimer***

4. Sous l'onglet **Paramètre**, sélectionnez une des options suivantes :
   - **Non configuré**. L'utilisateur définit la liste des dossiers à supprimer sur l'appareil mobile.
   - **Activé**. La liste des dossiers à supprimer est créée soit par l'utilisateur sur l'appareil mobile, soit par l'administrateur. La liste des dossiers à supprimer ajoutée par l'administrateur ne peut pas être modifiée ou supprimée par l'utilisateur.
5. Cliquez sur **Afficher**, puis créez dans la fenêtre qui s'ouvre la liste des dossiers à supprimer en cliquant sur **Ajouter** ou **Supprimer**.

CONFIGURATION DE LA STRATEGIE GEOLOCALISATION

Pour configurer la stratégie Géolocalisation, procédez comme suit :

1. Dans l'arborescence de la console de gestion, sélectionnez le dossier **Antivol**
2. Dans la partie droite de la fenêtre de console de gestion, sélectionnez la stratégie **Géolocalisation**.
3. Dans le menu contextuel de la stratégie, sélectionnez l'option **Propriétés**.

   La fenêtre **Propriétés de Géolocalisation** s'affiche (cf. ill. ci-après).

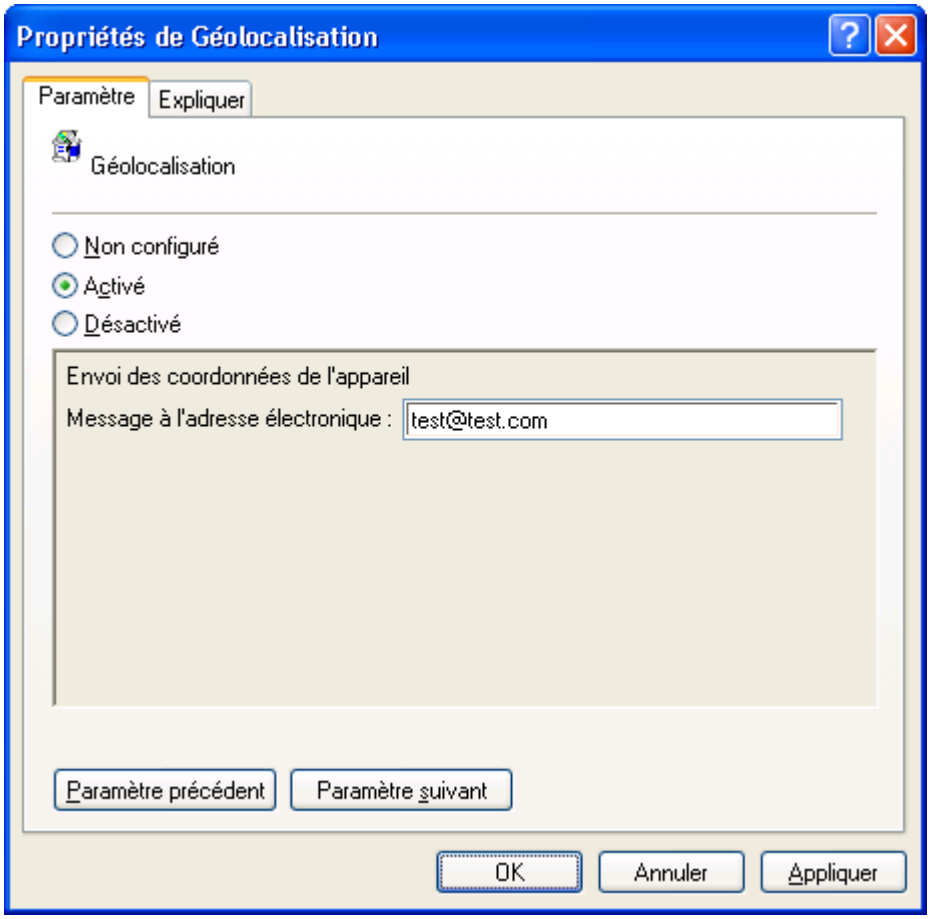


*Figure 50 : fenêtre **Propriétés : Géolocalisation***

4. Sous l'onglet **Paramètre**, sélectionnez une des options suivantes :
   - **Non configuré**. Le Composant / la fonction sont activés sur l'appareil mobile de l'utilisateur. Les paramètres définis par la stratégie peuvent être modifiés par l'utilisateur sur l'appareil mobile.

     Dans ce cas, le composant / la fonction utilisent les paramètres définis par l'utilisateur.
   - **Activé**. Le Composant / la fonction sont activés sur l'appareil mobile de l'utilisateur. Paramètres définis par la stratégie ne peuvent pas être modifiés par l'utilisateur sur l'appareil mobile. Dans ce cas, un verrou est affiché dans le coin supérieur gauche de l'écran de l'appareil.

     Le composant / la fonction utilisent les paramètres définis par la stratégie. En sélectionnant cette option, vous pouvez toujours configurer les paramètres de la stratégie.
   - **Désactivé**. Le Composant / la fonction définis par la stratégie sont désactivés sur l'appareil mobile de l'utilisateur. Impossible de modifier les paramètres. Dans ce cas, un verrou est affiché dans le coin supérieur gauche de l'écran de l'appareil.
5. Saisissez dans le champ **Message à l'adresse électronique** l'adresse électronique pour envoyer un message avec les coordonnées géographiques de l'appareil mobile de l'utilisateur.

CONFIGURATION DE LA STRATEGIE SIM-SURVEILLANCE

Pour configurer la stratégie SIM-Surveillance, procédez comme suit :

1. Dans l'arborescence de la console de gestion, sélectionnez le dossier **Antivol**.
2. Dans la partie droite de la fenêtre de console de gestion, sélectionnez la stratégie **SIM-Surveillance**.
3. Dans le menu contextuel de la stratégie, sélectionnez l'option **Propriétés**.

   La fenêtre **Propriété de SIM-Surveillance** s'affiche (cf. ill. ci-après).

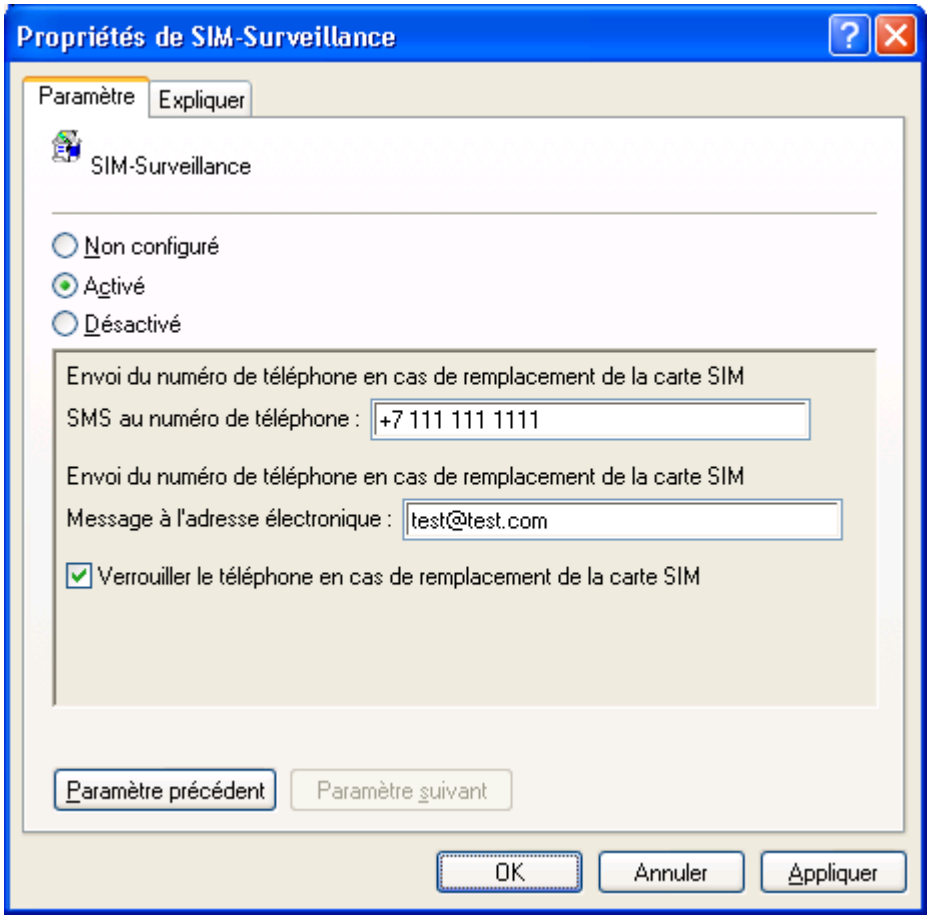


*Figure 51 : fenêtre **Propriétés : SIM-Surveillance***

4. Sous l'onglet **Paramètre**, sélectionnez une des options suivantes :

   - **Non configuré**. Le Composant / la fonction sont activés sur l'appareil mobile de l'utilisateur. Les paramètres définis par la stratégie peuvent être modifiés par l'utilisateur sur l'appareil mobile.

     Dans ce cas, le composant / la fonction utilisent les paramètres définis par l'utilisateur.

   - **Activé**. Le Composant / la fonction sont activés sur l'appareil mobile de l'utilisateur. Paramètres définis par la stratégie ne peuvent pas être modifiés par l'utilisateur sur l'appareil mobile. Dans ce cas, un verrou est affiché dans le coin supérieur gauche de l'écran de l'appareil.

     Le composant / la fonction utilisent les paramètres définis par la stratégie. En sélectionnant cette option, vous pouvez toujours configurer les paramètres de la stratégie.

     Attention ! En activant la stratégie SIM-Surveillance, spécifiez au moins un paramètre de cette stratégie.

   - **Désactivé**. Le Composant / la fonction définis par la stratégie sont désactivés sur l'appareil mobile de l'utilisateur. Impossible de modifier les paramètres. Dans ce cas, un verrou est affiché dans le coin supérieur gauche de l'écran de l'appareil.

5. Saisissez dans le champ **SMS au numéro de téléphone** le numéro de téléphone pour y envoyer en cas de remplacement de la carte SIM un SMS avec le nouveau numéro de téléphone qui correspond à la carte SIM insérée. Ces numéros peuvent commencer par un chiffre ou par le signe "+" et ne peuvent contenir que des chiffres.
6. Saisissez dans le champ **Message à l'adresse électronique** l'adresse électronique pour envoyer un message avec le nouveau numéro de téléphone qui correspond à la carte SIM insérée.
7. Cochez la case **Verrouiller le téléphone en cas de remplacement de la carte SIM** si vous souhaitez que l'application verrouille l'appareil en cas de remplacement de la carte SIM ou si l'appareil est allumé sans carte. L'appareil ne pourra être déverrouillé qu'après avoir entré le code secret.

CONFIGURATION DE LA STRATEGIE INTERDICTION DE L'UTILISATION DE L'ANTIDE L'ANTI-SPAM

Pour configurer la stratégie Interdiction de l'utilisation de l'Antide l'Anti-Spam, procédez comme suit :

1. Dans l'arborescence de la console de gestion, sélectionnez le dossier **Anti-Spam**
2. Dans la partie droite de la fenêtre de console de gestion, sélectionnez la stratégie **Interdiction de l'utilisation de l'Antide l'Anti-Spam**.
3. Dans le menu contextuel de la stratégie, sélectionnez l'option **Propriétés**.

   La fenêtre **Propriétés de Interdiction de l'utilisation de l'Antide l'Anti-Spam** s'affiche (cf. ill. ci-après).

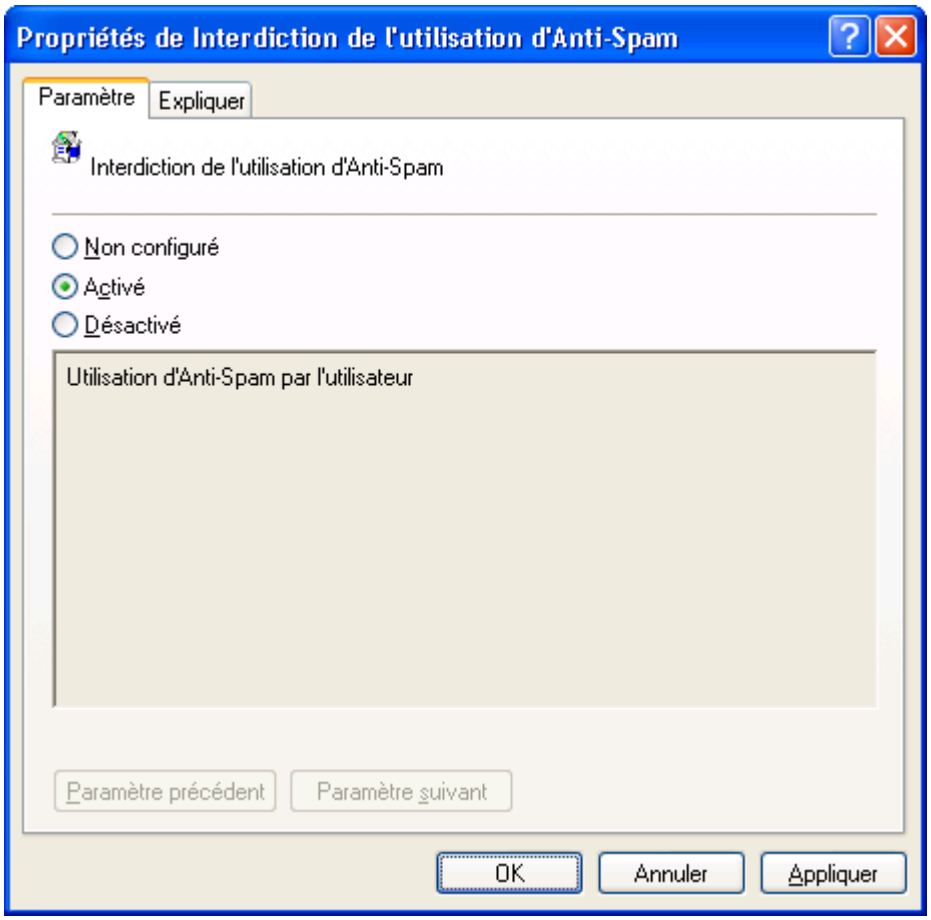


*Figure 52 : fenêtre **Propriétés : Interdiction de l'utilisation de l'Antide l'Anti-Spam***

4. Pour interdire la modification des paramètres de l'Antide l'Anti-Spam et la consultation du journal de ce composant par l'utilisateur, sélectionnez sous l'onglet **Paramètre** l'option **Activé**.

   Pour autoriser l'utilisateur à activer le composant Anti-Spam, sélectionnez sous l'onglet **Paramètre** l'option **Désactivé** ou **Non configuré**.

CONFIGURATION DE LA STRATEGIE INTERDICTION DE L'UTILISATION DE CONTACTS PERSONNELS

Pour configurer la stratégie Interdiction de l'utilisation de Contacts personnels, procédez comme suit :

1. Dans l'arborescence de la console de gestion, sélectionnez le dossier **Contacts personnels**.
2. Dans la partie droite de la fenêtre de console de gestion, sélectionnez la stratégie **Interdiction de l'utilisation de Contacts personnels**.
3. Dans le menu contextuel de la stratégie, sélectionnez l'option **Propriétés**.

   La fenêtre **Propriétés de Interdiction de l'utilisation de Contacts personnels** s'affiche (cf. ill. ci-après).

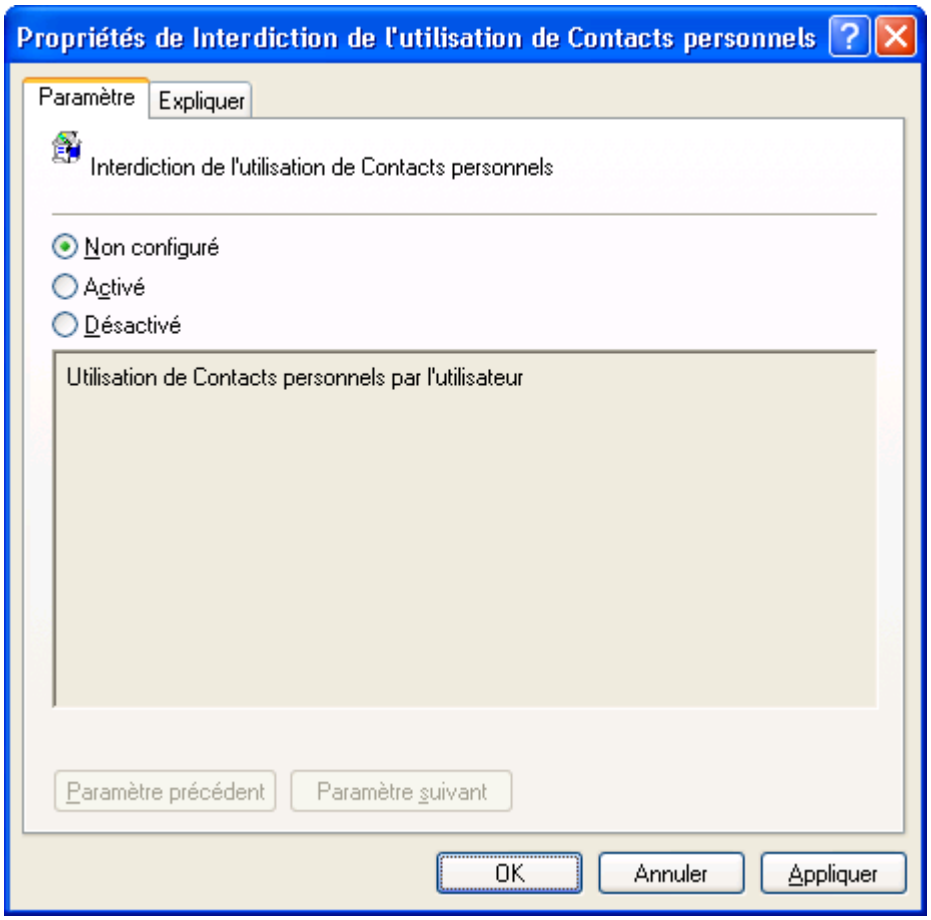


*Figure 53 : fenêtre **Propriétés : Interdiction de l'utilisation de Contacts personnels***

4. Pour interdire la modification des paramètres de Contacts personnels et la consultation du journal de ce composant par l'utilisateur, sélectionnez sous l'onglet **Paramètre** l'option **Activé**.

   Pour autoriser l'utilisateur à activer le composant Contacts personnels, sélectionnez sous l'onglet **Paramètre** l'option **Désactivé** ou **Non configuré**.

CONFIGURATION DE LA STRATEGIE INTERDICTION DE L'ACCES AUX DONNEES CHIFFREES

Pour configurer la stratégie Chiffrement automatique des données, procédez comme suit :

1. Dans l'arborescence de la console d'administration, sélectionnez le dossier **Chiffrement**.
2. Dans la partie droite de la fenêtre de console de gestion, sélectionnez la stratégie **Interdiction de l'accès aux données chiffrées**.
3. Dans le menu contextuel de la stratégie, sélectionnez l'option **Propriétés**.

   La fenêtre **Propriétés de Chiffrement automatique des données** s'affiche.

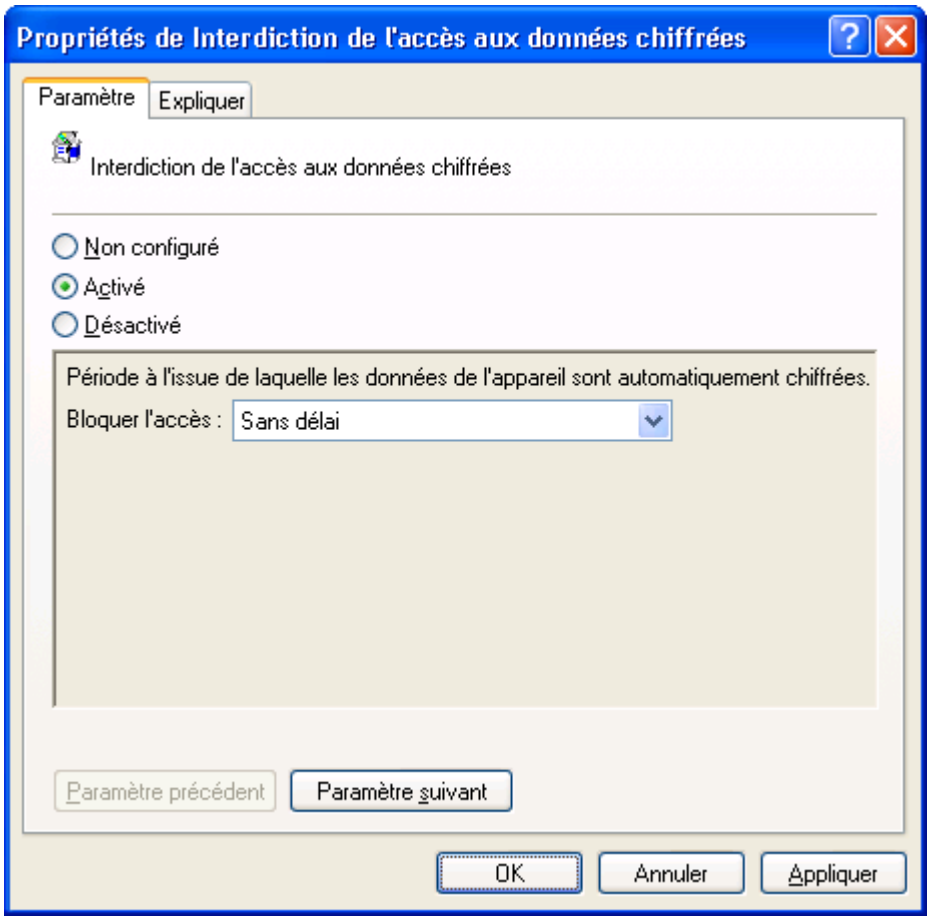


*Figure 54: Fenêtre **Propriétés : Chiffrement automatique des données***

4. Sous l'onglet **Paramètre**, sélectionnez une des options suivantes :
   - **Non configuré**. L'utilisateur peut modifier les paramètres de l'application sur l'appareil mobile. Dans ce cas, l'application utilise les paramètres définis par l'utilisateur.
   - **Activé**. La stratégie est activée. L'utilisateur ne peut pas modifier les paramètres de l'application sur l'appareil mobile. Dans ce cas, un verrou est affiché dans le coin supérieur gauche de l'écran de l'appareil.

     L'application utilise les paramètres définis par la stratégie. En sélectionnant cette option, vous pouvez toujours configurer les paramètres de la stratégie.
5. Sélectionnez dans la liste déroulante **Bloquer l'accès** la période à l'issue de laquelle l'interdiction de l'accès aux données chiffrées sera activée automatiquement. La fonction est activée quand l'appareil nomade est en mode d'économie d'énergie.

CONFIGURATION DE LA STRATEGIE LISTE DES DOSSIERS POUR LE CHIFFREMENT

Pour configurer la stratégie Liste des dossiers pour le chiffrement, procédez comme suit :

1. Dans l'arborescence de la console de gestion, sélectionnez le dossier **Chiffrement**.
2. Dans la partie droite de la fenêtre de console de gestion, sélectionnez la stratégie **Liste des dossiers pour le chiffrement**.
3. Dans le menu contextuel de la stratégie, sélectionnez l'option **Propriétés**.

   La fenêtre **Propriétés de Liste des dossiers pour le chiffrement** s'affiche (cf. ill. ci-après).

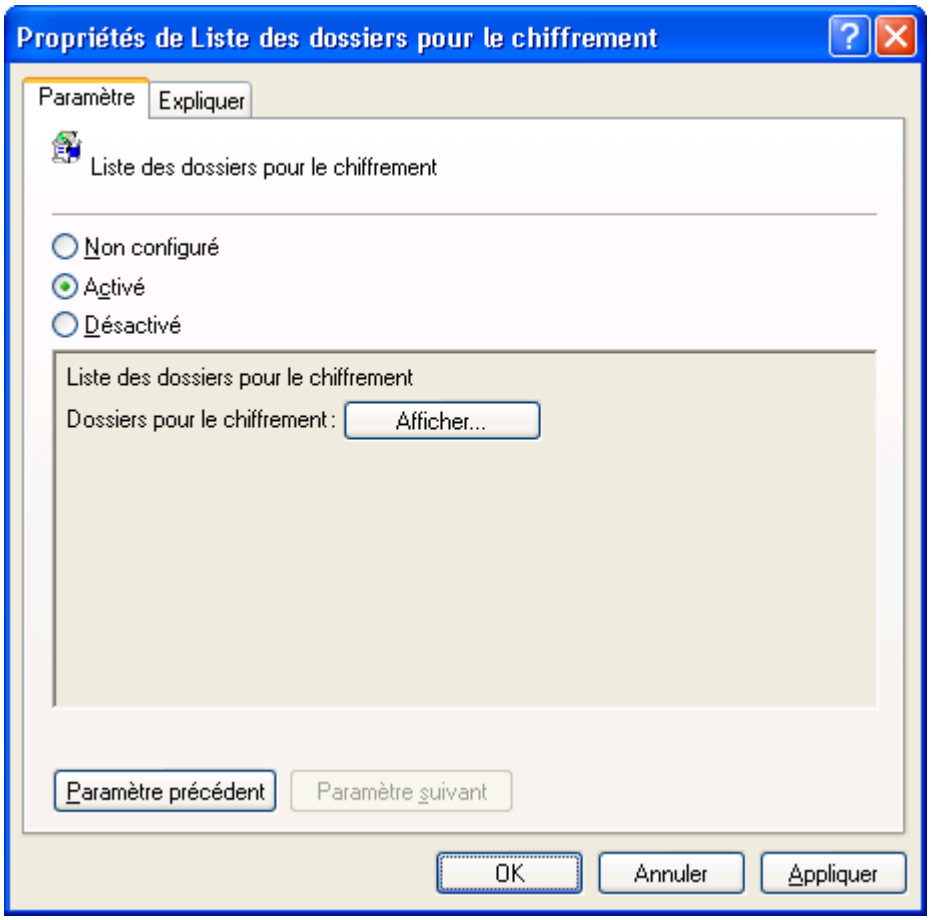


*Figure 55: Fenêtre **Propriétés de Liste des dossiers pour le chiffrement***

4. Sous l'onglet **Paramètre**, sélectionnez une des options suivantes :
   - **Non configuré**. L'utilisateur définit la liste des dossiers pour le chiffrement sur l'appareil mobile.
   - **Activé**. La Liste des dossiers pour le chiffrement est créée soit par l'utilisateur sur l'appareil mobile, soit par l'administrateur. La liste des dossiers pour le chiffrement ajoutée par l'administrateur ne peut pas être modifiée ou supprimée par l'utilisateur.
5. Cliquez sur **Afficher**, puis créez dans la fenêtre qui s'ouvre la liste des dossiers pour le chiffrement en cliquant sur **Ajouter** ou **Supprimer**.

CONFIGURATION DE LA STRATEGIE MODE DU PARE-FEU

Pour configurer la stratégie Mode du Pare-feu, procédez comme suit :

1. Dans l'arborescence de la console de gestion, sélectionnez le dossier **Pare-feu**.
2. Dans la partie droite de la fenêtre de console de gestion, sélectionnez la stratégie **Mode du Pare-feu**.
3. Dans le menu contextuel de la stratégie, sélectionnez l'option **Propriétés**.

   La fenêtre **Propriétés de Mode du Pare-feu** s'affiche (cf. ill. ci-après).

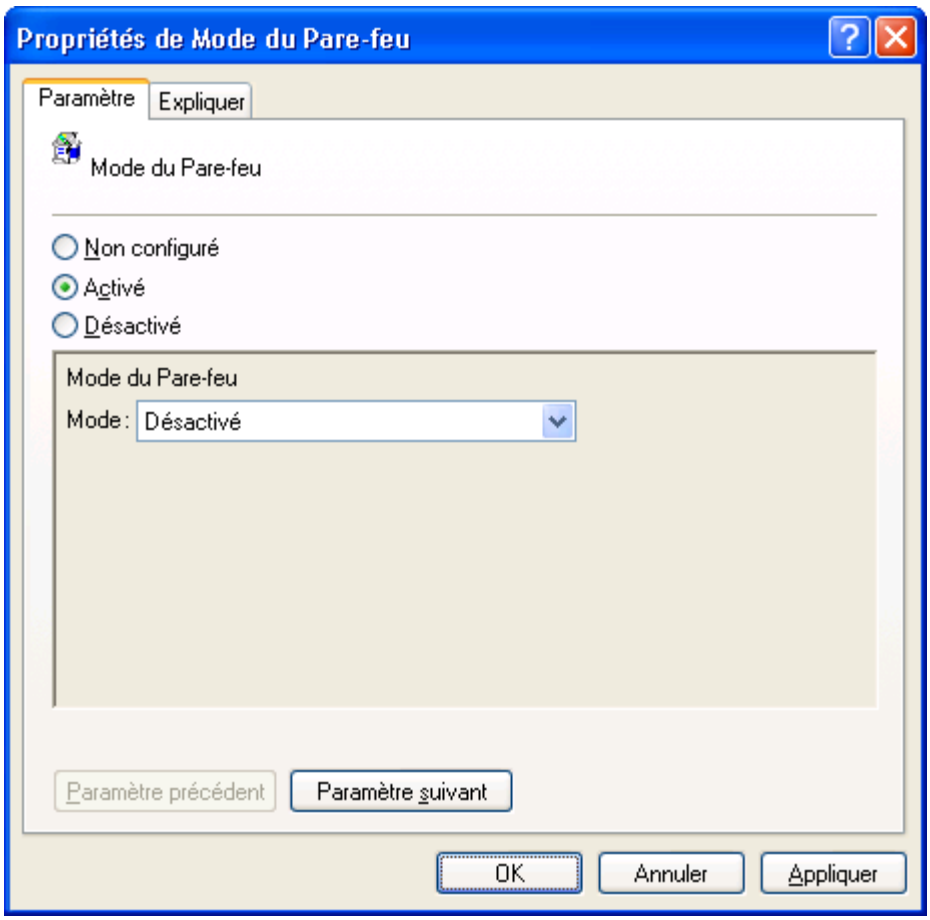


*Figure 56: Fenêtre **Propriétés de Mode du Pare-feu***

4. Sous l'onglet **Paramètre**, sélectionnez une des options suivantes :

   - **Non configuré**. Le Composant / la fonction sont activés sur l'appareil mobile de l'utilisateur. Les paramètres définis par la stratégie peuvent être modifiés par l'utilisateur sur l'appareil mobile.

     Dans ce cas, le composant / la fonction utilisent les paramètres définis par l'utilisateur.

   - **Activé**. Le Composant / la fonction sont activés sur l'appareil mobile de l'utilisateur. Paramètres définis par la stratégie ne peuvent pas être modifiés par l'utilisateur sur l'appareil mobile. Dans ce cas, un verrou est affiché dans le coin supérieur gauche de l'écran de l'appareil.

     Le composant / la fonction utilisent les paramètres définis par la stratégie. En sélectionnant cette option, vous pouvez toujours configurer les paramètres de la stratégie.

5. Sélectionnez dans la liste déroulante **Mode** le niveau de protection du Pare-feu. Valeurs possibles :
   - **Désactivé**. Le Pare-feu est désactivé. Toute activité de réseau est autorisée.
   - **Protection minimum**. Le Pare-feu interdit toutes les connexions entrantes. Toutes les connexions entrantes sont autorisées.
   - **Protection maximum**. Le Pare-feu interdit toutes les connexions entrantes. Les connexions sortantes sont autorisées via les protocoles SSH / HTTP / HTTPS / IMAP/ SMTP / POP3.
   - **Tout bloquer**. Le Pare-feu bloque la moindre activité de réseau sauf la mise à jour des bases de l'application et le fonctionnement de Mobile Device Manager.

CONFIGURATION DE LA STRATEGIE NOTIFICATION DU PARE-FEU

Pour configurer la stratégie Notification du Pare-feu, procédez comme suit :

1. Dans l'arborescence de la console de gestion, sélectionnez le dossier **Pare-feu**.
2. Dans la partie droite de la fenêtre de console de gestion, sélectionnez la stratégie **Notification du Pare-feu**.
3. Dans le menu contextuel de la stratégie, sélectionnez l'option **Propriétés**.

   La fenêtre **Propriétés de Notification du Pare-feu** s'affiche (cf. ill. ci-après).

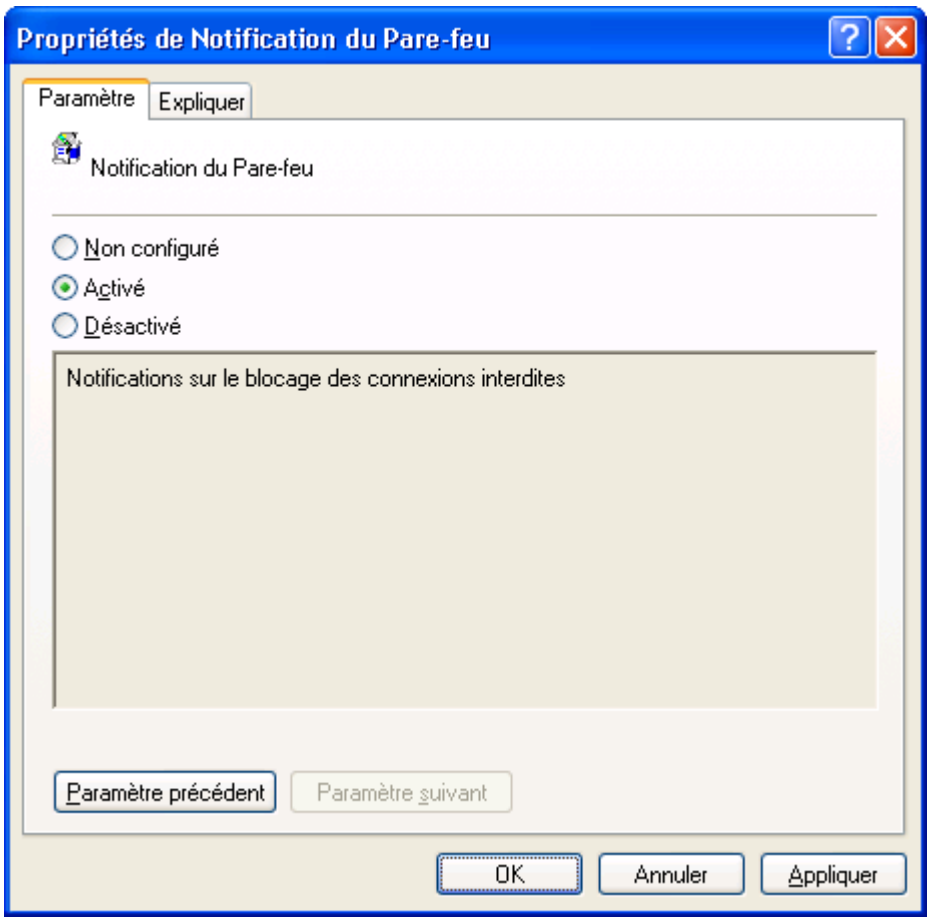


*Figure 57: Fenêtre **Propriétés de Notification du Pare-feu***

4. Pour notifier l'utilisateur sur les tentatives de connexions interdites pour le niveau de protection défini, sélectionnez sous l'onglet **Paramètre** l'option **Activé**.

   Pour interdire les notifications du Pare-feu sur les tentatives de connexions interdites sur l'appareil mobile, sélectionnez sous l'onglet **Paramètre** l'option **Désactivé**.

   Pour laisser l'utilisateur activer ou désactiver les notifications du Pare-feu, sélectionnez sous l'onglet **Paramètre** l'option **Non configuré**.

CONFIGURATION DE LA STRATEGIE LICENCE

Pour configurer la stratégie Licence, procédez comme suit :

1. Enregistrez sur le serveur MDM le fichier de licence qui vous a été envoyé par courrier électronique.
2. Ouvrez le dossier avec la distribution de l'application et exécutez l'utilitaire kes2mdm.exe.

   Dans la ligne de commande de la console du serveur, saisissez la commande rédigée selon le modèle suivant :

   `kes2mdm.exe <chemin complet au fichier de licence>\<nom du fichier de licence>`

   L'utilitaire ajoutera dans le dossier avec la distribution de l'application le fichier kes8key.txt qui contient la ligne de texte.

   Si le fichier kes8key.txt n'a pas été ajouté au dossier avec la distribution de l'application, copiez depuis la ligne de commande de la console du serveur les détails de l'erreur et envoyez-les à l'adresse du Service d'assistance technique de Kaspersky Lab.
3. Ouvrez le fichier kes8key.txt et copiez la ligne de texte dans le presse-papiers.
4. Ouvrez la console de gestion.
5. Sélectionnez dans l'arborescence de la console de gestion l'objet de stratégie de groupe pour installer la licence appropriée de Kaspersky Endpoint Security 8.0 for Smartphone.
6. Sélectionnez dans le nœud **Configuration de l'ordinateur** le dossier **Modèles d'administration**, ensuite le dossier **Paramètres de Kaspersky Endpoint Security 8 for Smartphone**.
7. Sélectionnez le dossier **Licence**.
8. Ouvrez la fenêtre **Propriétés de Licence** (cf. ill. ci-après).

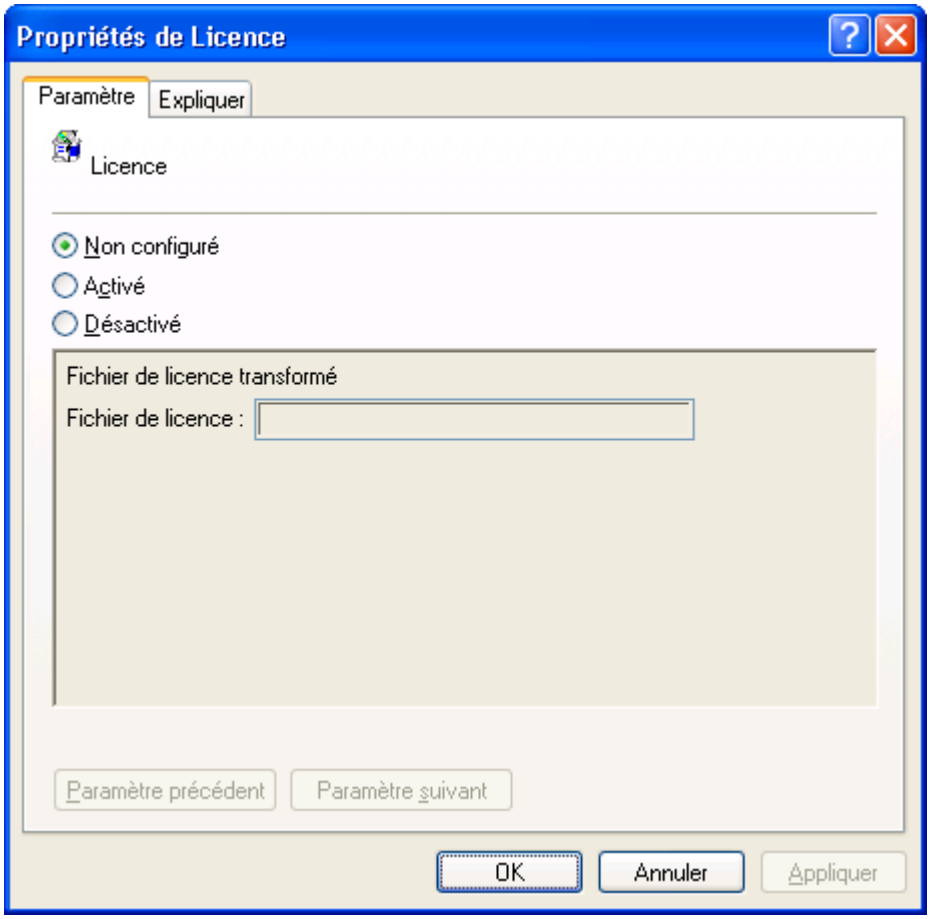


*Figure 58 : fenêtre **Propriétés : licence***

9. Sélectionnez sous l'onglet **Paramètre** l'option **Activé** pour configurer la stratégie.
10. Collez la ligne de texte depuis le presse-papiers dans le champ **Fichier de licence**.

    Pendant la synchronisation suivante des stratégies, la licence de Kaspersky Endpoint Security 8 for Smartphone sera installée sur les appareils mobiles d'utilisateurs.

ACTIVATION DU LOGICIEL

Pour installer la licence de l'application Kaspersky Endpoint Security 8 for Smartphone sur les appareils mobiles, l'administrateur doit configurer la stratégie Licence dans le modèle d'administration pour la gestion de l'application. Après la transmission de la stratégie sur les appareils d'utilisateurs, la licence sera installée et l'application sera activée.

Une fois installée sur l'appareil mobile, l'application Kaspersky Endpoint Security 8 for Smartphone reste opérationnelle pendant trois jours sans être activée. Si l'installation de la licence n'est pas effectuée dans les trois jours, les fonctionnalités de l'application seront limitées automatiquement.

Si vous n'avez pas acheté la licence avant d'installer l'application, vous pouvez l'ajouter à la stratégie à tout moment.

Par défaut, la licence n'est pas ajoutée à la stratégie.

INSTALLATION ET SUPPRESSION DE L'APPLICATION POUR LES APPAREILS MOBILES

Mobile Device Manager permet d'installer et de supprimer à distance Kaspersky Endpoint Security 8 for Smartphone sur les appareils mobiles d'utilisateurs.

Pour ce faire, dans la console System Center Mobile Device Manager Software Distribution il faut créer le paquet d'installation pour installer l'application (cf. la rubrique "Création d'un paquet d'installation" à la page 104) et le diffuser au groupe d'appareils mobiles enregistrés dans le domaine.

Avant de créer et de diffuser le paquet d'installation, il est conseillé de configurer les stratégies de gestion de l'application (cf. la rubrique "Configuration du modèle d'administration" à la page 81), parce que la période de synchronisation des appareils mobiles avec le serveur MDM est différente de celle de mise en place des stratégies. Cette action permet en même temps d'installer l'application et de mettre en place les stratégies sur les appareils mobiles d'utilisateurs.

Pendant la synchronisation suivante des appareils mobiles avec le serveur MDM, l'application sera installée automatiquement sur les appareils en question. Dans ce cas, l'état de l'installation de l'application ne sera pas affiché et l'installation sera effectuée sans aucune intervention de l'utilisateur.

Une fois l'application installée sur les appareils mobiles, vous pourrez modifier ses paramètres de fonctionnement à l'aide des stratégies. Après la mise en place des stratégies pendant la synchronisation des appareils mobiles avec le serveur MDM, l'application utilisera les paramètres modifiés.

Pour supprimer à distance l'application des appareils mobiles d'utilisateurs, il faut cochez la case de suppression pour le paquet d'installation dans la console System Center Mobile Device Manager Software Distribution. Pendant la synchronisation suivante des appareils mobiles avec le serveur MDM, l'application sera automatiquement supprimée des appareils mobiles.

Pendant la création d'un paquet d'installation, vous pouvez autoriser les utilisateurs à supprimer l'application des appareils mobiles avec la procédure standard "Suppression des programmes".

DANS CETTE SECTION

CREATION DU PAQUET D'INSTALLATION

Pour diffuser Kaspersky Endpoint Security 8 for Smartphone sur les appareils mobiles des utilisateurs enregistrés dans le domaine, il faut créer un paquet d'installation de l'application. Le paquet d'installation comprendra le fichier d'installation qui sera exécuté automatiquement après l'enregistrement du fichier sur les appareils mobiles.

Avant de créer le paquet d'installation, assurez-vous que le certificat qui sert de signature pour le fichier d'installation de Kaspersky Endpoint Security 8 for Smartphone et le certificat du centre de certification sont installés sur le serveur MDM. Le certificat de l'application est ajouté à la liste des Éditeurs approuvés (Trusted Publishers) et le certificat du centre de certification est ajouté à la liste des Autorités de certification racines de confiance (Trusted Root Certification Authorities).

Pour créer le paquet d'installation de Kaspersky Endpoint Security 8 for Smartphone pour les appareils mobiles d'utilisateurs, procédez comme suit :

1. Ouvrez la console System Center Mobile Device Manager Software Distribution.
2. Ouvrez l'assistant de création du paquet d'installation en cliquant sur le lien **Create** (cf. ill. ci-après).

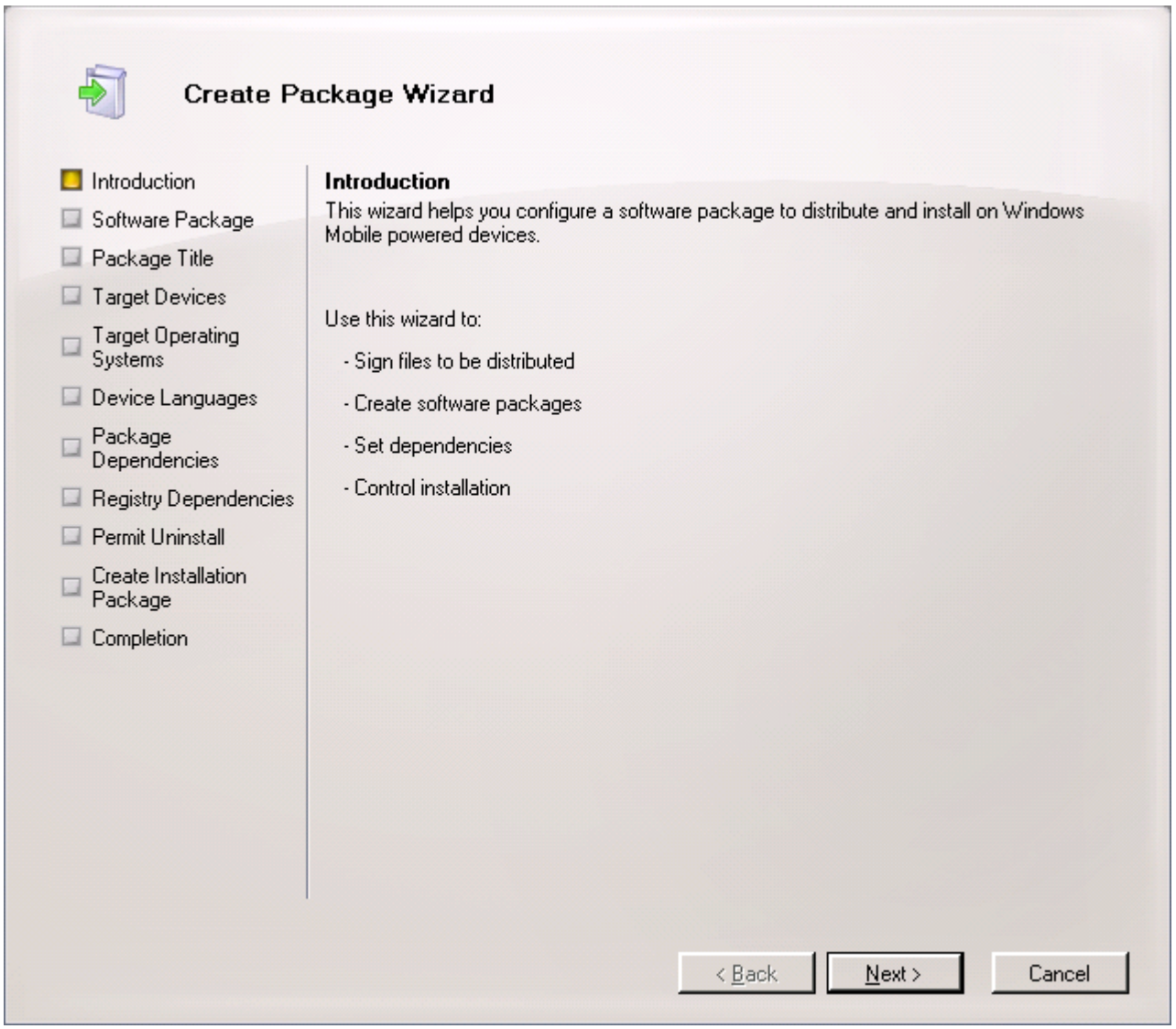


*Figure 59 : fenêtre **Create Package Wizard***

3. Sous l'onglet **Software Package** dans le champ **Cabinet file**, cliquez sur **Browse** pour ouvrir le dossier avec la distribution de l'application et sélectionnez le fichier d'installation endpoint_MDM_Afaria_8_0_x_xx_fr.cab, enregistré sur le serveur MDM (cf. ill. ci-après).

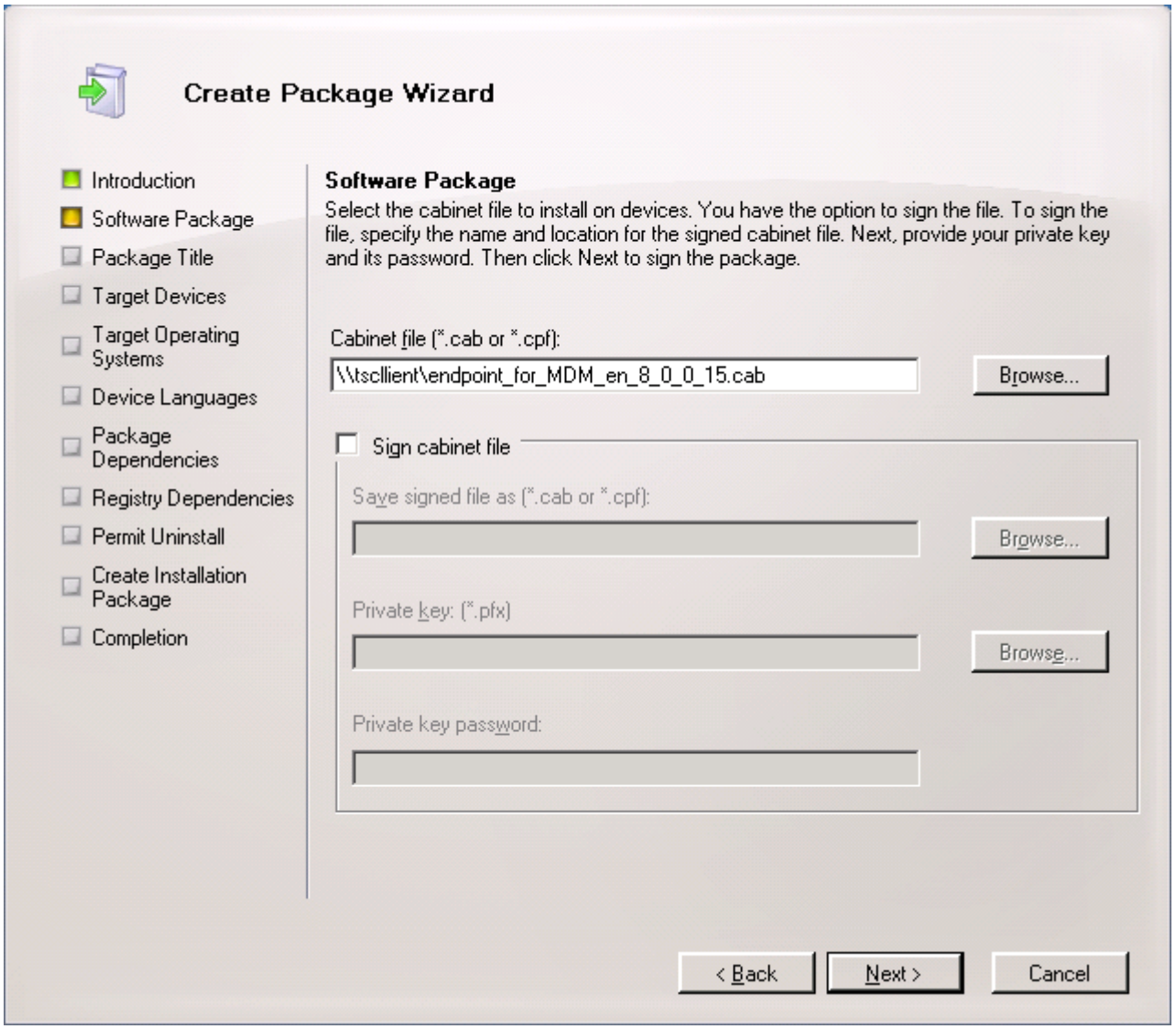


*Figure 60 : onglet **Software Package***

4. Spécifiez sous l'onglet **Package Title** dans le champ **Package title** le nom du paquet d'installation créé et mettez la description du paquet dans le champ **Package description** (cf. ill. ci-après).

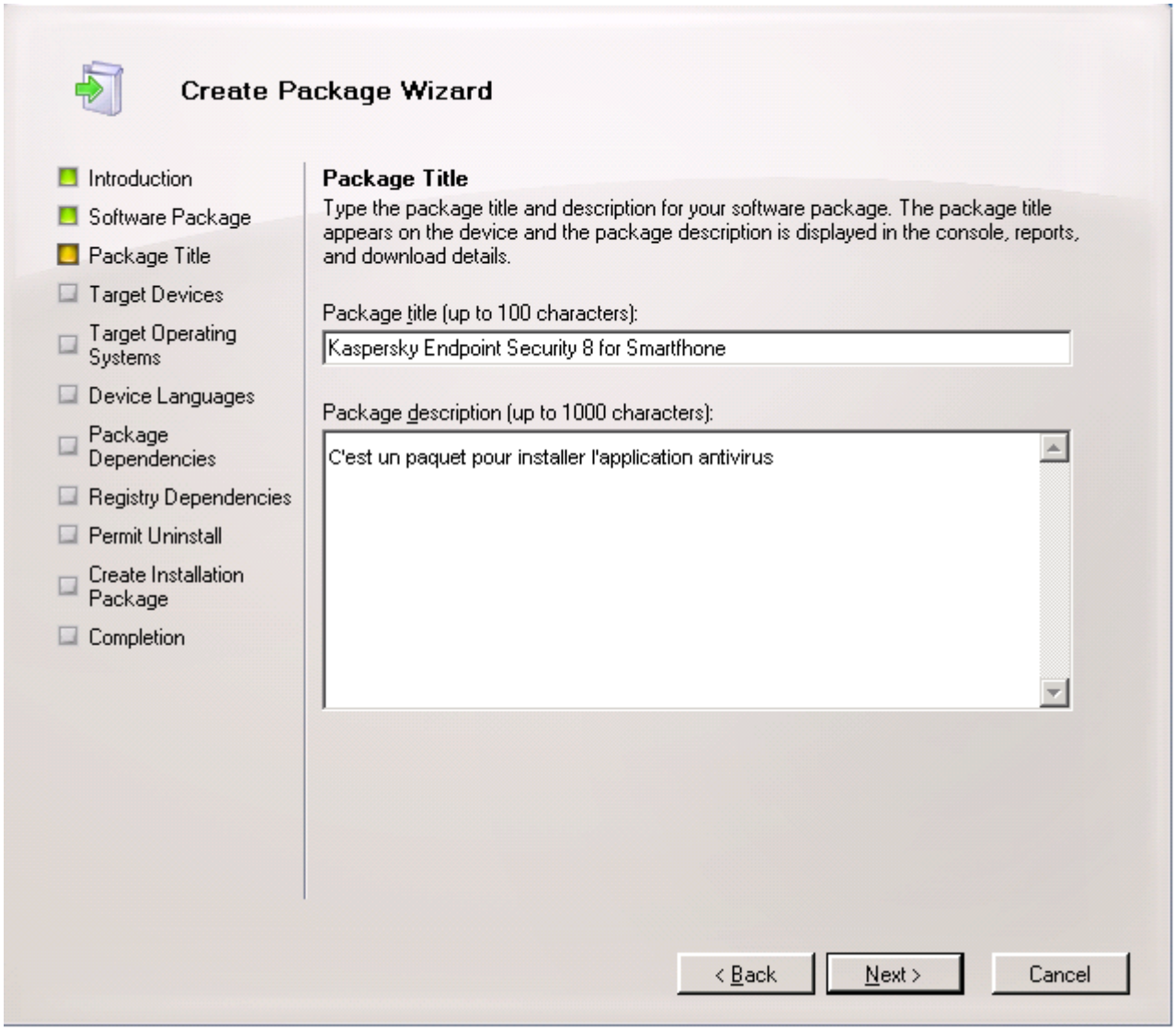


*Figure 61 : onglet **Package Title***

5. Sélectionnez sous l'onglet **Target Devices** (cf. ill. ci-après) le type de système d'exploitation des appareils mobiles destinés à recevoir Kaspersky Endpoint Security 8 for Smartphone.

   Pour installer l'application sur les appareils mobiles avec des systèmes d'exploitation différents, sélectionnez l'option **All**. Il est conseillé de sélectionner la valeur proposée.

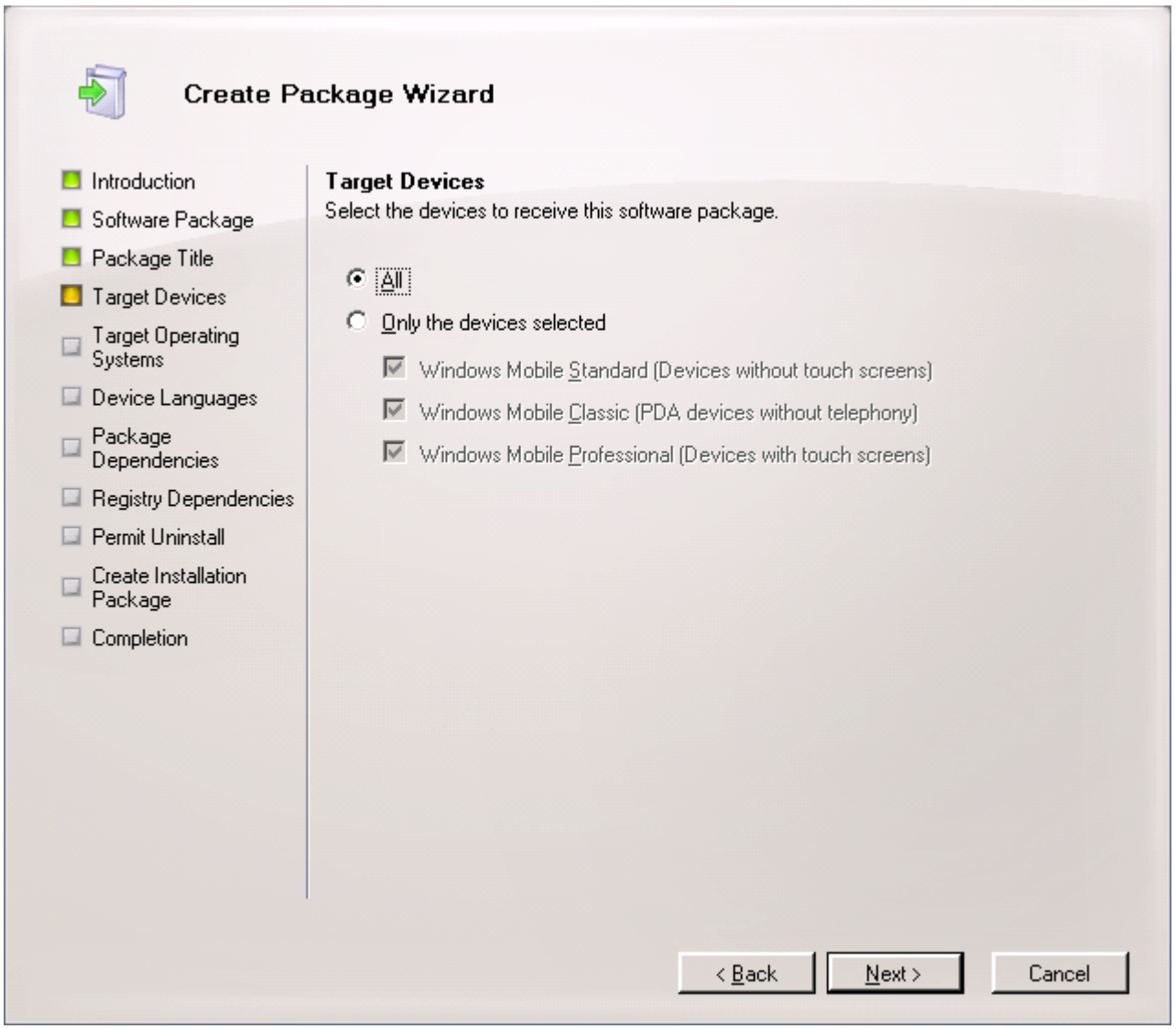


*Figure 62 : onglet **Target Devices***

6. Spécifiez sous l'onglet **Target Operating Systems** (cf. ill. ci-après) la sélection des versions du système d'exploitation des appareils mobiles destinés à recevoir Kaspersky Endpoint Security 8 for Smartphone.

   Pour installer l'application sur les appareils mobiles avec les versions différentes du système d'exploitation, sélectionnez l'option **All**. Il est conseillé de sélectionner la valeur proposée.

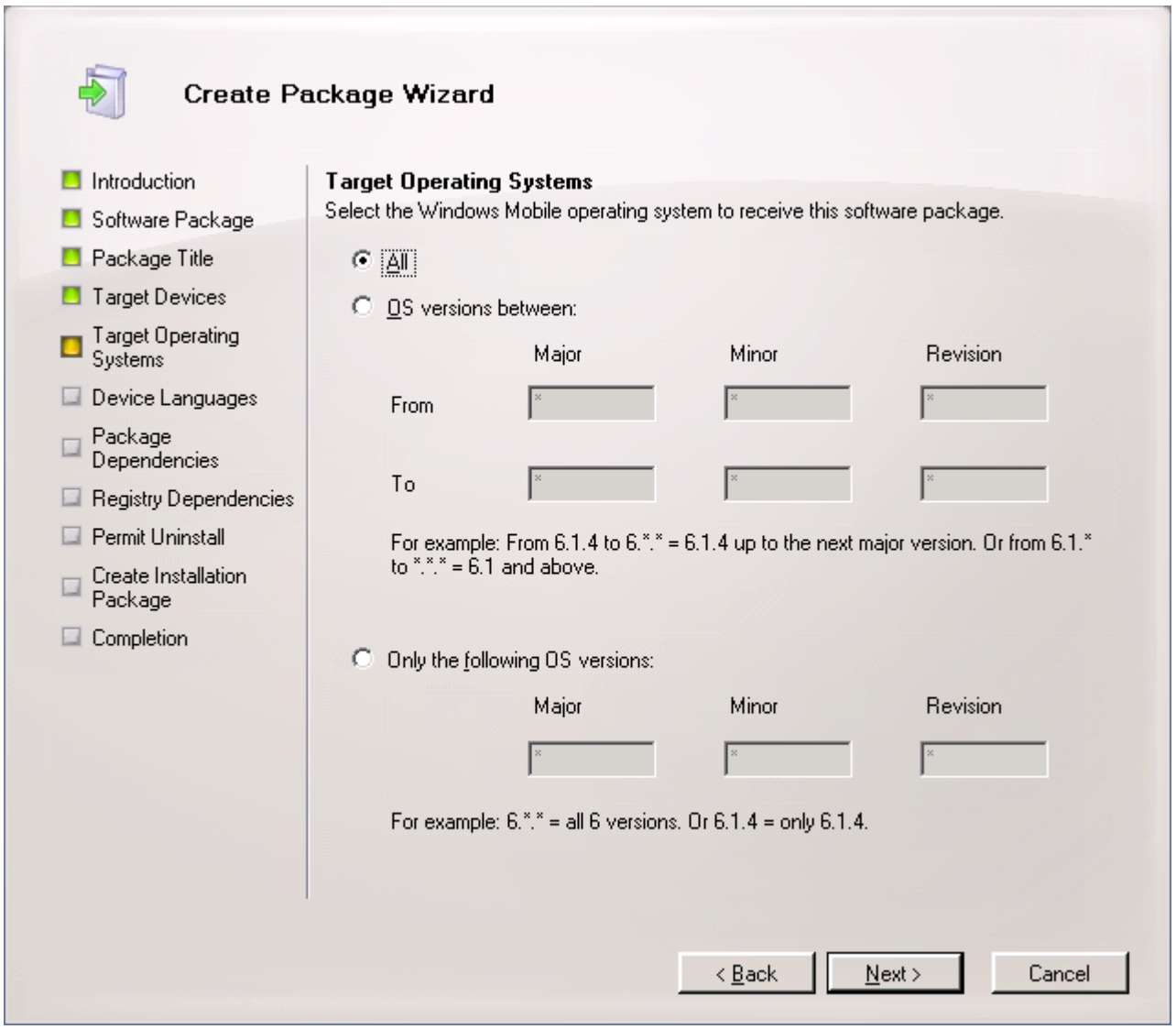


*Figure 63 : onglet **Target Operating Systems***

7. Sélectionnez sous l'onglet **Device Languages** (cf. ill. ci-après) la langue de l'interface des appareils mobiles destinés à recevoir Kaspersky Endpoint Security 8 for Smartphone.

   Pour installer l'application sur les appareils mobiles avec des langues de l'interface différentes, sélectionnez l'option **All**.

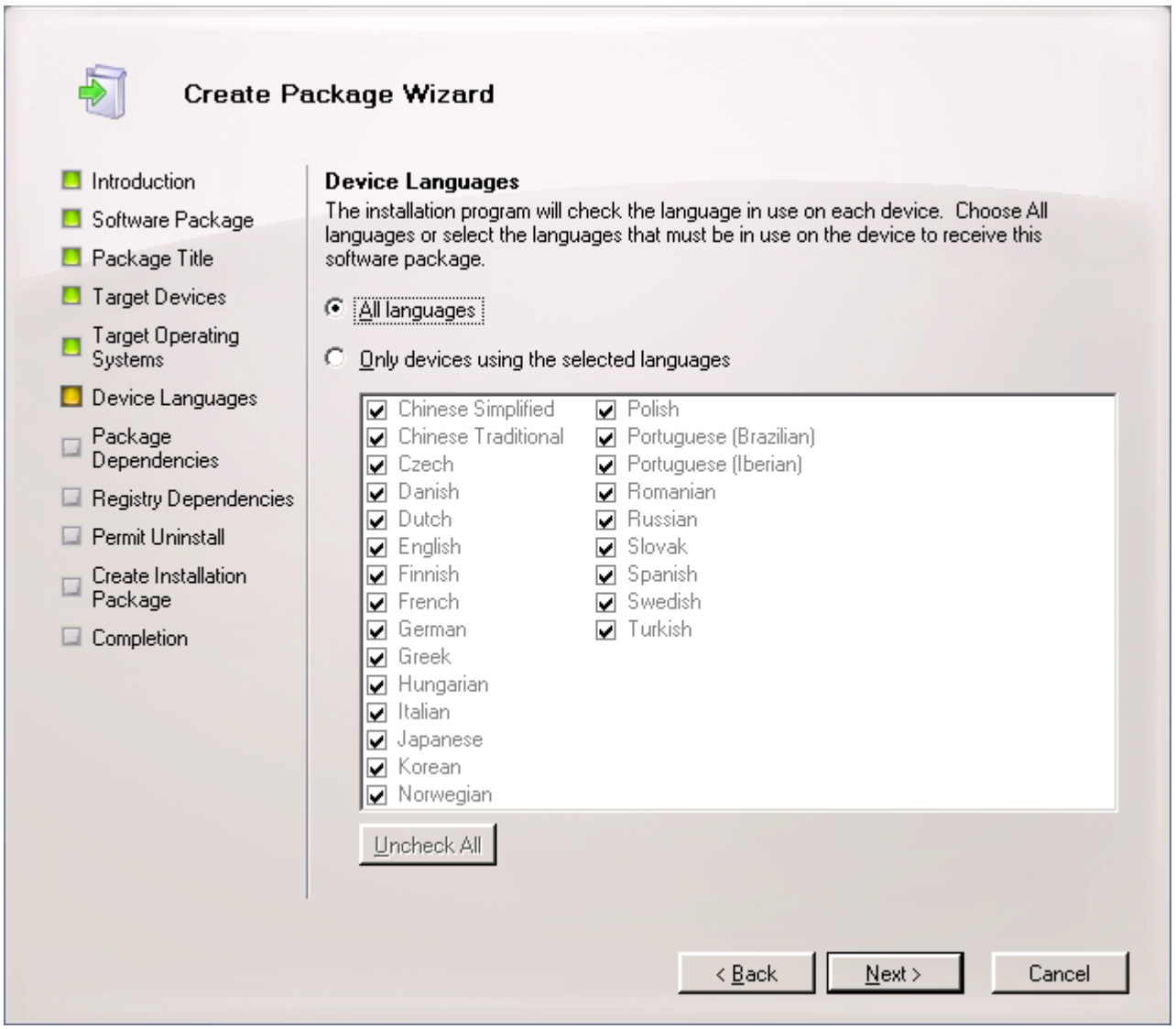


*Figure 64 : onglet **Device Languages***

8. Spécifiez sous l'onglet **Package Dependencies** (cf. ill. ci-après) les dépendances du paquet créé par rapport à d'autres paquets d'installation.

   En l'absence de dépendances, sélectionnez **No dependencies**. Il est conseillé de sélectionner la valeur proposée.

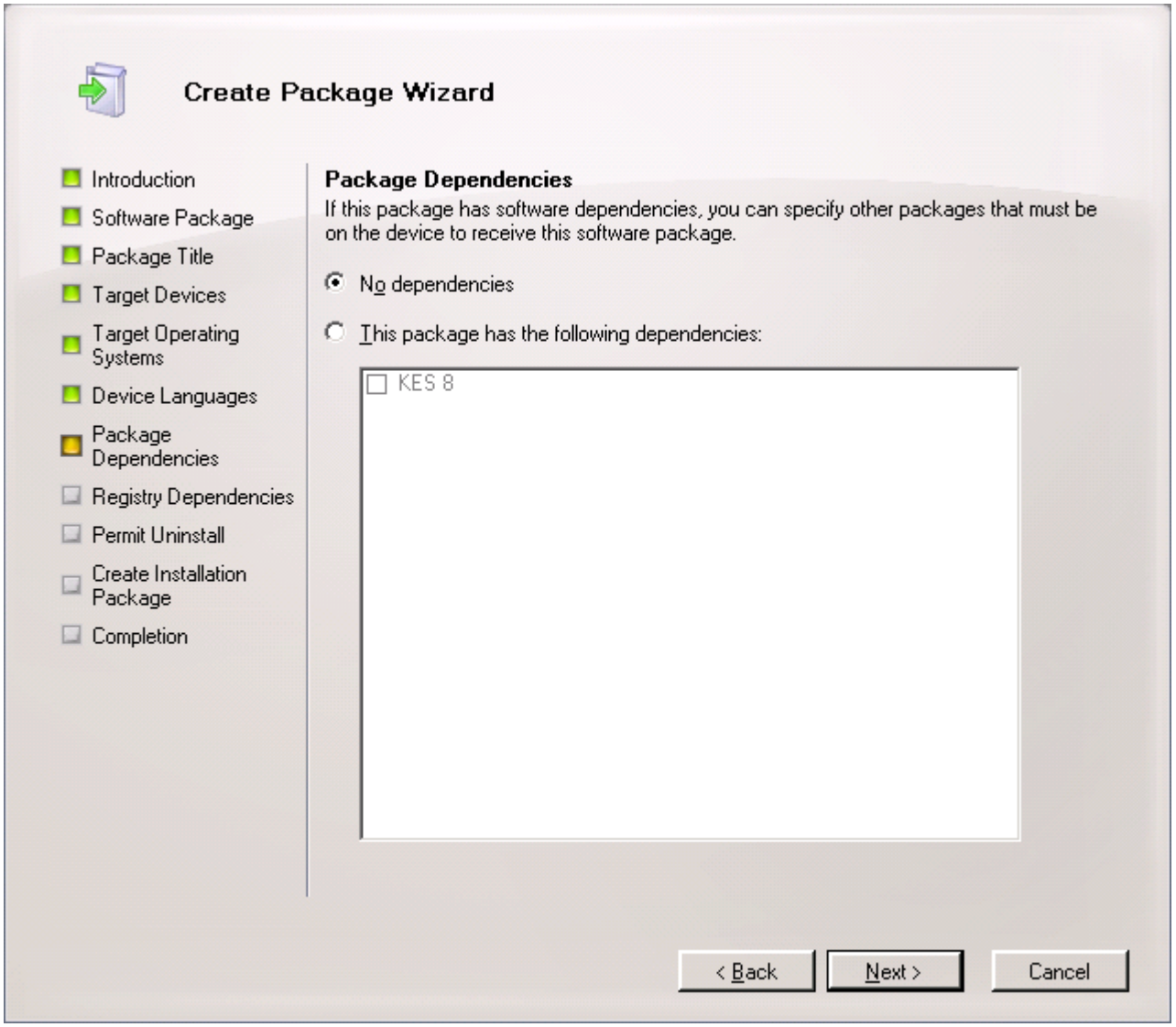


*Figure 65 : onglet **Package Dependencies***

9. Spécifiez sous l'onglet **Registry Dependencies** (cf. ill. ci-après) les dépendances du paquet créé par rapport à la présence des clés de registre requises.

   En l'absence de dépendances, sélectionnez **No registry dependencies**. Il est conseillé de sélectionner la valeur proposée.

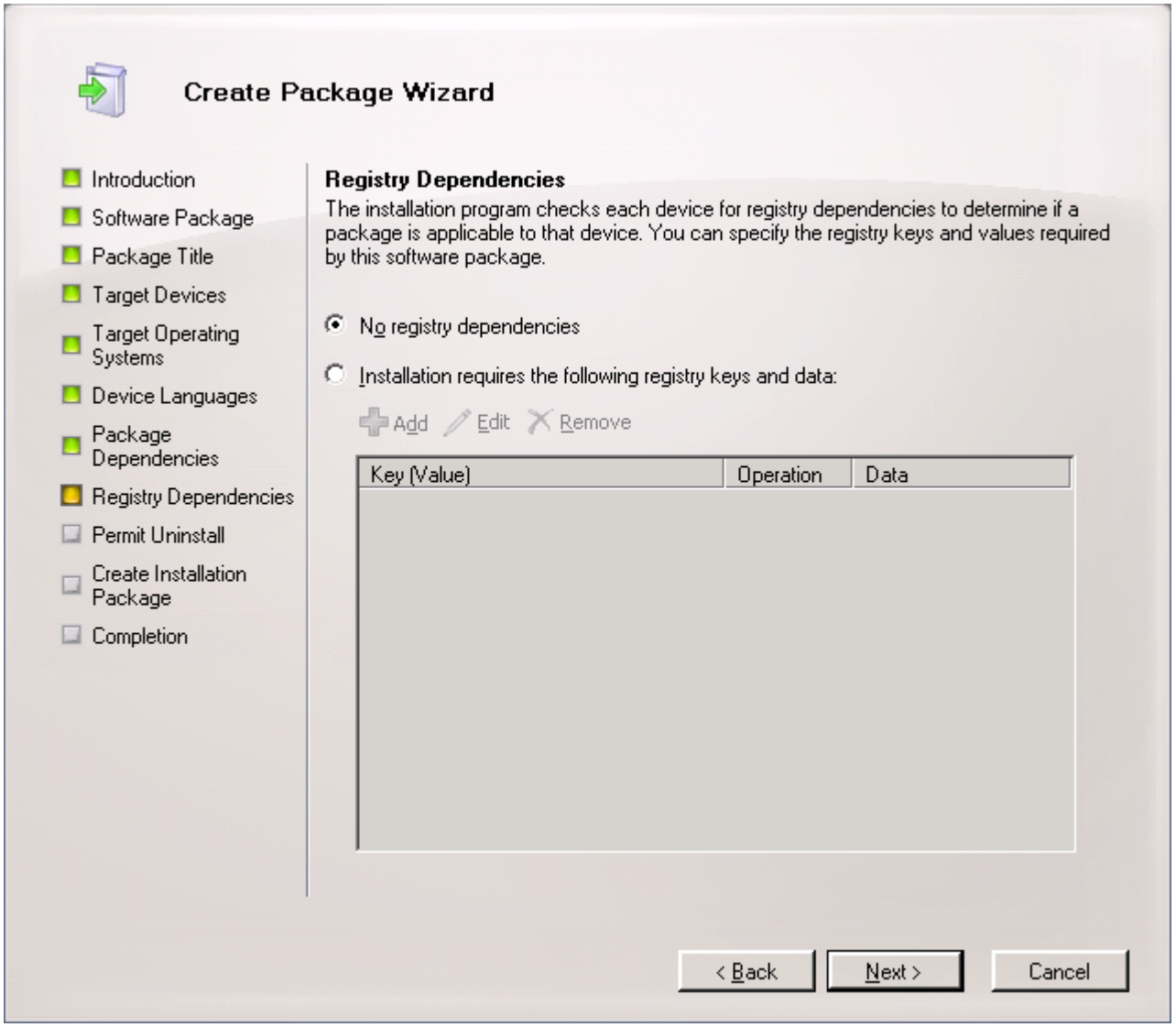


*Figure 66 : onglet **Registry Dependencies***

10. Pour laisser l'utilisateur supprimer l'application de l'appareil mobile, sélectionnez sous l'onglet **Permit Uninstall** l'option **Yes** (cf. ill. ci-après).

    Pour ne pas laisser l'utilisateur supprimer l'application de l'appareil mobile, sélectionnez sous l'onglet **Permit Uninstall** l'option **No**.

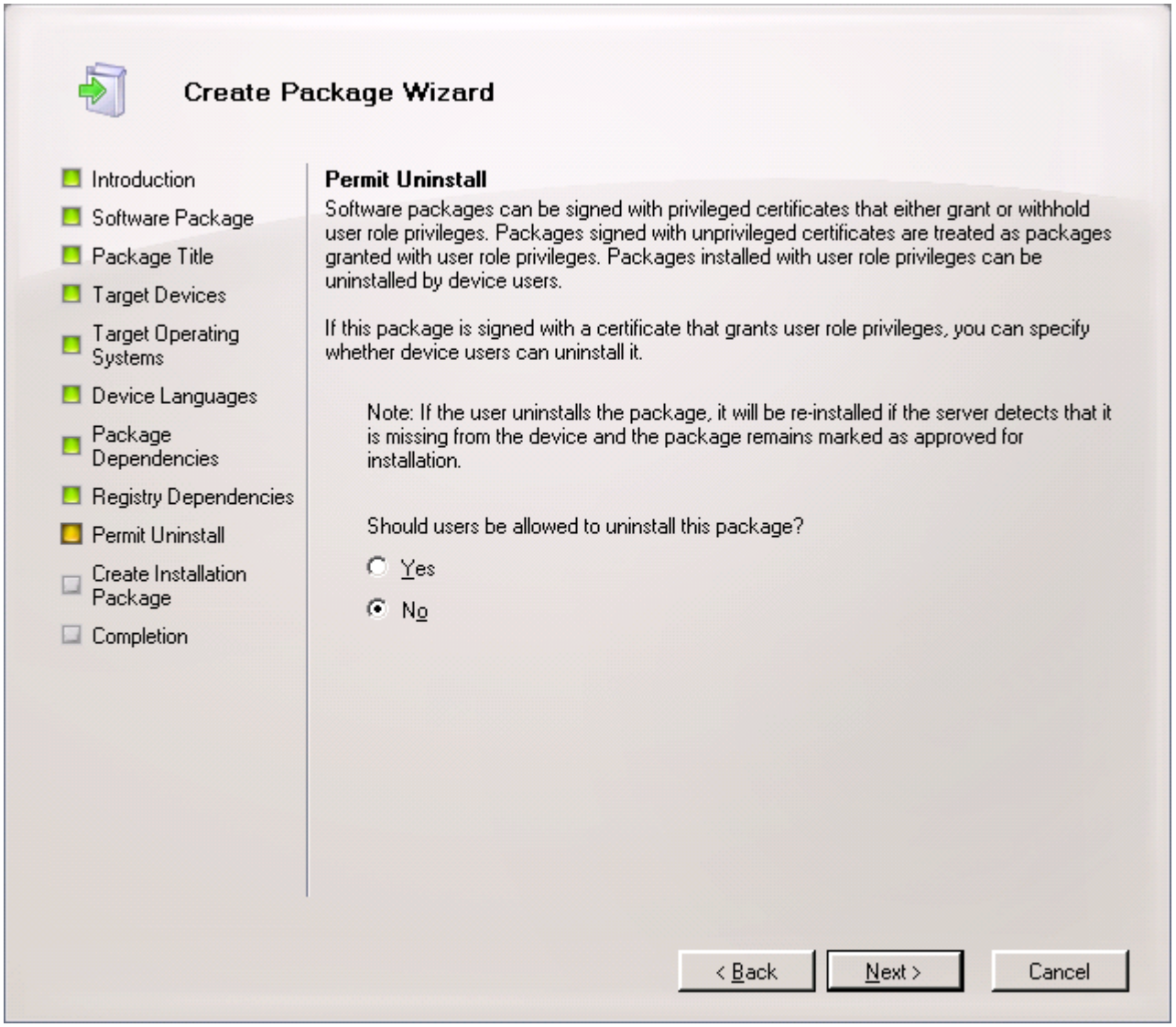


*Figure 67 : onglet **Permit Uninstall***

11. Cliquez sur **Next** pour continuer à utiliser l'assistant (cf. ill. ci-après).

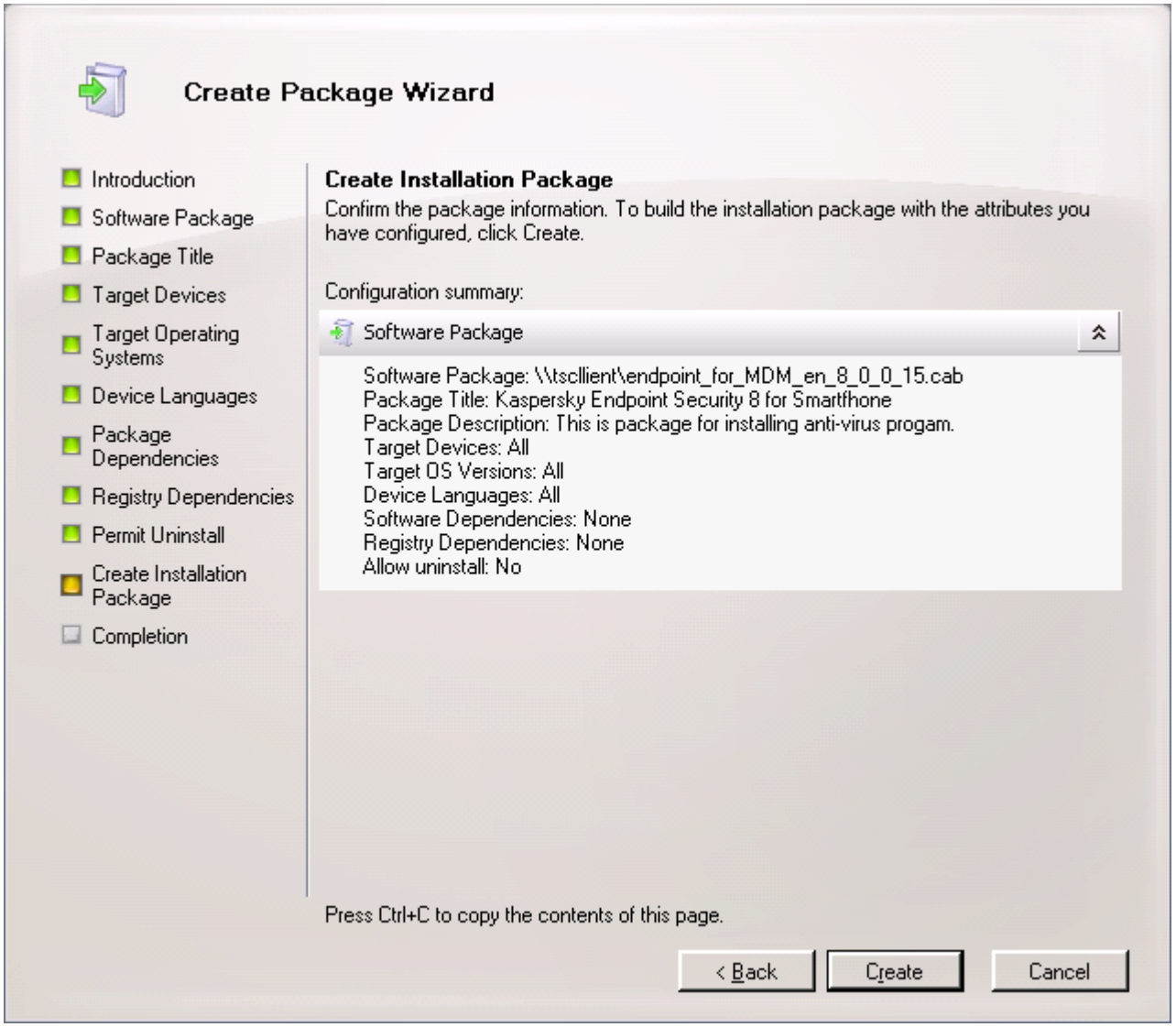


*Figure 68 : onglet **Create Installation Package***

12. Cliquez sur **Create**. L'assistant passera à l'onglet **Completion** qui affiche l'état de création du paquet d'installation (cf. ill. ci-après).

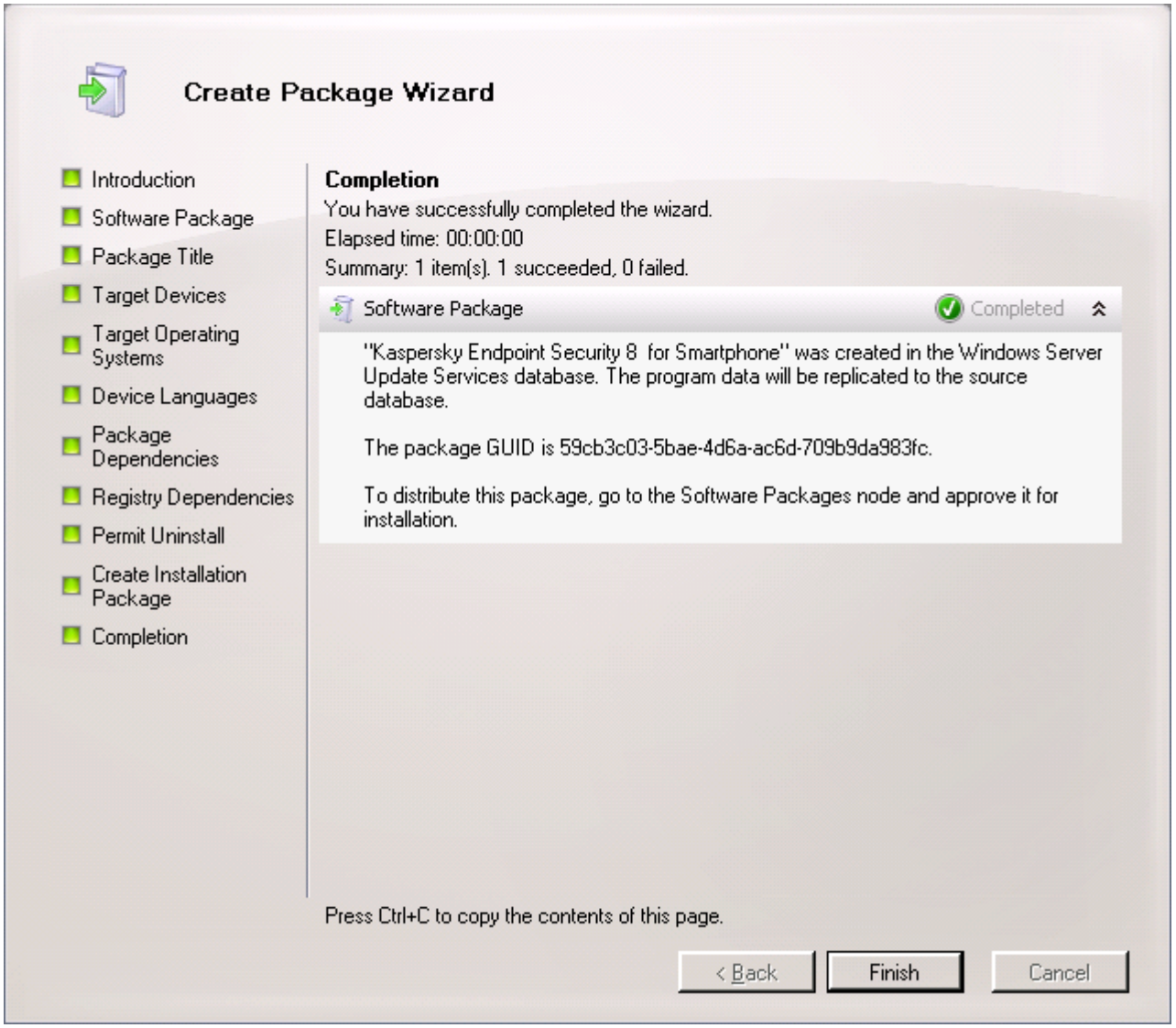


*Figure 69 : onglet **Completion***

Après la fermeture de l'assistant, le paquet créé sera ajouté au groupe Software Packages dans la zone de stockage des paquets d'installation et sera affiché dans la liste des paquets d'installation de console System Center Mobile Device Manager Software Distribution. Vous pourrez utiliser ce paquet pour installer l'application sur les appareils mobiles d'utilisateurs.

INSTALLATION DE L'APPLICATION SUR LES APPAREILS MOBILES

Vous pouvez installer à distance Kaspersky Endpoint Security 8 for Smartphone sur les appareils mobiles des utilisateurs enregistrés dans le domaine.

Pour installer Kaspersky Endpoint Security 8 for Smartphone sur les appareils mobiles d'utilisateurs, procédez comme suit :

1. Ouvrez la console System Center Mobile Device Manager Software Distribution.
2. Sélectionnez le paquet d'installation de l'application dans la zone de stockage des paquets d'installation.
3. Ouvrez le menu contextuel et sélectionnez l'option **Approve**.
4. Dans la fenêtre **Approve Packages** qui s'affiche, sélectionnez le groupe d'appareils mobiles destinés à recevoir l'application.
5. Ouvrez le menu contextuel et sélectionnez l'option **Approved for Install**.

   Kaspersky Endpoint Security 8 for Smartphone sera installé pendant la synchronisation suivante des appareils mobiles avec le serveur MDM.

SUPPRESSION DE L'APPLICATION DES APPAREILS MOBILES

Vous pouvez supprimer à distance Kaspersky Endpoint Security 8 for Smartphone des appareils mobiles des utilisateurs enregistrés dans le domaine.

Pour supprimer Kaspersky Endpoint Security 8 for Smartphone des appareils mobiles d'utilisateurs, procédez comme suit :

1. Ouvrez la console System Center Mobile Device Manager Software Distribution.
2. Sélectionnez le paquet d'installation de l'application dans la zone de stockage des paquets d'installation.
3. Ouvrez le menu contextuel et sélectionnez l'option **Approve**.
4. Dans la fenêtre **Approve Packages** qui s'affiche, sélectionnez le groupe d'appareils mobiles pour la suppression de l'application.
5. Ouvrez le menu contextuel et sélectionnez l'option **Approved for Removal**.

   Kaspersky Endpoint Security 8 for Smartphone sera supprimé pendant la synchronisation suivante des appareils mobiles avec le serveur MDM.

DEPLOIEMENT DE L'APPLICATION VIA SYBASE AFARIA

Cette section décrit la procédure de déploiement de Kaspersky Endpoint Security 8 for Smartphone via Sybase Afaria.

DANS CETTE SECTION

CONCEPTION DE LA GESTION DE L'APPLICATION VIA SYBASE AFARIA

Tous les paramètres de fonctionnement de l'application y compris la licence sont définis via la stratégie de Kaspersky Endpoint Security 8 for Smartphone. La stratégie permet de définir les mêmes valeurs des paramètres de fonctionnement de l'application pour les groupes cibles de l'appareil.

La création et la modification des stratégies pour Kaspersky Endpoint Security 8 for Smartphone sont effectuées à l'aide de l'utilitaire de gestion de la stratégie KES2Afaria.exe qui fait partie de la distribution de l'application. L'utilitaire permet à l'administrateur de configurer les paramètres de l'application et de les enregistrer dans le fichier de stratégie avec l'extension kes (cf. la rubrique "Création de la stratégie. Configuration des paramètres de Kaspersky Endpoint Security 8 for Smartphone" à la page 118).

L'utilitaire peut être installé sur le poste de travail de l'administrateur ou sur le serveur de Sybase Afaria (cf. la rubrique "Installation de l'utilitaire de gestion de la stratégie" à la page 118).

Le fichier de stratégie doit être enregistré sur le serveur Sybase Afaria. Si l'utilitaire est installé sur un autre ordinateur, après la configuration des paramètres l'administrateur doit copier le fichier de stratégie sur le serveur Sybase Afaria.

Après la création du fichier de stratégie, l'administrateur crée un canal qui copie le fichier de stratégie sur les appareils mobiles. L'administrateur doit assurer par la suite le transport du canal vers les appareils mobiles. Le transport est effectué par les outils standards de Sybase Afaria.

Il est conseillé d'utiliser pour les systèmes d'exploitation Microsoft Windows Mobile et Symbian deux canaux distincts pour copier le fichier de stratégie et d'installation de l'application. Cela exclut une nouvelle installation de l'application lors de la mise à jour de la stratégie. Il est conseillé d'utiliser pour les systèmes d'exploitation BlackBerry un seul canal avec la séquence d'installation de l'application définie.

L'administrateur peut créer plusieurs fichiers de stratégie. Le fichier copié sur l'appareil doit porter le nom policy.kes. L'application ne peut pas identifier les fichiers de stratégie avec un autre nom.

Une fois le canal avec le fichier de stratégie transporté sur l'appareil, le fichier de stratégie sera enregistré dans le dossier sélectionné par l'administrateur. Pour les systèmes d'exploitation Microsoft Windows Mobile, l'administrateur doit spécifier le dossier **\Temp**, pour les systèmes d'exploitation Symbian – le dossier **C:\Data**. Pour SE BlackBerry le fichier de stratégie est enregistré automatiquement dans le dossier **store\home\user**.

En cas de modification du fichier de stratégie sur le serveur, les modifications des paramètres seront transportées vers l'appareil lors de la synchronisation suivante des appareils avec Sybase Afaria. La fréquence de synchronisation des appareils mobiles avec Sybase Afaria est définie dans le moniteur par l'administrateur.

En cas de suppression du ficher de stratégie de l'appareil, les valeurs appliquées des paramètres de l'application restent inchangées. Lorsque l'administrateur actualise le fichier de stratégie sur le serveur, ce fichier de stratégie sera encore une fois copié sur les appareils mobiles pendant leur synchronisation avec Sybase Afaria.

Chaque paramètre présent dans la stratégie a un attribut – un "cadenas" qui permet à l'administrateur de gérer la modification des paramètres de l'application sur les appareils mobiles.

Si un paramètre de la stratégie est "verrouillé", après l'application de la stratégie pour les appareils mobiles ils vont utiliser les valeurs définies par la stratégie. Dans ce cas, l'utilisateur de l'appareil mobile ne pourra pas modifier ces valeurs. Pour les paramètres non "verrouillés", l'appareil mobile utilisera les valeurs locales définies par défaut ou par l'utilisateur lui-même.

Une fois l'application installée, l'utilisateur doit saisir le code secret de l'application. Ensuite, l'utilisateur peut configurer les paramètres de fonctionnement Anti-Spam, des Contacts personnels et d'autres composants si l'administrateur n'a pas interdit leur modification.

PROCEDURE DU DEPLOIEMENT DE L'APPLICATION VIA SYBASE AFARIA

La distribution de Sybase Afaria contient une archive auto-extractible KES8_forSybaseAfaria_fr.exe, avec des fichiers suivants qui assurent l'installation de l'application sur les appareils mobiles :

- endpoint_MDM_Afaria_8_0_x_xx_fr.cab : fichier d'installation de l'application pour le système d'exploitation Microsoft Windows Mobile ;
- endpoint8_mobile_8_x_xx_eu4.sisx : fichier d'installation de l'application pour le système d'exploitation Symbian ;
- Endpoint8_Mobile_Installer.cod : fichier d'installation de l'application pour le système d'exploitation BlackBerry ;
- KES2Afaria.exe : utilitaire de gestion de la stratégie pour l'application Kaspersky Endpoint Security 8 for Smartphone ;
- kl.pbv, licensing.dll, oper.pbv : ensemble des fichiers qui font partie de l'utilitaire KES2Afaria.exe et assurent son fonctionnement.

L'installation est effectuée selon la procédure standard d'installation d'application via Sybase Afaria.

L'administrateur installe l'utilitaire de gestion de la stratégie KES2Afaria.exe sur le poste de travail ou directement sur le serveur Sybase Afaria. Une fois l'installation terminée, l'administrateur crée la stratégie en y ajoutant la licence et enregistre les paramètres configurés dans le fichier de stratégie. Si la licence est inaccessible, l'administrateur peut l'ajouter ultérieurement.

Ensuite, l'administrateur crée un canal pour appliquer la stratégie et installer l'application sur les appareils. Il est conseillé d'utiliser pour les systèmes d'exploitation Microsoft Windows Mobile et Symbian deux canaux Software Manager Channel pour copier le fichier de stratégie et la distribution de l'application sur les appareils.

S'il s'agit du système d'exploitation BlackBerry, il faut utiliser un canal Session Manager Channel. L'administrateur doit y créer une liste des tâches (worklist) où il ajoute le script avec la séquence d'installation de l'application.

L'administrateur doit effectuer l'installation de l'application en suivant strictement la séquence : il faut d'abord transmettre le fichier de stratégie sur l'appareil et ensuite la distribution de l'application. Si la séquence d'installation de l'application sur l'appareil n'est pas respectée, l'application ne sera pas opérationnelle.

La publication et la transmission des canaux sont effectuées par les procédés standards Sybase Afaria. Pendant la synchronisation des appareils mobiles avec Sybase Afaria les canaux sont transmis sur les appareils, ensuite ils reçoivent le fichier de la stratégie et exécutent l'installation automatique de l'application. Les paramètres configurés par l'administrateur sont appliqués après l'installation de l'application.

Si l'administrateur a ajouté une licence à la stratégie, cette licence sera installée pendant l'application de la stratégie pour activer l'application.

À la première exécution de l'application, l'utilisateur devra saisir le code secret. Ensuite, l'utilisateur peut installer les paramètres des composants Anti-Spam et Contacts personnels, et les paramètres des autres composants si l'administrateur n'a pas interdit leur modification.

L'administrateur pourra modifier ultérieurement les paramètres de la stratégie. Lorsque l'administrateur actualise le fichier de stratégie sur le serveur, pendant la synchronisation suivante des appareils avec le serveur Sybase Afaria le fichier de stratégie sera actualisé sur l'appareil et les paramètres de l'application seront modifiés.

Ainsi, le déploiement de l'application comprend les étapes suivantes :

1. Installation de l'utilitaire (cf. la rubrique "Installation de l'utilitaire de gestion de la stratégie" à la page 118).
2. Création de la stratégie, configuration des paramètres de l'application et ajout de la licence de l'application.
3. Création d'un canal / système de canaux pour installer l'application sur les appareils et appliquer la stratégie (cf. la rubrique "Installation de l'application" à la page 137).
4. Diffusion du canal / du système des canaux sur les appareils. Cette procédure est assurée par les outils standards de Sybase Afaria.
5. Installation de l'application sur les appareils mobiles (cf. la rubrique "Installation de l'application sur les appareils mobiles" à la page 142).

PREPARATION AU DEPLOIEMENT DE KASPERSKY ENDPOINT SECURITY 8 FOR SMARTPHONE

Avant de déployer Kaspersky Endpoint Security 8 for Smartphone via Sybase Afaria, l'administrateur doit s'assurer que les conditions suivantes sont satisfaites :

1. Sybase Afaria est déployé et configuré dans le réseau.
2. Les appareils sont conformes aux spécifications matérielles et système d'installation de l'application.
3. Les groupes d'appareils (Groups) sur le serveur Sybase Afaria ont été créés.
4. Les profiles d'appareils (Profiles) sur le serveur Sybase Afaria ont été créés.
5. La synchronisation des appareils avec le serveur Sybase Afaria a été configurée : l'application **Client Afaria** est installée sur les appareils.

INSTALLATION DE L'UTILITAIRE DE GESTION DE LA STRATEGIE

L'utilitaire KES2Afaria.exe est utilisé pour créer et modifier les stratégies de Kaspersky Endpoint Security 8 for Smartphone.

L'utilitaire fait partie de la distribution KES8_forSybaseAfaria_fr.exe et peut être installé sur le poste de travail de l'administrateur ou sur le serveur Sybase Afaria.

Vous avez besoin des fichiers kl.pbv, licensing.dll, oper.pbv pour lancer l'utilitaire. Ces fichiers aussi font partie de la distribution et doivent être enregistrés dans le même dossier que l'utilitaire.

- *Pour installer l'utilitaire,*

  copiez les fichiers KES2Afaria.exe, kl.pbv, licensing.dll, oper.pbv depuis la distribution de l'application dans un même dossier sur le poste de travail ou sur le serveur Sybase Afaria.

CREATION DE LA STRATEGIE. CONFIGURATION DES PARAMETRES DE KASPERSKY ENDPOINT SECURITY 8 FOR SMARTPHONE

Après l'installation de l'utilitaire KES2Afaria.exe, vous devez créer la stratégie Kaspersky Endpoint Security 8 for Smartphone.

Vous pouvez créer une nouvelle stratégie ou modifier les paramètres de la stratégie existante (cf. la rubrique "Modification de la stratégie" à la page 137).

Pendant la modification des paramètres, vous pouvez utiliser le bouton pour autoriser / interdire la modification des paramètres sur l'appareil mobile.

Les sections suivantes présentent les procédures détaillées pour configurer les paramètres de chacun des composants de l'application.

Pour créer la stratégie de Kaspersky Endpoint Security 8 for Smartphone, procédez comme suit :

1. Exécutez l'utilitaire **KES2Afaria.exe**.

   La fenêtre **Kaspersky Endpoint Security 8 for Smartphone** avec les paramètres des composants de l'application s'affiche.

2. Configurez les paramètres de chacun des composants de l'application.

3. Enregistrez le fichier de stratégie que vous avez reçu en sélectionnant le menu **Fichier →Enregistrer sous**.

Si vous avez installé l'utilitaire sur le poste de travail, vous devez copier le fichier de stratégie reçu sur le serveur après la configuration des paramètres.

DANS CETTE SECTION

CONFIGURATION DES PARAMETRES DE LA FONCTION PROTECTION

Pour configurer les paramètres de la fonction Protection, procédez comme suit :

1. Ouvrez l'onglet **Protection** dans la fenêtre de **Kaspersky Endpoint Security 8 for Smartphone** (cf. ill. ci-après).

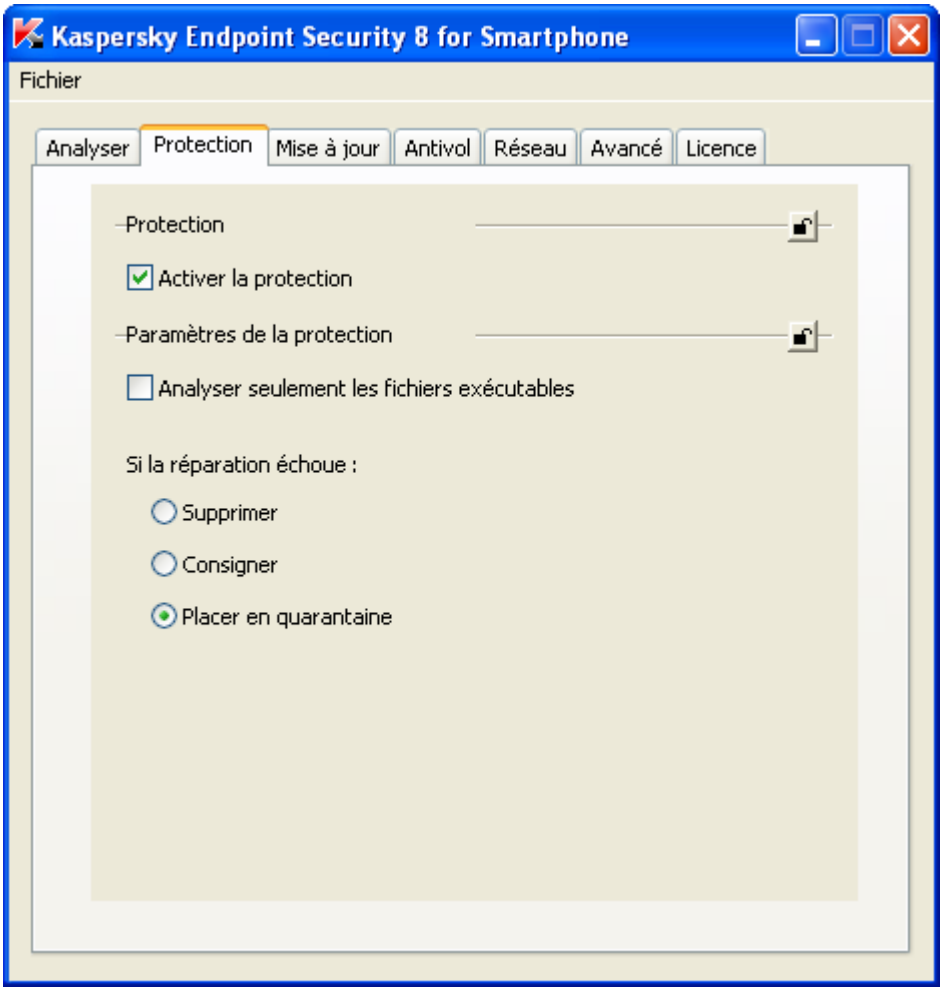


*Figure 70: Onglet **Protection***

2. Activez / désactivez la fonction Protection de l'appareil. Pour ce faite, dans le groupe **Protection** cochez / décochez la case **Activer la protection**.

   Par défaut, la Protection est activée et la case **Activer la protection** est cochée.

3. Sélectionnez le type de fichiers à analyser par Kaspersky Endpoint Security 8 for Smartphone.

   Pour que l'application analyse uniquement les fichiers exécutables, dans le groupe **Paramètres de la protection** cochez la case **Analyser seulement les fichiers exécutables**.

   Pour que l'application analyse les fichiers de tous les types, décochez la case **Analyser seulement les fichiers exécutables**.

   Par défaut, l'application analyse tous les types de fichiers et la case **Analyser seulement les fichiers exécutables** est décochée.

4. Sélectionnez l'action que Kaspersky Endpoint Security 8 for Smartphone exécutera en cas de détection d'une menace. Pour ce faire, sélectionnez dans le groupe **Paramètres de la protection** une des valeurs proposées pour le paramètre **Si la réparation échoue** :

   - **Supprimer :** supprime physiquement les objets malveillants sans notifier l'utilisateur.
   - **Consigner :** ignore les objets malveillants, mais consigne les informations relatives à leur découverte dans le journal de l'application et bloque les tentatives d'accès à l'objet (par exemple, copie ou ouverture).

- **Placer en quarantaine** : place les objets malveillants en quarantaine.

Par défaut, l'application place les objets malveillants détectés en quarantaine et la valeur **Placer en quarantaine** est sélectionnée.

CONFIGURATION DES PARAMETRES DE LA FONCTION ANALYSE A LA DEMANDE

Pour configurer les paramètres de l'Analyse à la demande, procédez comme suit :

1. Ouvrez l'onglet **Analyse** dans la fenêtre de **Kaspersky Endpoint Security 8 for Smartphone** (cf. ill. ci-après).

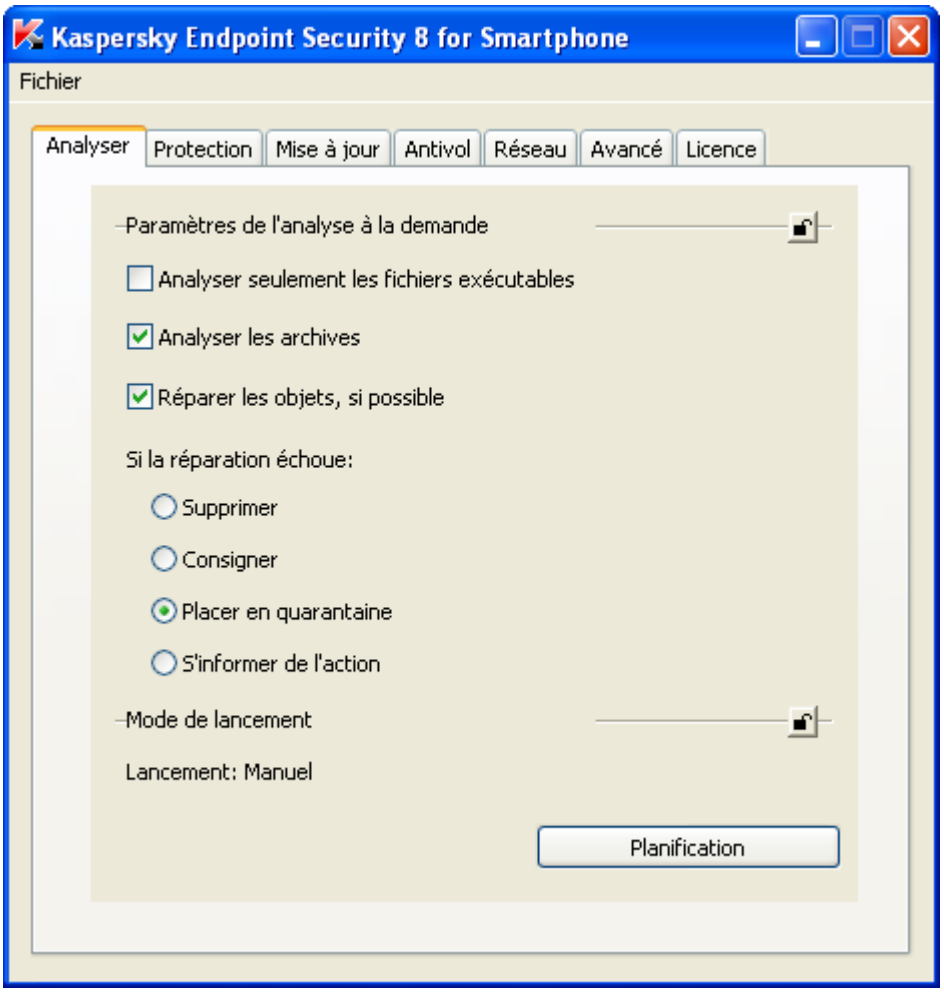


*Figure 71: Onglet **Analyser***

2. Sélectionnez le type de fichiers à analyser par Kaspersky Endpoint Security 8 for Smartphone.

   Pour que l'application analyse uniquement les fichiers exécutables, dans le groupe **Paramètres de l'analyse à la demande** cochez la case **Analyser seulement les fichiers exécutables**. Anti-Virus prend en charge l'analyse des fichiers exécutables des applications des formats suivants : EXE, DLL, MDL, APP, RDL, PRT, PXT, LDD, PDD, CLASS.

   Pour que l'application analyse tous les types de fichiers, dans le groupe **Paramètres de l'analyse à la demande** décochez la case **Analyser seulement les fichiers exécutables**.

   Par défaut, l'application analyse tous les types de fichiers et la case **Analyser seulement les fichiers exécutables** est décochée.

3. Activez / désactivez l'analyse des archives stockées sur les appareils. Pour ce faire, dans le groupe **Paramètres de l'analyse à la demande** cochez / décochez la case **Analyser les archives**.

Pour Microsoft Windows Mobile, l'application analyse par défaut les archives des formats suivants : ZIP, JAR, JAD и CAB. Pour Symbian, l'application permet d'analyser les archives des formats suivants : ZIP, JAR, JAD, SIS и SISX.

Si la case **Analyser les archives** n'est pas cochée et la case **Analyser uniquement les types de fichiers exécutables** est décochée, l'application analysera tous les fichiers sauf les fichiers archivés.

Par défaut, l'application décompresse et analyse les archives, et la case **Analyser les archives** est cochées.

4. Activez / désactivez la tentative de l'application de réparer les objets détectés au moment de la détection. Pour ce faire, dans le groupe **Paramètres de l'analyse à la demande** cochez / décochez la case **Réparer les objets, si possible**.

   Par défaut, l'application tente de réparer l'objet malveillant détecté et la case **Réparer les objets, si possible** est cochée.

5. Sélectionnez l'action que l'application exécutera en cas de détection des objets malveillants. Pour ce faire, sélectionnez dans le groupe **Paramètres de l'analyse à la demande** une des valeurs proposées pour le paramètre **Si la réparation échoue** :

   - **Supprimer :** supprime physiquement les objets malveillants sans notifier l'utilisateur.
   - **Consigner** : ignore les objets malveillants mais consigne les informations relatives à leur découverte dans le journal de l'application.
   - **Placer en quarantaine** : bloque l'objet, déplace l'objet vers un dossier spécifique – celui de quarantaine.
   - **S'informer de l'action** : notifie l'utilisateur en cas de détection d'un objet malveillant et lui propose de sélectionner l'action à exécuter sur l'objet détecté.

6. Sélectionnez le mode de lancement de l'Analyse à la demande sur l'appareil. Pour ce faire, cliquez dans le groupe **Mode de lancement** sur **Planification** et sélectionnez dans la fenêtre **Planification** qui s'ouvre un des types de lancement suivants :

   - **Manuel** : désactive l'analyse programmée. L'utilisateur lance l'analyse en temps voulu.
   - **Chaque jour** : l'analyse s'exécutera tous les jours. Indiquez l'heure de lancement dans le champ **Heure de lancement**. L'heure est spécifiée pour une journée de 24h au format HH:MM.
   - **Chaque semaine** : l'analyse s'exécutera une fois par semaine. Indiquez l'heure et le jour de lancement de l'analyse. Pour ce faire, sélectionnez dans la liste déroulante le jour de lancement et saisissez l'heure de lancement dans le champ **Heure de lancement**. L'heure est spécifiée pour une journée de 24h au format HH:MM.

   Par défaut, l'analyse à la demande est lancée par l'utilisateur en mode manuel et la valeur du paramètre **Type de lancement** est **Manuel**.

CONFIGURATION DES PARAMETRES DE LA MISE A JOUR DES BASES ANTIVIRUS

Pour configurer les paramètres de la mise à jour des bases antivirus, procédez comme suit :

1. Ouvrez l'onglet **Mise à jour** dans la fenêtre **Kaspersky Endpoint Security 8 for Smartphone** (cf. ill. ci-après).

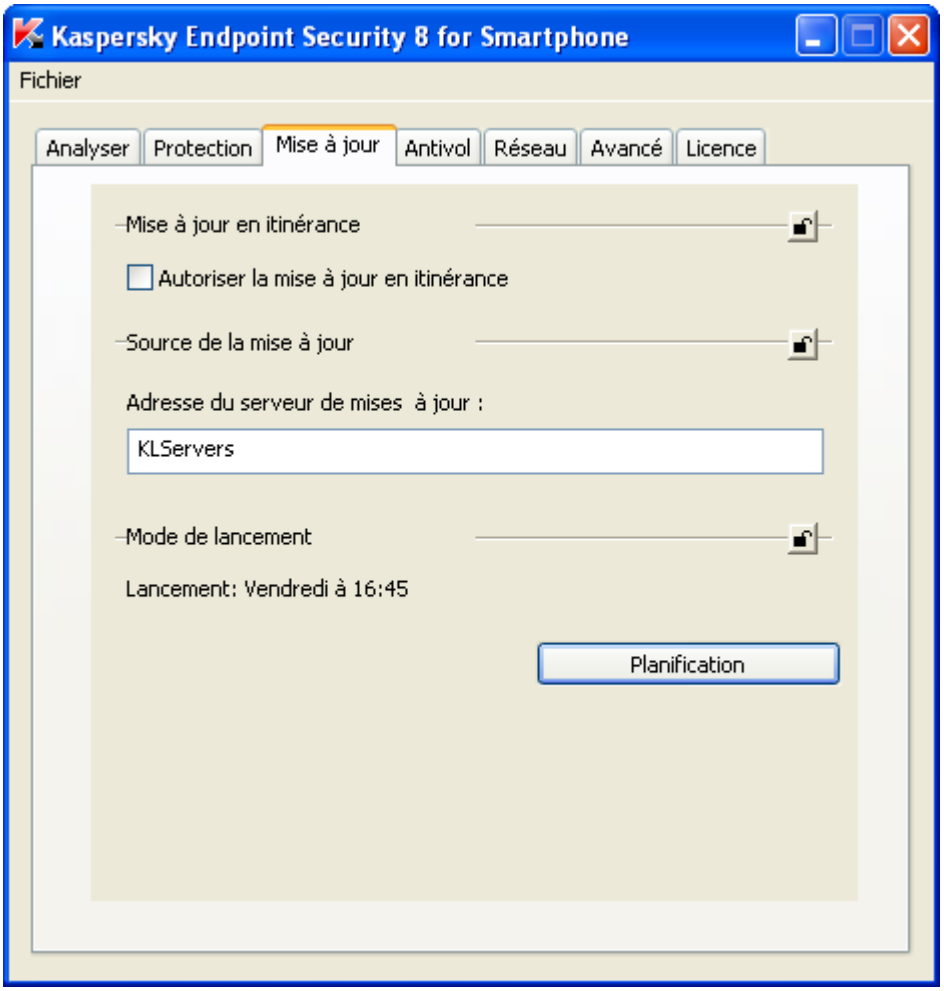


*Figure 72: Onglet **Mise à jour***

2. Autorisez / interdisez l'exécution automatique de la mise à jour programmée des bases antivirus lorsque l'appareil est en itinérance. Pour ce faire, cochez / décochez dans le groupe **Mise à jour en itinérance** la case **Autoriser la mise à jour en itinérance**.

   Par défaut, la mise à jour automatique en itinérance est interdite et la case **Autoriser la mise à jour en itinérance** est décochée.

3. Spécifiez l'adresse de la source pour télécharger les mises à jour des bases antivirus. Vous pouvez spécifier un serveur HTTP un dossier local ou un dossier réseau (par exemple, http://domain.com/index/). Pour ce faire, dans le groupe **Source de notifications** remplissez le champ **Adresse du serveur de mises à jour**.

   La structure des dossiers dans la source de la mise à jour doit être identique à celle du serveur de mise à jour Kaspersky Lab.

   Par défaut, ce champ contient l'adresse des serveurs de mises à jour du Kaspersky Lab **KLServeurs**.

4. Sélectionnez le mode de lancement des mises à jour. Pour ce faire, cliquez dans le groupe **Mode de lancement** sur **Planification** et sélectionnez dans la fenêtre **Planification** qui s'ouvre un des types de lancement suivants :

- **Manuel** : désactive la mise à jour selon planification. L'utilisateur lance la mise à jour des bases antivirus de l'application en temps voulu.
- **Chaque jour** : exécute la mise à jour tous les jours. Indiquez l'heure de lancement dans le champ **Heure de lancement**. L'heure est spécifiée pour une journée de 24h au format HH:MM.
- **Chaque semaine** : exécute la mise à jour une fois par semaine. Indiquez l'heure et le jour de lancement de la mise à jour. Pour ce faire, sélectionnez dans la liste déroulante le jour de lancement et saisissez l'heure de lancement dans le champ **Heure de lancement**. L'heure est spécifiée pour une journée de 24h au format HH:MM.

Par défaut, la mise à jour est exécutée une fois par semaine, la valeur du paramètre **Type de lancement** est **Chaque semaine**. Le jour de lancement est la date actuelle. L'heure de lancement est l'heure de lancement de l'utilitaire +1 minute.

CONFIGURATION DES PARAMETRES DU COMPOSANT ANTIVOL

Configuration des paramètres du composant Antivol prévoit la configuration des fonctions suivantes :

- Suppression (cf. la rubrique "Configuration des paramètres de la fonction Suppression" à la page 124).
- Verrouillage (cf. la rubrique "Configuration des paramètres de la fonction Verrouillage" à la page 127).
- SIM-Surveillance (cf. la rubrique "Configuration des paramètres de la fonction SIM-Surveillance" à la page 128).
- Géolocalisation (cf. la rubrique "Configuration des paramètres de la fonction Géolocalisation" à la page 130).

DANS CETTE SECTION

CONFIGURATION DES PARAMETRES DE LA FONCTION SUPPRESSION

Pour configurer les paramètres de la fonction Suppression, procédez comme suit :

1. Ouvrez l'onglet **Antivol** dans la fenêtre **Kaspersky Endpoint Security 8 for Smartphone** (cf. ill. ci-après).

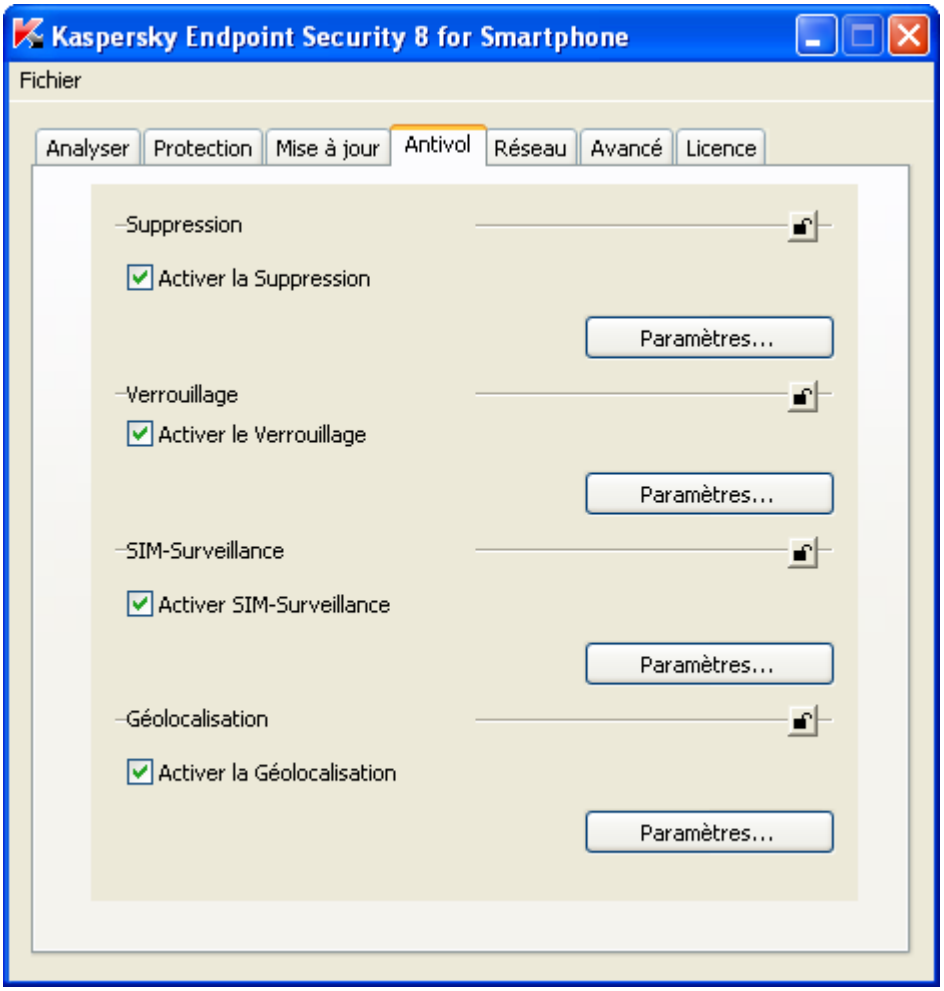


*Figure 73: Onglet **Antivol***

2. Activez / désactivez l'utilisation de la fonction Suppression de l'appareil. Pour ce faire, dans le groupe **Suppression** cochez / décochez la case **Activer la Suppression**.

   Par défaut, la fonction Suppression est désactivée.

3. Si vous avez activé la fonction Suppression, sélectionnez les données que l'application va supprimer de l'appareil après la réception d'une instruction SMS. Pour ce faire, dans le groupe **Suppression des données** cliquez sur **Paramètres** et dans la fenêtre **Paramètres de suppression des données** procédez comme suit en fonction des conditions suivantes :

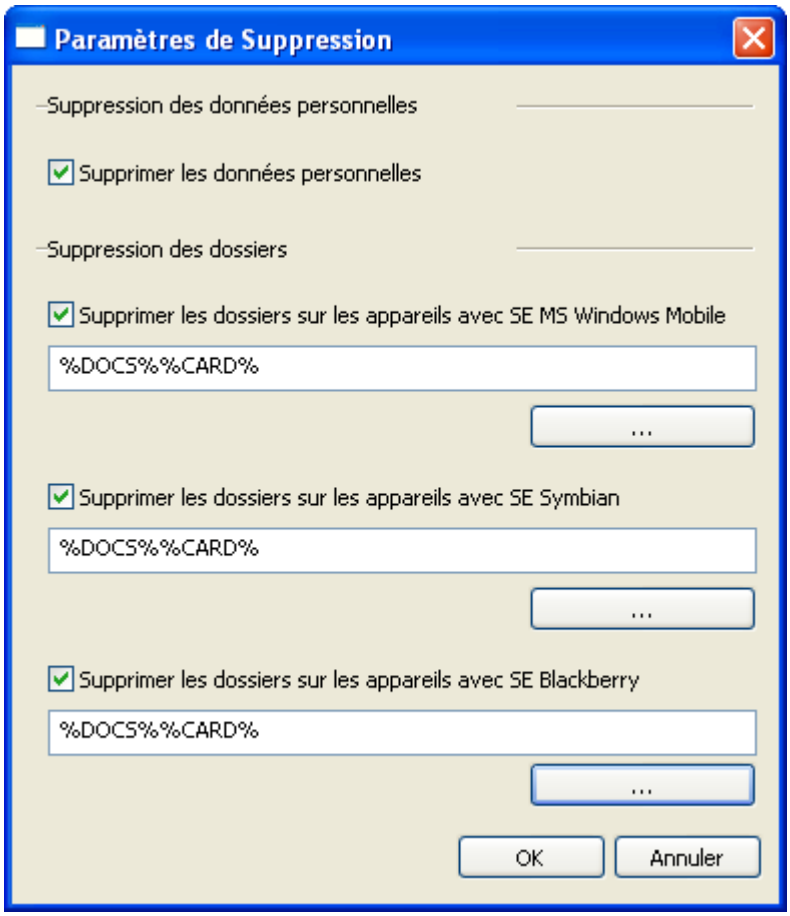


Figure 74: paramètres de la fonction de suppression de données

- Pour que l'application supprime les données personnelles de l'appareil à la réception de l'instruction de l'utilisateur, cochez dans le groupe **Suppression des données personnelles** la case **Supprimer les données personnelles**.

  L'application permet de supprimer les informations suivantes stockées sur les appareils tournant sous SE Microsoft Windows Mobile et Symbian : entrées des Contacts et sur la carte SIM, SMS, galerie, calendrier, paramètres de connexion à Internet. L'application supprime les informations personnelles suivantes stockées sur les appareils tournant sous BlackBerry : entrées des Contacts, calendrier, messages électroniques, journal des appels. L'utilisateur ne pourra pas restaurer ces données ! La fonction est activée lorsque l'appareil reçoit l'instruction SMS spéciale.

  Par défaut, la case **Supprimer les données personnelles** est cochée.

- Pour autoriser l'application à supprimer les fichiers stockés sur l'appareil et mis sur la liste des dossiers à supprimer à la réception de l'instruction de l'utilisateur, dans le groupe **Suppression des dossiers** cochez la case **Supprimer les dossiers des appareils avec SE <nom_du_système_d'exploitation>**, appuyez sur le bouton ... et dans la fenêtre **Choix des dossiers à supprimer** spécifiez les dossiers à supprimer.

  La liste des dossiers à supprimer comprend les dossiers ajoutés par l'administrateur et les dossiers ajoutés à la main par l'utilisateur de l'appareil. L'utilisateur ne peut pas supprimer de la liste les dossiers mis sur la liste par l'administrateur.

Vous pouvez utiliser les macros des dossiers pour créer la liste des dossiers. Pour utiliser une macro afin de supprimer le contenu du dossier **Mes documents**, dans la fenêtre **Choix des dossiers à supprimer** cliquez sur **Mes documents**. La macro **%DOCS%** s'ajoute. Pour utiliser une macro afin de chiffrer les données sur la carte mémoire, dans la fenêtre **Choix des dossiers à supprimer** cliquez sur **Carte mémoire**. La macro **%CARD%** s'ajoute.

L'application tournant sous Microsoft Windows Mobile supprime avec **%DOCS%** le dossier **Mes documents** (le nom exact dépend de la localisation de l'appareil) et avec **%CARD%** les dossiers stockés sur toutes les cartes mémoire accessibles sur l'appareil.

L'application tournant sous Symbian supprime avec **%DOCS%** le dossier **C:\Data** et avec **%CARD%** les dossiers stockés sur toutes les cartes mémoire accessibles sur l'appareil.

L'application tournant sous SE BlackBerry supprime avec **%DOCS%** le dossier **\store\home\user\documents** et avec **%CARD%** le dossier **\SDCard**.

Par défaut, la liste des dossiers à supprimer est vide.

CONFIGURATION DES PARAMETRES DE LA FONCTION VERROUILLAGE

Pour configurer les paramètres de Verrouillage, procédez comme suit :

1. Ouvrez l'onglet **Antivol** dans la fenêtre **Kaspersky Endpoint Security 8 for Smartphone** (cf. ill. ci-après).

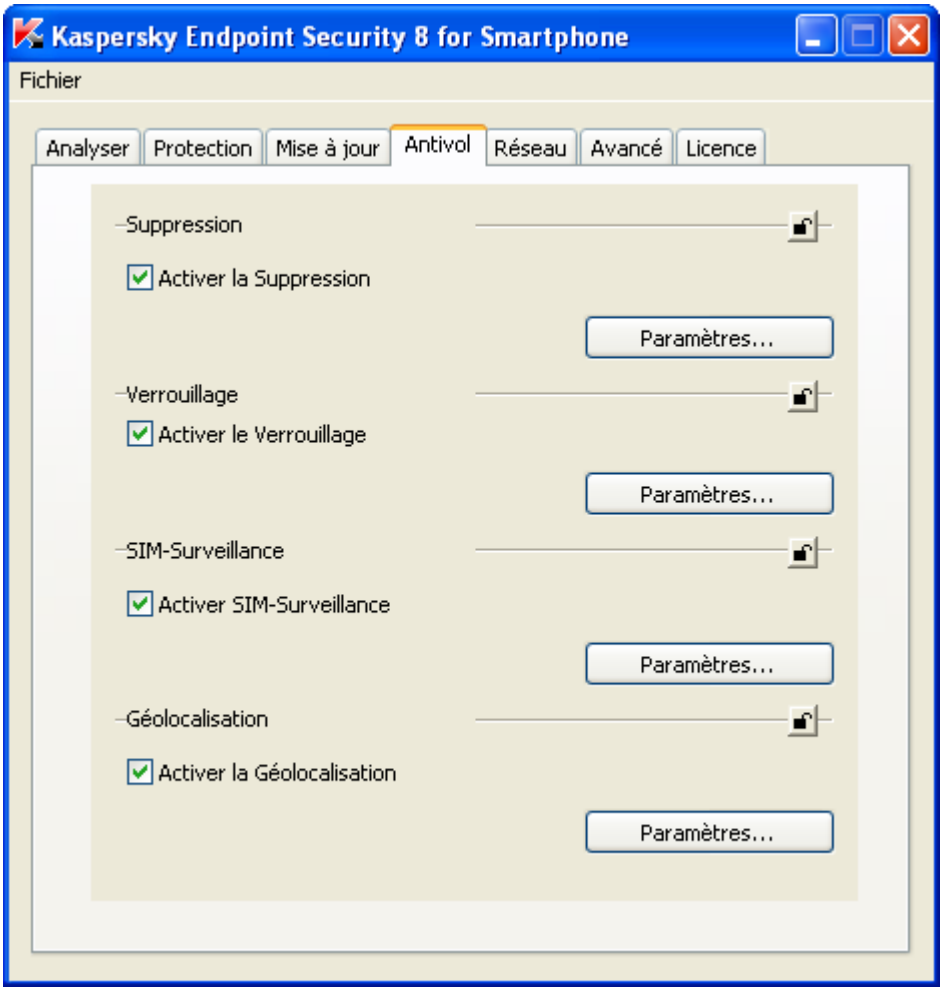


*Figure 75: Onglet **Antivol***

2. Activez / désactivez l'utilisation de la fonction Verrouillage de l'appareil. Pour ce faite, dans le groupe **Verrouillage** cochez / décochez la case **Activer le verrouillage**.

   La fonction Verrouillage est désactivée par défaut.

   Pour afficher un texte sur l'écran de l'appareil verrouillé, dans le groupe **Verrouillage** cliquez sur **Paramètres** et dans la fenêtre **Paramètres de verrouillage** qui s'ouvre remplissez le champ **Texte en cas de verrouillage**. Par défaut, aucun texte n'est saisi.

CONFIGURATION DES PARAMETRES DE LA FONCTION SIM-SURVEILLANCE

Pour configurer les paramètres Antivol, procédez comme suit :

1. Ouvrez l'onglet **Antivol** dans la fenêtre **Kaspersky Endpoint Security 8 for Smartphone** (cf. ill. ci-après).

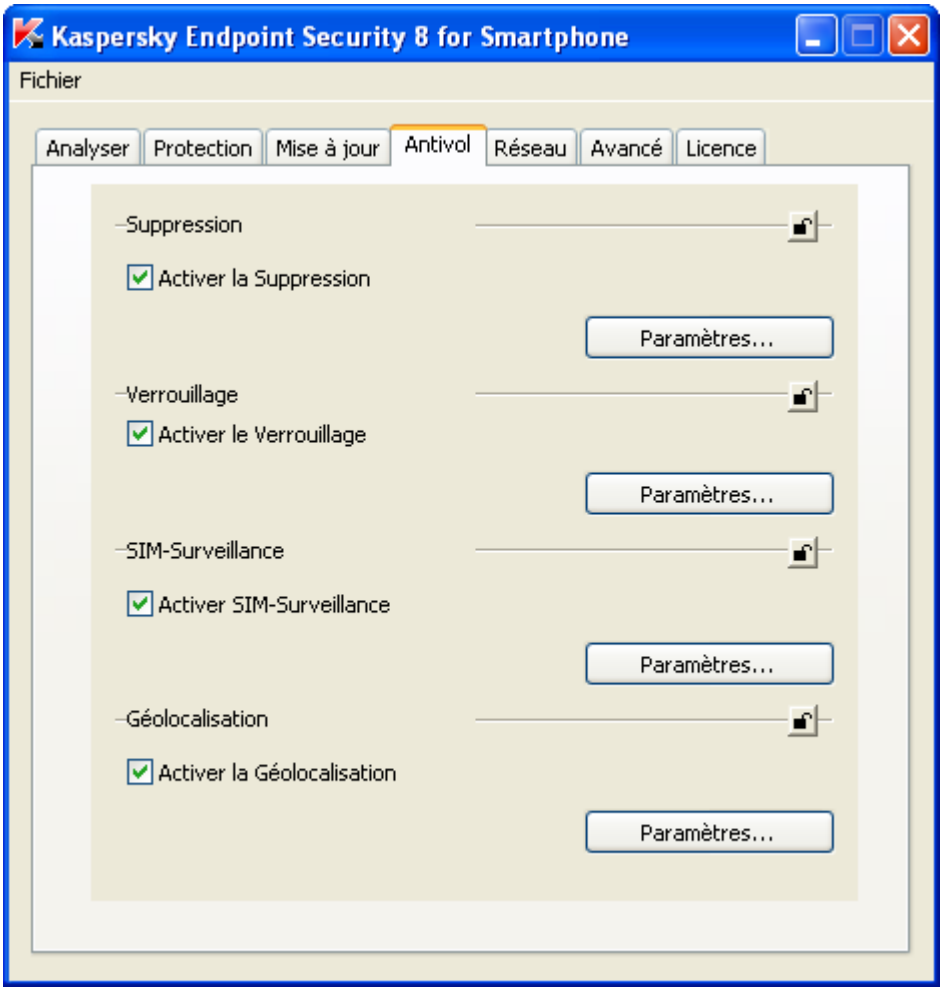


*Figure 76: Onglet **Antivol***

2. Activez / désactivez l'utilisation de la fonction SIM-Surveillance de l'appareil. Pour ce faire, cochez / décochez dans le groupe **SIM-Surveillance** la case **Activer SIM-Surveillance**.

   Par défaut, la fonction SIM-Surveillance est désactivée.

3. Spécifiez l'action que l'application exécutera au remplacement de la carte SIM de l'appareil.

   Pour envoyer le nouveau numéro de téléphone au remplacement de la carte SIM de l'appareil, dans le groupe **SIM-Surveillance** cliquez sur **Paramètres** et dans la fenêtre **Paramètres de SIM-surveillance** (cf. ill. ci-après) qui s'ouvre, procédez comme suit en fonction des conditions suivantes :

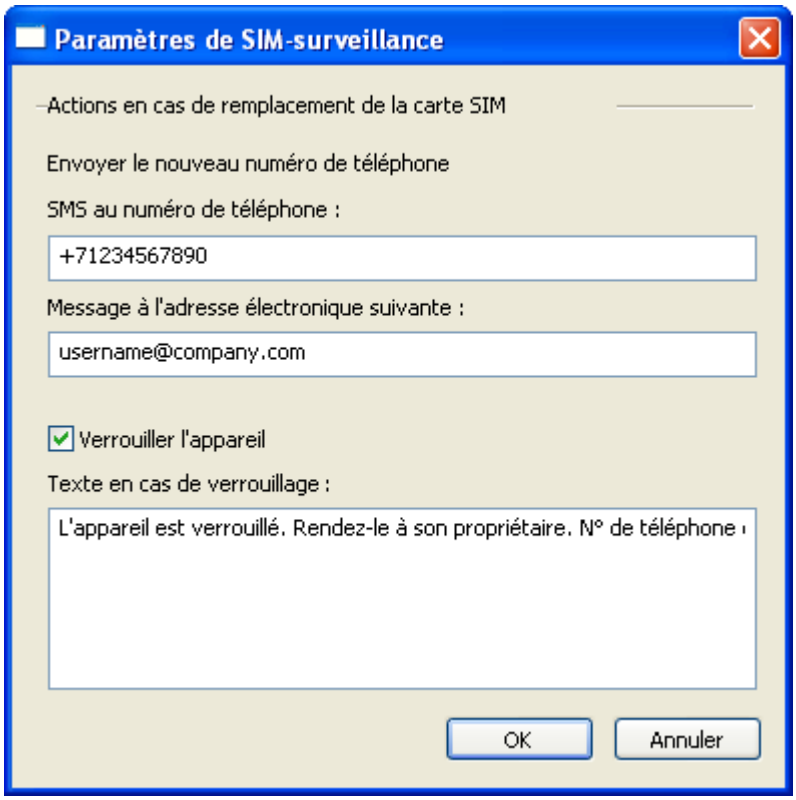


Figure 77: paramètres de la fonction SIM-Surveillance

- Pour envoyer un SMS avec le nouveau numéro de téléphone vers le numéro de téléphone défini, saisissez-le dans le champ **SMS au numéro de téléphone**. Ces numéros peuvent commencer par un chiffre ou par le signe "+" et ne peuvent contenir que des chiffres. Il est conseillé de saisir le numéro au format utilisé par votre opérateur de téléphonie mobile.
- Pour recevoir le nouveau numéro à l'adresse électronique, saisissez-le dans le champ **Message à l'adresse électronique**.

Pour verrouiller l'appareil au remplacement de la carte SIM, dans le groupe **SIM-Surveillance** cliquez sur **Paramètres**, et dans la fenêtre **Paramètres de SIM-surveillance** qui s'ouvre cochez la case **Verrouiller l'appareil** en saisissant dans le champ **Texte en cas de verrouillage** le texte qui apparaîtra sur l'écran de l'appareil verrouillé.

CONFIGURATION DES PARAMETRES DE LA FONCTION GEOLOCALISATION

Pour configurer les paramètres Antivol, procédez comme suit :

1. Ouvrez l'onglet **Antivol** dans la fenêtre **Kaspersky Endpoint Security 8 for Smartphone** (cf. ill. ci-après).

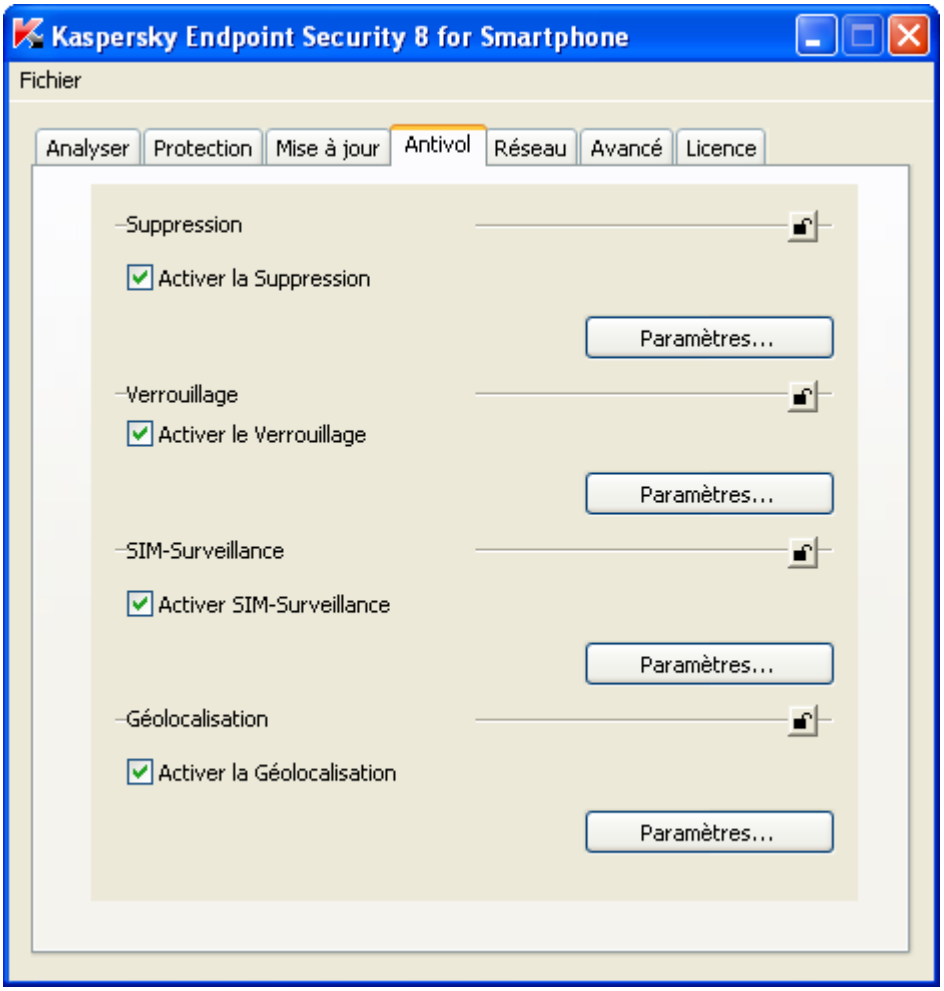


*Figure 78: Onglet **Antivol***

2. Activez / désactivez l'utilisation de la fonction Géolocalisation de l'appareil. Pour ce faire, cochez / décochez dans le groupe **Géolocalisation** la case **Activer la Géolocalisation**.

   Par défaut, l'application envoie les coordonnées uniquement par SMS à l'appareil qui a émis l'instruction SMS. Par défaut, la fonction Géolocalisation est désactivée.

   Pour envoyer les coordonnées de l'appareil à l'adresse électronique définie, dans le groupe **Géolocalisation** cliquez sur **Paramètres** et dans la fenêtre qui s'ouvre saisissez l'adresse dans le champ **Message à l'adresse électronique**.

CONFIGURATION DES PARAMETRES DU COMPOSANT PARE-FEU

Pour configurer les paramètres du composant Pare-feu, procédez comme suit :

1. Ouvrez l'onglet **Réseau** (cf. ill. ci-après).

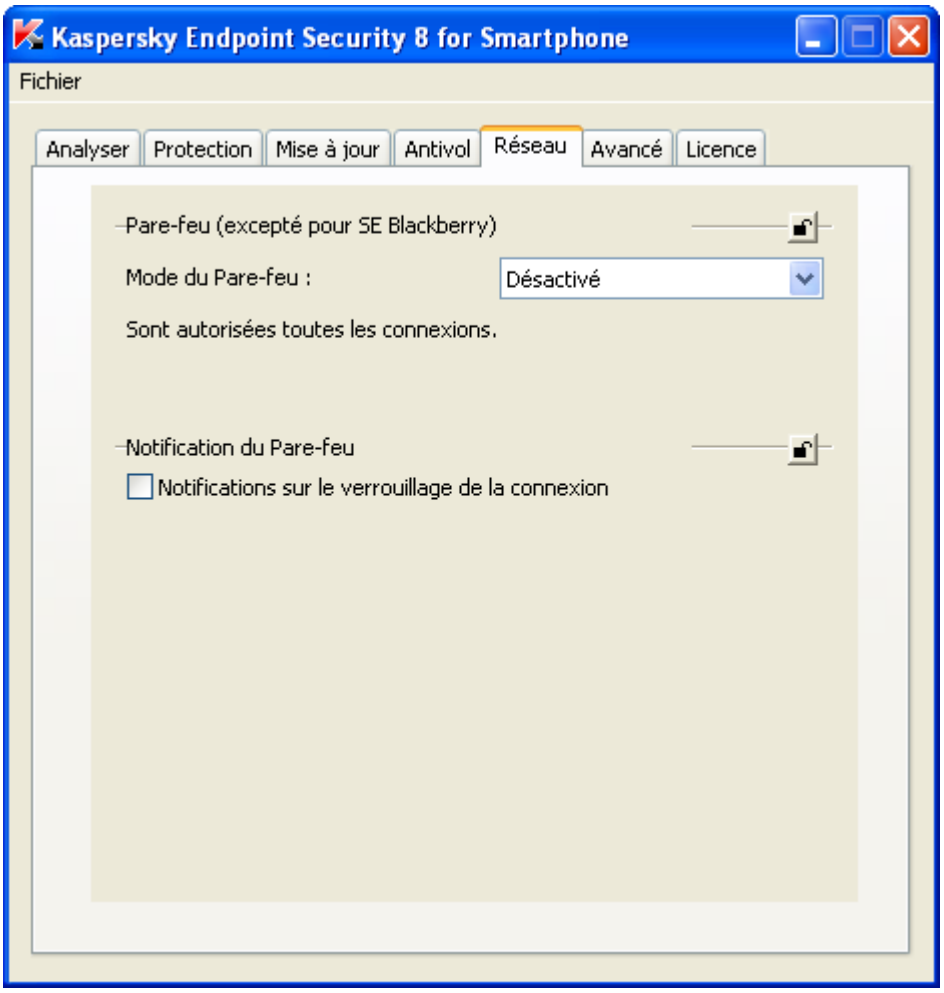


*Figure 79: Onglet **Réseau***

2. Sélectionner le mode Pare-feu pour définir les connexions autorisées et interdites sur l'appareil. Pour ce faire, sélectionnez dans la liste déroulante **Mode du Pare-feu** une des valeurs suivantes :

   - **Désactivé** : autorisation de la moindre activité de réseau. Le Pare-feu est désactivé.
   - **Protection minimum** : bloque uniquement les connexions entrantes. Les connexions sortantes sont autorisées.
   - **Protection maximum** : bloque toutes les connexions entrantes. L'utilisateur peut recevoir les messages électroniques, surfer sur le Web et télécharger les fichiers. Les connexions sortantes peuvent être réalisées uniquement via les ports SSH, HTTP, HTTPS, IMAP, SMTP, POP3.
   - **Tout bloquer** : bloque toute activité de réseau, sauf la mise à jour des bases antivirus et la connexion au Serveur d'administration.

   Par défaut, le Pare-feu n'est pas activé et la valeur du paramètre **Mode du Pare-feu** est **Désactivé**.

3. Activez / désactivez les notifications à l'utilisateur sur le blocage des connexions. Pour ce faire, cochez / décochez dans le groupe **Notification du Pare-feu** la case **Notifications sur le blocage des connexions**.

   Par défaut, les notifications du Pare-feu sont désactivées.

CONFIGURATION DES PARAMETRES DU COMPOSANT CHIFFREMENT

Pour configurer les paramètres du composant Chiffrement, procédez comme suit :

1. Ouvrez l'onglet **Avancé** (cf. ill. ci-après).

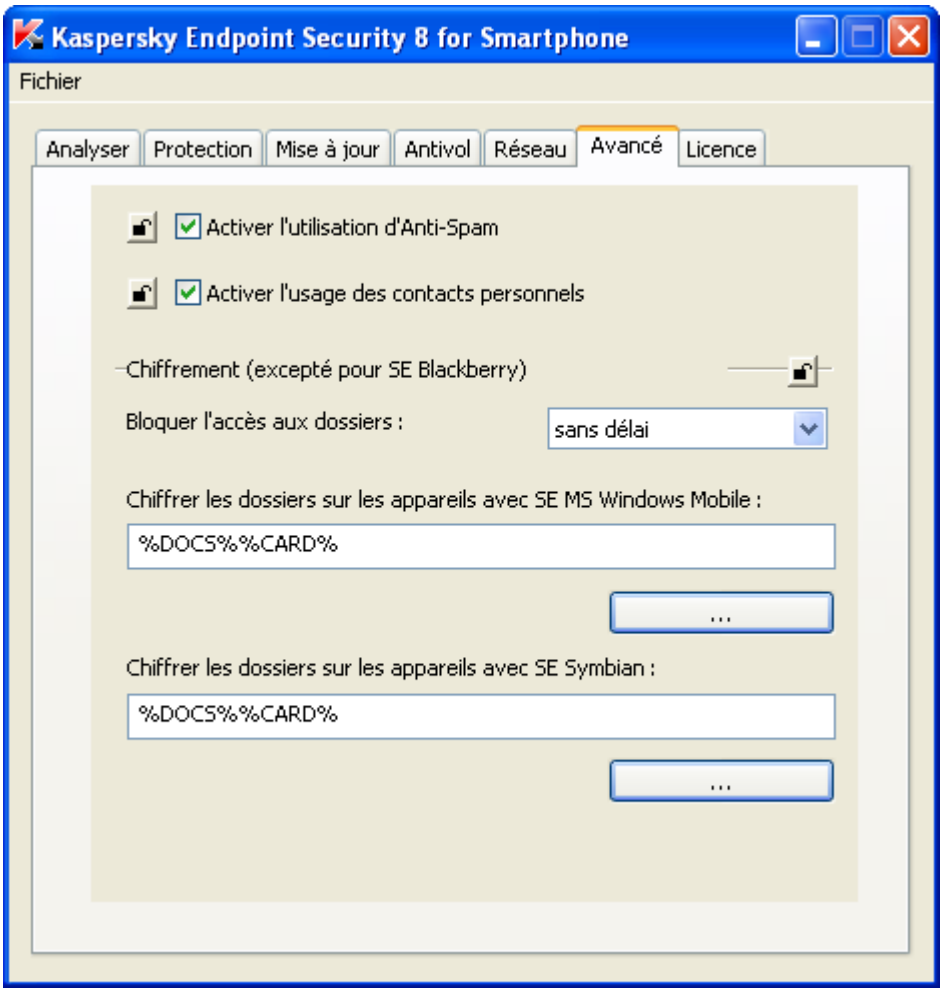


*Figure 80: Onglet **Avancé***

2. Spécifiez la période à l'issue de laquelle après le passage de l'appareil en mode économie énergétique l'application bloque l'accès aux données chiffrées. Pour ce faire, sélectionnez une valeur de la liste déroulante **Bloquer l'accès**.

   Par défaut, l'accès aux dossiers chiffrés utilisés est bloqué directement après le passage de l'appareil en mode économie énergétique. La valeur sélectionnée pour le paramètre **Bloquer l'accès** est **Sans délai**.

3. Rédigez une liste des dossiers chiffrés sur les appareils pour le système d'exploitation sélectionné. Pour y accéder, l'utilisateur devra saisir le code secret de l'application. La liste comprend les dossiers ajoutés par l'administrateur et les dossiers ajoutés à la main par l'utilisateur de l'appareil. L'utilisateur ne peut pas déchiffrer ou supprimer de la liste des dossiers pour le chiffrement les dossiers chiffrés par l'administrateur.

   Pour rédiger la liste des dossiers chiffrés spécifiez-les dans les champs **Chiffrer les dossiers des appareils tournants sous <nom_du_système_d'exploitation>** ou appuyez sur le bouton 

qui correspond au système d'exploitation requis. Dans la fenêtre **Choix des dossiers pour le chiffrement** qui s'ouvre, spécifiez les dossiers à chiffrer sur l'appareil.

   Vous pouvez utiliser les macros des dossiers pour créer la liste des dossiers. Pour utiliser une macro afin de chiffrer le contenu du dossier **Mes documents**, dans la fenêtre **Choix des dossiers pour le chiffrement** cliquez sur **Mes documents**. La macro **%DOCS%** s'ajoute. Pour utiliser une macro afin de chiffrer les données sur la carte mémoire, dans la fenêtre **Sélection du dossier à chiffrer** cliquez sur **Carte mémoire**. La macro **%CARD%** s'ajoute.

L'application tournant sous Microsoft Windows Mobile chiffre avec la macro **%DOCS%** le dossier **Mes documents** (le nom exact dépend de la localisation de l'appareil) et avec la macro **%CARD%** les dossiers stockés sur toutes les cartes mémoire accessibles sur l'appareil.

L'application tournant sous SE Symbian chiffre avec la macro **%DOCS%** le dossier **C:\Data** et avec la macro **%CARD%** les dossiers stockés sur toutes les cartes mémoire accessibles sur l'appareil.

Par défaut, la liste des dossiers pour le chiffrement est vide.

CONFIGURATION DES PARAMETRES DU COMPOSANT ANTI-SPAM

Pour configurer les paramètres du composant Anti-Spam, procédez comme suit :

1. Ouvrez l'onglet **Avancé** (cf. ill. ci-après).

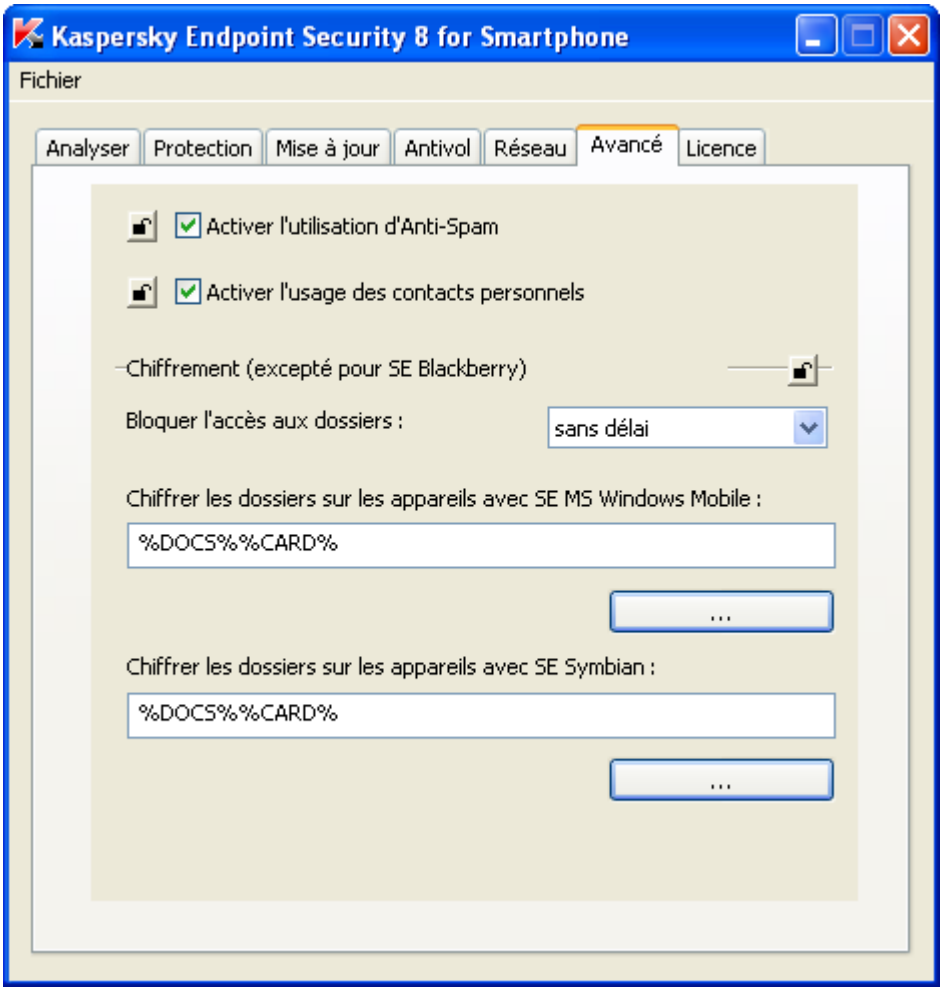


*Figure 81: Onglet **Avancé***

2. Autorisez / interdisez l'utilisation de l'Antide l'Anti-Spam et la modification de ses paramètres sur l'appareil. Pour ce faire, cochez / décochez la case **Activer l'utilisation de l'Antide l'Anti-Spam**.

   Si l'utilisation de l'Antide l'Anti-Spam est autorisée, tous les paramètres du composant peuvent être configurés par l'utilisateur sur l'appareil. Si l'utilisation de l'Antide l'Anti-Spam est interdite, l'accès au composant sur l'appareil est bloqué.

   Par défaut, l'utilisation de l'Antide l'Anti-Spam et la modification de ses paramètres sur l'appareil sont autorisées.

CONFIGURATION DES PARAMETRES DU COMPOSANT CONTACTS PERSONNELS

Pour configurer les paramètres du composant Contacts personnels, procédez comme suit :

1. Ouvrez l'onglet **Avancé** (cf. ill. ci-après).

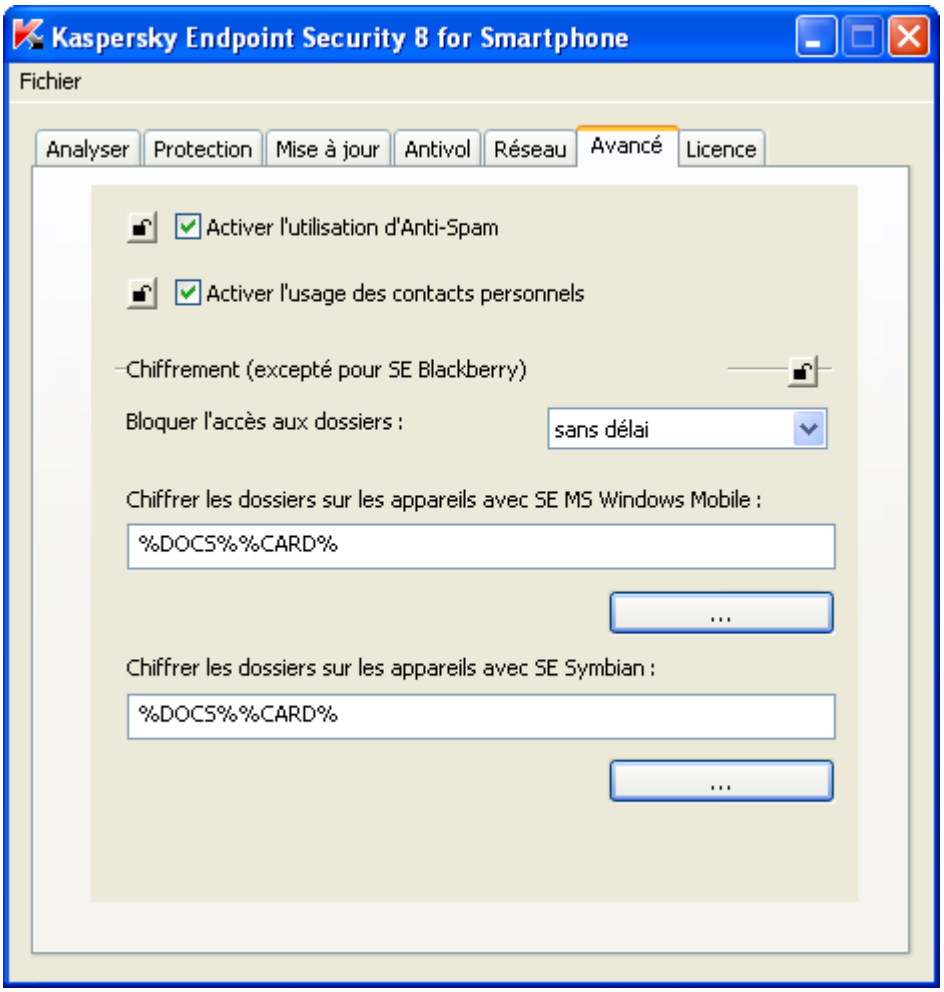


*Figure 82: Onglet **Avancé***

2. Autorisez / interdisez l'utilisation des Contacts personnels et la modification des paramètres du composant sur l'appareil. Pour ce faire, cochez / décochez la case **Activer l'utilisation des contacts personnels**.

   Si l'utilisation des Contacts personnels est autorisée, tous les paramètres du composant peuvent être configurés par l'utilisateur sur l'appareil. Si l'utilisation des Contacts personnels est interdite, l'accès au composant sur l'appareil est bloqué.

   Par défaut, l'utilisation des Contacts personnels et la modification de leurs paramètres sur l'appareil sont autorisées.

CONFIGURATION DES PARAMETRES DE LA LICENCE

Pour ajouter la licence à la stratégie, procédez comme suit :

1. Ouvrez l'onglet **Licence** (cf. ill. ci-après).

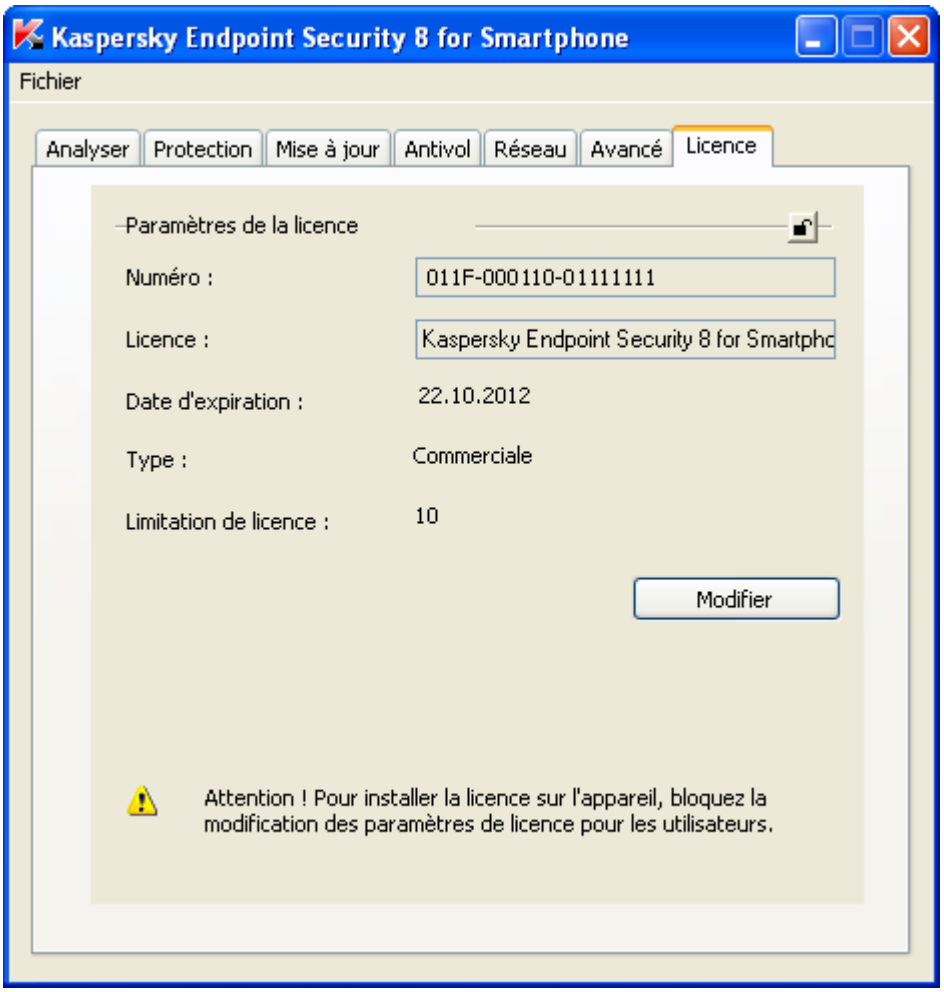


*Figure 83: Onglet **Licence***

2. Cliquez sur **Modifier** et sélectionnez dans la fenêtre qui s'ouvre le fichier de licence obtenu lors de l'achat de l'application.

   Une fois le fichier de licence téléchargé, les informations sur la licence s'affichent sous l'onglet.

3. Enregistrez le fichier de stratégie.

AJOUT DE LA LICENCE VIA SYBASE AFARIA

Pour installer la licence sur les appareils mobiles, l'administrateur doit créer une stratégie de Kaspersky Endpoint Security 8 for Smartphone et ajouter la licence à cette stratégie (cf. la rubrique "Configuration des paramètres de la licence" à la page 135). Ensuite, l'administrateur doit assurer le transport de la stratégie créée vers les appareils du profil sélectionné (cf. la rubrique "Installation de l'application" à la page 137). Pendant la synchronisation suivante des appareils mobiles avec Sybase Afaria, la stratégie de l'application avec sa licence sera transmise et appliquée sur les appareils pour activer l'application.

Si la licence n'est pas installée sur les appareils, l'application reste opérationnelle pendant trois jours qui suivent l'installation de l'application sur les appareils.

Si la licence n'a pas été installée pendant trois jours, les fonctionnalités de l'application seront limitées.

Si vous n'avez pas acheté la licence avant d'installer l'application, vous pouvez l'ajouter à la stratégie à tout moment.

Par défaut, la licence n'est pas ajoutée à la stratégie.

MODIFICATION DE LA STRATEGIE

- *Pour modifier les paramètres de l'application dans la stratégie existante de Kaspersky Endpoint Security 8 for Smartphone, procédez comme suit :*

  1. Lancez l'utilitaire **KES2Afaria.exe**.

     La fenêtre **Kaspersky Endpoint Security 8 for Smartphone** est affichée avec plusieurs onglets.

  2. Sélectionnez dans le menu **Fichier →Ouvrir** et spécifiez le fichier de stratégie dont les paramètres de l'application doivent être modifiés.

  3. Effectuez des modifications nécessaires et enregistrez le fichier de stratégie reçu en sélectionnant dans le menu **Fichier →Enregistrer**.

INSTALLATION DE L'APPLICATION

Sybase Afaria permet d'installer à distance Kaspersky Endpoint Security 8 for Smartphone sur les appareils mobiles.

Pour installer l'application sur les appareils, l'administrateur assure le transport vers les appareils mobiles des canaux avec des fichiers de stratégie et la distribution de l'application pour tous les types d'appareils.

L'administrateur doit assurer une exécution des canaux sur les appareils en suivant strictement la séquence : il faut d'abord transmettre le fichier de stratégie sur l'appareil et ensuite la distribution de l'application. Si la séquence d'exécution des canaux sur l'appareil n'est pas respectée, l'application ne sera pas opérationnelle.

Pour installer l'application sur les appareils tournants sous SE Microsoft Windows Mobile et Symbian, l'administrateur doit procéder comme suit :

1. Créer le canal Software Manager Channel avec le fichier de stratégie de l'application (cf. la rubrique "Création du canal avec la stratégie de l'application pour les appareils tournants sous SE Microsoft Windows Mobile et Symbian" à la page 138).
2. Créer le canal Software Manager Channel avec la distribution de l'application (cf. la rubrique "Création du canal avec la distribution de l'application pour les appareils tournants sous SE Microsoft Windows Mobile et Symbian" à la page 139).
3. Fusionner les canaux (channel set) (cf. la rubrique "Fusion des canaux pour installer l'application sur les appareils tournants sous SE Microsoft Windows Mobile et Symbian" à la page 140).
4. Publier les canaux / canaux fusionnés (publish).
5. Transporter les canaux vers les appareils avec le moniteur.

Pour installer l'application sur les appareils tournants sous SE BlackBerry, l'administrateur doit procéder comme suit :

1. Créer le canal Session Manager Channel (cf. la rubrique "Création du canal pour les appareils tournants sous SE BlackBerry" à la page 140).
2. Créer une liste des tâches (worklist) qui va guider l'installation de l'application.
3. Publier le canal.
4. Transmettre le canal vers les appareils avec le moniteur.

Pendant la synchronisation suivante des appareils mobiles avec le serveur Sybase Afaria l'application sera installée automatiquement et la stratégie configurée sera appliquée.

Une fois l'application installée, vous pourrez modifier les paramètres de l'application à l'aide des stratégies. Pour ce faire, il faut actualiser le fichier de stratégie sur le serveur. Pendant la synchronisation suivante, le fichier de stratégie sera actualisé sur les appareils et les paramètres modifiés seront appliqués.

Ainsi, l'installation de l'application pour les systèmes d'exploitation Microsoft Windows Mobile et Symbian comprend les étapes suivantes :

- Création du canal Software Manager Channel avec la distribution de l'application (cf. la rubrique "Création du canal avec la distribution de l'application pour les appareils tournants sous SE Microsoft Windows Mobile et Symbian " à la page 139).
- Création du canal Software Manager Channel avec la stratégie de l'application (cf. la rubrique "Création du canal avec la stratégie de l'application pour les appareils tournants sous SE Microsoft Windows Mobile et Symbian" à la page 138).
- Fusion des canaux avec la stratégie et la distribution de l'application (channel set) (cf. la rubrique "Fusion des canaux pour installer l'application sur les appareils tournants sous SE Microsoft Windows Mobile et Symbian" à la page 140).
- Publication des canaux (Publishing).
- Transmission des canaux vers les appareils avec le moniteur (monitor).

L'installation de l'application sous BlackBerry contient les étapes suivantes :

- Création du canal Session Manager Channel avec la liste des tâches pour guider l'installation de l'application (cf. la rubrique "Création du canal pour les appareils tournants sous SE BlackBerry" à la page 140).
- Publication du canal (Publishing).
- Transmission du canal vers les appareils avec le moniteur (monitor).

DANS CETTE SECTION

CREATION DU CANAL AVEC LA STRATEGIE DE L'APPLICATION POUR LES APPAREILS TOURNANTS SOUS SE MICROSOFT WINDOWS MOBILE ET SYMBIAN

Pour appliquer la stratégie de Kaspersky Endpoint Security 8 for Smartphone le canal Software Manager Channel est utilisé sur les appareils.

Lorsque le canal sera transmis sur les appareils, le fichier de stratégie policy.kes sera envoyé et installé dans le dossier créé par l'administrateur.

Si le fichier est actualisé par la suite sur le serveur, pendant la synchronisation suivante il sera actualisé sur l'appareil et les modifications des paramètres seront appliquées automatiquement.

Avant de créer le canal, assurez-vous que le fichier de stratégie est enregistré sur le serveur.

Pour créer le canal avec la stratégie de Kaspersky Endpoint Security 8 for Smartphone, procédez comme suit :

1. Sélectionnez dans le menu **Administration** l'option **Policies and Profiles**.
2. Sélectionnez le profil requis dans la barre **Policies and Profiles** du dossier **Group Profiles**.
3. Pour le profil sélectionné sous l'onglet **Allowed channels**, cliquez sur le lien **Create →Software Manager Channel**.

   La fenêtre **Software Manager Channel Wizard** s'affiche.

4. Saisissez le nom et la description du nouveau canal.
5. Sélectionnez les types d'appareils dans la liste **Select one or more Client Types** et cliquez sur **Next**.
6. Sélectionnez le dossier sur le serveur et cliquez sur **Next**.
7. Sélectionnez le fichier de stratégie policy.kes. Pour ce faire, cliquez sur le lien **Add**.
8. Dans la fenêtre qui s'affiche, sélectionnez le chemin au fichier de stratégie sur le serveur.
9. Dans la liste déroulante du groupe **Destination directory for selected files**, sélectionnez **Let administrator specify destination**.
10. Dans le champ **Administrator specified destination folder**, spécifiez le dossier de l'appareil pour copier le fichier de stratégie sélectionné.

    Pour les appareils tournants sous SE Microsoft Windows Mobile, sélectionnez le dossier **\Temp**.

    Pour les appareils tournants sous SE Symbian, sélectionnez le dossier **C:\Data**.
11. Sélectionnez dans le groupe **Check file options** l'option **Always check file**.
12. Assurez-vous que l'option sélectionnée dans le groupe **Send file options** est **Send file when server file is newer** et cliquez sur **OK**. Après avoir sélectionné la stratégie dans la fenêtre **Software Manager Channel Wizard**, cliquez sur **Next**.
13. Cliquez sur **Finish**.

    Le canal est créé.

CREATION DU CANAL AVEC LA DISTRIBUTION DE L'APPLICATION POUR LES APPAREILS TOURNANTS SOUS SE MICROSOFT WINDOWS MOBILE ET SYMBIAN

Pour installer l'application sur les appareils tournants sous SE Microsoft Windows Mobile et Symbian, le canal Software Manager Channel est utilisé. Le canal est appliqué au profil sélectionné pour les appareils.

Le canal est utilisé pour copier la distribution dans le dossier spécifié sur l'appareil et pour lancer automatiquement l'installation de l'application.

Si la fonction du lancement automatique d'installation est activée dans le canal, il ne faut pas y ajouter le fichier de stratégie. Pour appliquer la stratégie, il faut utiliser le canal spécifique Software Manager Channel. Cela exclut une nouvelle installation de l'application lors de la mise à jour de la stratégie sur les appareils. Sinon, une fois le fichier sur le serveur est actualisé, pendant la synchronisation des appareils mobiles avec le serveur Sybase Afaria leur fichier de stratégie sera actualisé et une nouvelle installation de l'application sera exécutée.

Avant de créer le canal, enregistrez les fichiers d'installation pour les systèmes d'exploitation Microsoft Windows Mobile / Symbian sur le serveur. Les fichiers d'installation font partie de la distribution de Kaspersky Endpoint Security 8 for Smartphone.

Pour créer un canal afin d'installer l'application sur les appareils tournants sous SE Microsoft Windows Mobile / Symbian, procédez comme suit :

1. Sélectionnez dans le menu **Administration** l'option **Policies and Profiles**.
2. Sélectionnez le profil requis dans la barre **Policies and Profiles** du dossier **Group Profiles**.
3. Pour le profil sélectionné sous l'onglet **Allowed channels**, cliquez sur **Create →Software Manager Channel**.

   La fenêtre **Software Manager Channel Wizard** s'affiche.
4. Saisissez le nom et la description du nouveau canal.
5. Sélectionnez les types d'appareils dans la liste **Select one or more Client Types** et cliquez sur **Next**.
6. Sélectionnez le dossier sur le serveur et cliquez sur **Next**.
7. Sélectionnez la distribution de l'application à transmettre sur les appareils. Pour ce faire, cliquez sur **Add** et spécifiez dans la fenêtre qui s'affiche le chemin au fichier d'installation de l'application.

   Pour les appareils tournants sous SE Microsoft Windows Mobile, sélectionnez l'archive CAB obtenue lors de l'achat de l'application.

Pour les appareils tournants sous SE Symbian, sélectionnez l'archive SISX obtenue lors de l'achat de l'application.

Après avoir sélectionné la distribution de l'application à transmettre sur les appareils, cliquez sur **Next**.

8. Spécifiez le dossier pour copier le fichier sélectionné et cliquez sur **Next**.

   Pour les appareils tournants sous SE Microsoft Windows Mobile, sélectionnez le dossier **\Temp**.

   Pour les appareils tournants sous SE Symbian, sélectionnez le dossier **C:\Data**.

9. Cochez la case **Continue editing** pour continuer à modifier les paramètres du canal et cliquez sur **Finish**.

   La fenêtre **Software Manager Channel Editor: <nom_du_canal>** s'affiche.

10. Sélectionnez l'installation automatique de l'application après la transmission de la distribution sur l'appareil. Pour ce faire, cochez sous l'onglet **Install** du groupe **Installation program** la case **Start installation automatically**.

    Si vous avez activé l'installation automatique de l'application, créez un canal spécifique pour transmettre le fichier de stratégie. Cela exclut une nouvelle installation de l'application lors de la mise à jour du fichier de stratégie sur les appareils.

11. Sélectionnez dans la liste déroulante **File name** la distribution de l'application, puis cliquez sur **OK**.

FUSION DES CANAUX POUR INSTALLER L'APPLICATION SUR LES APPAREILS TOURNANTS SOUS SE MICROSOFT WINDOWS MOBILE ET SYMBIAN

L'administrateur doit assurer une exécution des canaux sur l'appareil en suivant strictement la séquence : il faut d'abord transmettre le fichier de stratégie de l'application sur l'appareil et ensuite transmettre la distribution de l'application. Cela permet de transmettre d'abord les stratégies de l'application pendant l'exécution des canaux sur les appareils mobiles et de lancer ensuite l'installation de l'application en appliquant immédiatement les paramètres configurés de l'application. Si la séquence d'exécution des canaux sur l'appareil n'est pas respectée, l'application ne sera pas opérationnelle.

Pour rendre l'administration des canaux avec la stratégie et la distribution de l'application plus confortable, il est conseillé de les fusionner.

Pour fusionner les canaux, procédez comme suit :

1. Sélectionnez dans le menu **Administration** l'option **Policies and Profiles**.
2. Sélectionnez le profil requis dans la barre **Policies and Profiles** du dossier **Group Profiles**.
3. Pour le profil sélectionné sous l'onglet **Allowed channels**, cliquez sur **Create** →**Channel Set**.

   La fenêtre **Channel Set Wizard** s'affiche.
4. Saisissez le nom et la description des canaux fusionnés.
5. Sélectionnez le dossier sur le serveur et cliquez sur **Next**.
6. Sélectionnez dans la liste les chaînes à fusionner et cliquez sur **Next**.
7. Spécifiez la séquence de l'exécution des canaux et cliquez sur **Finish**.

CREATION DU CANAL POUR LES APPAREILS TOURNANTS SOUS BLACKBERRY

Pour installer Kaspersky Endpoint Security 8 for Smartphone sur les appareils tournant sous SE BlackBerry, utilisez le canal **Session Manager Channel**. Il faut y créer une liste des tâches (worklist) qui va guider l'installation de l'application sur les appareils.

Avant de créer la liste des tâches, enregistrez le fichier Endpoint8_Mobile_Installer.cod pour BlackBerry sur le serveur. Ce fichier fait partie de la distribution Kaspersky Endpoint Security 8 for Smartphone.

Pour installer l'application sur les appareils tournants sous SE BlackBerry, procédez comme suit :

1. Sélectionnez dans le menu **Administration** →**Policies and Profiles**.

2. Sélectionnez le profil requis dans la barre **Policies and Profiles** du dossier **Group Profiles**.
3. Pour le profil sélectionné sous l'onglet **Allowed channels**, cliquez sur le lien **Create →Session Manager Channel**.

   La fenêtre **Software Manager Channel Wizard** s'affiche.
4. Saisissez le nom et la description du canal dans les champs **Name**, **Description**.
5. Sélectionnez dans la liste **Select one or more types BlackBerry Clients**. Cliquez sur **Next**.
6. Sélectionnez le dossier sur le serveur et cliquez sur **Finish**.

   Le canal est créé. La fenêtre **Session Manager Channel Editor** s'affiche.
7. Cliquez sur **Create worklist**. Saisissez dans la fenêtre qui s'affiche le nom de la nouvelle liste des tâches (worklist).
8. Créez pour la nouvelle liste des tâches (worklist) la liste d'événements (eventlist) suivante :

```
Send <chemin au fichier de stratégie>\policy.kes TO policy.kes
Client Find File ksgui
If Previous Event FALSE
   Send <chemin à la distribution de l'application>\Endpoint8_Mobile_Installer.cod TO
   Endpoint8_Mobile_Installer.cod
End if
```

L'exécution de ce script permet de transmettre sur les appareils le fichier des stratégies policy.kes et de l'appliquer. Ensuite, le script vérifie si l'application a été installée sur l'appareil. Si l'application a été installée sur l'appareil, le script est terminé. Si l'application n'a pas été installée, les appareils reçoivent le fichier Endpoint8_Mobile_Installer.cod qui télécharge les fichiers d'installation de l'application depuis les serveurs de Kaspersky Lab et lance automatiquement l'installation de l'application. Le script est terminé.

1. Enregistrez la liste d'évènement (eventlist) en cliquant sur **Save**.
2. Publiez le canal (publish).

Pour créer la liste d'événements, procédez comme suit :

1. Dans la fenêtre **Session Manager Channel** (dans la partie droite de la fenêtre), sélectionnez dans la liste d'événements **Send file to Client**.
2. Dans la fenêtre **Event details: Send File to Client** qui s'affiche, spécifiez dans le champ **Source file** le fichier de stratégie policy.kes pour transmettre sur les appareils. Pour ce faire, cliquez sur le lien **Browse** et spécifiez le chemin au fichier de stratégie policy.kes sur le serveur.

   Le champ **Target file** sera rempli automatiquement.
3. Dans le groupe **File comparison and transfer options**, sélectionnez dans la liste déroulante **Transfer** l'option **Always**. Assurez-vous que la case **Use safe transfer** est cochée.
4. Assurez-vous que dans le groupe **Options** les cases **Make target path**, **Ignore hidden files** sont cochées.
5. Assurez vous que dans le groupe **Status** la valeur sélectionnée est **Enable** et cliquez sur **OK**.
6. Sélectionnez dans la barre de la partie droite de la fenêtre **Session Manager Channel** l'option **Find File**.
7. Dans la fenêtre **Event details:Find File** qui s'affiche, saisissez dans le champ **Starting path** la valeur **ksgui**. Cela permet de vérifier si l'application Kaspersky Endpoint Security 8 for Smartphone a été déjà installée sur les appareils.
8. Assurez-vous que dans le groupe **Options** les cases **Ignore hidden options**, **Include subdirectories** sont cochées.
9. Assurez-vous que dans le groupe **Execute** la valeur sélectionnée est **On Client**.
10. Assurez vous que dans le groupe **Status** la valeur sélectionnée est **Enable** et cliquez sur **OK**.
11. Sélectionnez dans la barre de la partie droite de la fenêtre **Session Manager Channel** l'option **If**.
12. Dans la fenêtre **Event details: If** squi s'affiche, sélectionnez la valeur **Previous event FALSE** et cliquez sur **OK**.
13. Sélectionnez dans la barre de la partie droite de la fenêtre **Session Manager Channel** l'option **Send file to Client**.
14. Indiquez dans le champ **Source file** le fichier Endpoint8_Mobile_Installer.cod. Pour ce faire, utilisez le lien **Browse** et spécifiez le chemin au fichier sur le serveur. Le champ **Target file** sera rempli automatiquement.

15. Dans le groupe **File comparison and transfer options**, sélectionnez dans la liste déroulante **Transfer** l'option **Always**. Assurez-vous que la case **Use safe transfer** est cochée.
16. Assurez-vous que dans le groupe **Options** les cases **Make target path**, **Ignore hidden files** sont cochées.
17. Assurez vous que dans le groupe **Status** la valeur sélectionnée est **Enable** et cliquez sur **OK**.
18. Sélectionnez dans la barre de la partie droite de la fenêtre **Session Manager Channel** l'option **End if**.
19. Enregistrez la liste d'événement créée en cliquant sur **Save**.

INSTALLATION DE L'APPLICATION SUR LES APPAREILS MOBILES

L'installation de l'application sur les appareils mobiles est effectuée à distance.

Pendant la synchronisation des appareils mobiles avec le serveur Sybase Afaria est transmis le canal / les canaux fusionnés avec le fichier de stratégie et la distribution de l'application. Ensuite, le fichier de stratégie est copié dans le dossier indiqué par l'administrateur sur l'appareil et l'installation de l'application est lancée automatiquement.

S'il s'agit de Microsoft Windows Mobile ou BlackBerry, l'utilisateur n'a pas besoin d'intervenir pendant l'installation de l'application.

S'il s'agit de Symbian, l'utilisateur doit intervenir pendant l'installation de l'application. Pour en savoir plus, consultez le Guide de l'utilisateur pour Symbian.

Une fois l'installation terminée, la stratégie configurée par l'administrateur sera appliquée automatiquement. Si l'administrateur a ajouté la licence à la stratégie (cf. la rubrique "Ajout de la licence via Sybase Afaria" à la page 136), la licence sera installée automatiquement et l'application sera activée après l'application de la stratégie.

Si l'administrateur n'a pas ajouté la licence à la stratégie, l'application reste opérationnelle pendant trois jours. Si pendant cette période l'administrateur n'a pas ajouté la licence à la stratégie, les fonctionnalités de l'application installée sur les appareils seront limitées.

À la première exécution de l'application, l'utilisateur devra saisir le code secret. L'utilisateur peut modifier uniquement les paramètres de l'appareil qui ne sont pas interdits à la modification par l'administrateur dans la stratégie.

La fréquence de synchronisation des appareils mobiles avec Sybase Afaria est définie dans le moniteur par l'administrateur. Pour mettre à jour les paramètres de l'application (cf. la rubrique "Création de la stratégie. Configuration des paramètres de Kaspersky Endpoint Security 8 for Smartphone" à la page 118) sur l'appareil, l'administrateur doit actualiser le fichier de la stratégie sur le serveur. Pendant la synchronisation suivante, le fichier de stratégie sera actualisé sur les appareils et les paramètres modifiés de l'application seront appliqués automatiquement.

SUPPRESSION DE L'APPLICATION

La suppression de l'application de l'appareil mobile est effectuée par l'utilisateur à la main.

Pour Microsoft Windows Mobile et Symbian avant la suppression de l'application, la dissimulation des informations confidentielles sur l'appareil sera désactivée automatiquement et les informations chiffrées seront déchiffrées en mode automatique. Pour BlackBerry avant la suppression de l'application, l'utilisateur doit manuellement désactiver la dissimulation des informations confidentielles.

Pour en savoir plus sur la procédure de suppression de l'application, consultez le Guide de l'utilisateur de Kaspersky Endpoint Security 8 for Smartphone.

CONTACTER LE SERVICE DU SUPPORT TECHNIQUE

Si vous avez déjà acheté Kaspersky Endpoint Security, vous pouvez obtenir les informations sur l'application auprès du Service d'assistance technique par téléphone ou par Internet.

Les experts du service d'assistance technique sont là pour répondre à vos questions sur l'installation et l'utilisation de l'application. En cas d'infection de l'ordinateur, ils vous aideront à éliminer les conséquences des actions des programmes malveillants.

Avant de prendre contact avec le Service d'assistance technique, prenez connaissance des Règles de support (http://support.kaspersky.com/support/rules).

Formulaire de soumission de demande du Support Technique

Vous pouvez poser vos questions aux experts du Support Technique en remplissant le formulaire en ligne du Helpdesk (http://support.kaspersky.ru/helpdesk.html?LANG=fr).

Les messages peuvent être envoyés en russe, en anglais, en allemand, en français ou en espagnol.

Pour traiter votre demande par messagerie, indiquez le reçu en même temps que votre **numéro de client** et **mot de passe** reçus lors de votre enregistrement sur le site du Service d'assistance technique.

Si vous n'êtes pas encore inscrit en tant qu'utilisateur des applications de Kaspersky Lab, remplissez le formulaire (https://support.kaspersky.com/ru/personalcabinet/registration/form/). Lors de l'enregistrement, indiquez *le code d'activation* de l'application ou *le nom du fichier de licence*.

L'opérateur du service du Support Technique vous enverra sa réponse dans votre Espace personnel (https://support.kaspersky.com/ru/personalcabinet?LANG=fr) ainsi qu'à l'adresse électronique que vous avez indiquée dans votre demande.

Dans le formulaire en ligne de demande, décrivez le problème rencontré avec le plus de détails possible. Dans les champs obligatoires, indiquez :

- **Type de la demande**. Sélectionnez l'objet qui correspond le mieux au problème (" Problème lors de l'installation/la suppression du produit " ou " Problème de recherche/suppression de virus ". Si vous ne trouvez pas le sujet qui vous concerne, sélectionnez "Question générale".
- **Nom et version de l'application**.
- **Texte de la demande**. Décrivez le problème rencontré avec le plus de détails possible.
- **Numéro de client et mot de passe**. Saisissez le numéro de client et le mot de passe que vous avez reçu lors de l'enregistrement sur le site Web du service du Support Technique.
- **Adresse électronique**. Les experts du service du Support Technique vous enverront la réponse à votre question.

Support Technique par téléphone

En cas de problème urgent, vous pouvez toujours contacter le service d'assistance technique par téléphone dans votre ville. Avant de contacter les experts du service d'assistance technique, rassemblez les informations (http://support.kaspersky.ru/support/details) relatives à votre ordinateur. Ces informations réduiront le temps de réponse de nos spécialistes.

GLOSSAIRE

A

ACTIVATION DU LOGICIEL

Passage de l'application en mode pleinement opérationnel. L'application ne peut être activée qu'avec une licence installée.

ANALYSE A LA DEMANDE

Mode de fonctionnement du programme Kaspersky Lab exécuté à la demande de l'utilisateur et conçu pour analyser et vérifier tous les fichiers résidents.

ARCHIVE

Fichier "conteneur" d'un ou plusieurs autres objets pouvant être eux-mêmes des archives.

B

BASES ANTIVIRUS

Bases de données maintenues par les experts de Kaspersky Lab contenant des descriptions détaillées de toutes les menaces de sécurité informatique existantes, ainsi que les méthodes permettant de les détecter et de les neutraliser. La base de données est constamment mise à jour par Kaspersky Lab chaque fois qu'une nouvelle menace apparaît.

BLOCAGE D'UN OBJET

Interdire l'accès à un objet par des programmes externes. Un objet interdit ne peut pas être lu, exécuté, modifié ni supprimé.

C

CODE SECRET DE L'APPLICATION

Le code secret de l'application permet d'éviter l'accès non autorisé aux paramètres de l'application et aux données protégées de l'appareil. Il est saisi par l'utilisateur à la première exécution de l'application et compte au moins quatre chiffres. Il faut saisir le code secret de l'application dans les cas suivants :

- Pour accéder aux paramètres de l'application ;
- Pour accéder aux dossiers cryptés ;
- Pour envoyer une instruction SMS depuis un autre appareil mobile afin d'activer à distance les fonctions suivantes : Verrouillage, Suppression, SIM-Surveillance, Géolocalisation, Contacts personnels ;
- Pour supprimer l'application.

D

DUREE DE VALIDITE DE LA LICENCE

Période durant laquelle vous pouvez utiliser l'ensemble des fonctions de l'application de Kaspersky Lab. A l'expiration de la licence, les fonctionnalités de l'application seront limitées. Dans ce mode sont accessibles les fonctions suivantes :

- désactiver tous les composants ;
- déchiffrer un ou plusieurs dossiers ;
- désactiver de la dissimulation des informations confidentielles ;
- désactiver la dissimulation automatique des informations confidentielles ;
- consulter le système d'aide.

DESINFECTION OU REPARATION D'OBJETS

Méthode de traitement d'objets infectés permettant la récupération complète ou partielle des données, ou la prise d'une décision si l'objet ne peut être réparé. La réparation d'objets fait appel au contenu des bases de données. La réparation peut entraîner la perte d'une partie des données.

L

LISTE BLANCHE

Les entrées de cette liste contiennent les informations suivantes :

- Numéro de téléphone dont les appels et/ou les SMS sont acceptés par Anti-Spam.
- Type d'événement en provenance de ce numéro que l'Antique l'Anti-Spam accepte. Types d'événements représentés : appels et SMS, appels seuls, SMS seuls.
- Expression clé qui permet à Anti-Spam d'identifier des SMS sollicités (qui ne sont pas du spam). Anti-Spam accepte uniquement les SMS avec l'expression clé et refuse tous les autres SMS.

LISTE NOIRE

Les entrées de cette liste contiennent les informations suivantes :

- Numéro de téléphone dont les appels et/ou les SMS sont bloqués par Anti-Spam.
- Type d'événement en provenance de ce numéro que l'Antique l'Anti-Spam bloque. Types d'événements représentés : appels et SMS, appels seuls, SMS seuls.
- Expression clé qui permet à Anti-Spam d'identifier des SMS non sollicités (spam). Anti-Spam accepte uniquement les SMS avec l'expression clé et refuse tous les autres SMS.

M

MISE A JOUR DES BASES

Une des fonctions de l'application de Kaspersky Lab qui permet de maintenir la protection à jour. Elle copie les bases antivirus depuis les serveurs de mises à jour de Kaspersky Lab sur l'appareil en les intégrant à l'application en mode automatique.

O

OBJET INFECTE.

Objet contenant du code malveillant : sa détection au cours de l'analyse est possible car une section du code de l'objet est identique à la section de code d'une menace déjà connue. Les experts de Kaspersky Lab ne recommandent pas d'utiliser des objets de ce type, qui peuvent causer l'infection de l'appareil.

P

PAQUET D'INSTALLATION

Sélection de fichiers pour installer à distance de l'application de Kaspersky Lab à l'aide du système d'administration distante. Le paquet d'installation est créé sur la base de fichiers spéciaux qui font partie de la distribution de l'application, et contient un ensemble de paramètres nécessaires pour installer l'application et assurer son fonctionnement immédiatement après l'installation. Les valeurs des paramètres correspondent aux valeurs des paramètres de l'application par défaut.

PLUG-IN D'ADMINISTRATION DE L'APPLICATION

Composant spécial, qui fait office d'interface pour l'administration du fonctionnement de l'application par la Console d'administration. Le plug-in d'administration est spécifique à chaque application. Il est repris dans toutes les applications de Kaspersky Lab qui peuvent être administrées à l'aide de Kaspersky Endpoint Security.

POSTE DE TRAVAIL DE L'ADMINISTRATEUR

Ordinateur sur lequel est installé le composant qui fait office d'interface pour l'administration de l'application.

Depuis le poste de travail de l'administrateur, il est possible de configurer et de gérer l'application, et, s'il s'agit de Kaspersky Administration Kit, de créer et de gérer un système de protection antivirus centralisée du réseau de la société sur la base des applications de Kaspersky Lab.

PROTECTION

Mode de fonctionnement du programme dans lequel les objets sont analysés à la recherche de code malveillant en temps réel.

Le programme intercepte toutes les tentatives d'accès à n'importe quel objet en lecture, en écriture ou en exécution, et analyse la présence de menaces dans l'objet. Les objets non infectés sont délivrés à l'utilisateur ; les objets contenant des menaces ou suspects d'en contenir, sont traités conformément à la configuration des tâches (désinfection, suppression, quarantaine, etc.).

Q

QUARANTAINE

Dossier spécial dans lequel sont placés tous les objets probablement infectés, détectés pendant l'analyse de l' appareil ou par la protection en temps réel.

S

SERVEURS DE MISES A JOUR DE KASPERSKY LAB.

Liste des serveurs HTTP et FTP de Kaspersky Lab que l'application utilise pour copier la mise à jour des bases sur les appareils mobiles.

STRATEGIE

Ensemble des paramètres de fonctionnement de l'application pour un groupe cible des appareils. Les paramètres de fonctionnement de l'application peuvent varier en fonction des groupes. La stratégie contient les paramètres de la configuration complète de toutes les fonctions de l'application.

STRATEGIE DE GROUPE

voir Stratégie

SUPPRESSION SMS

Méthode de traitement d'un SMS contenant des caractéristiques indésirables (SPAM) impliquant sa suppression physique. Nous recommandons cette méthode pour des messages SMS clairement indésirables.

SUPPRESSION D'UN OBJET

Procédé de traitement d'un objet, impliquant sa suppression physique de l'emplacement où il a été détecté par le programme (disque fixe, dossier, ressource réseau). Nous recommandons d'appliquer ce traitement aux objets dangereux qui ne peuvent être, pour une raison quelconque, réparés.

SYNCHRONISATION

Un processus d'établissement de la connexion entre l'appareil mobile et le système d'administration distante suivi de la transmission des données. Lors de la synchronisation, l'appareil reçois les paramètres de l'application, installés par l'administrateur. L'appareil envoie dans le système d'administration distante les rapports sur le fonctionnement des composants de l'application.

SYSTEME D'ADMINISTRATION DISTANTE

Un système qui permet de contrôler les appareils à distance et de les administrer en temps réel.

KASPERSKY LAB

Kaspersky Lab a vu le jour en 1997. Il produit un large éventail de logiciels de sécurité des données, et distribue des solutions techniquement avancées et complètes afin de protéger les ordinateurs et les réseaux contre tous types de programmes malveillants, les courriers électroniques non sollicités ou indésirables, et contre les tentatives d'intrusion.

Kaspersky Lab est une société internationale. Son siège principal se trouve dans la Fédération Russe, et la société possède des délégations au Royaume Uni, en France, en Allemagne, au Japon, dans les pays du Benelux, en Chine, en Pologne, en Roumanie et aux Etats-Unis (Californie). Un nouveau service de la compagnie, le centre européen de recherches Anti-Virus, a été récemment installé en France. Le réseau de partenaires de Kaspersky Lab compte plus de 500 entreprises du monde entier.

Aujourd'hui, Kaspersky Lab emploie plus de 1000 spécialistes, tous spécialistes des technologies antivirus : 10 d'entre eux possèdent un M.B.A, 16 autres un doctorat. Les analystes seniors de Kaspersky Lab sont membres permanents de la CARO (Organisation pour la recherche antivirus en informatique).

Kaspersky Lab offre les meilleures solutions de sécurité, soutenues par une expérience unique et un savoir-faire accumulé pendant plus de 14 années de lutte contre les virus informatiques. Une analyse approfondie de l'activité virale informatique permet aux spécialistes de la société de détecter les tendances dans l'évolution du code malveillant et d'offrir à nos utilisateurs une protection permanente contre les nouveaux types d'attaques. La résistance à de futures attaques est la stratégie de base mise en œuvre dans toutes les applications Kaspersky Lab. Les produits de la société ont toujours fait preuve d'une longueur d'avance sur ceux de ses nombreux concurrents, pour assurer la plus grande des protections anti-virus aussi bien aux particuliers, qu'aux clients corporatifs.

Des années de dur travail ont fait de notre société l'un des premiers fabricants de logiciels antivirus. Kaspersky Lab fut l'une des premières entreprises à mettre au point les standards de défense antivirale les plus exigeants. Le produit vitrine de la société est Kaspersky Anti-Virus : il assure une protection complète de tous les systèmes informatiques contre les attaques de virus, comprenant les postes de travail, les serveurs de fichiers, les systèmes de messagerie, les pare-feu et passerelles Internet, ainsi que les ordinateurs portables. Les clients de Kaspersky Lab profitent d'un large éventail de services complémentaires qui leur assurent non seulement un bon fonctionnement des applications, mais également l'adaptation à certaines exigences spécifiques de leurs entreprises. De nombreux fabricants reconnus utilisent le noyau Kaspersky Anti-Virus : Nokia ICG (Etats-Unis), Aladdin (Israël), Sybari (Etats-Unis), G Data (Allemagne), Deerfield (Etats-Unis), Alt-N (Etats-Unis), Microworld (Inde) et BorderWare (Canada).

Les clients de Kaspersky Lab profitent d'un large éventail de services complémentaires qui leur assurent non seulement un bon fonctionnement des applications, mais également l'adaptation à certaines exigences spécifiques de leurs entreprises. Nous assurons l'étude, l'installation et la maintenance de suites antivirus de grandes organisations. La base anti-virus de Kaspersky Lab est mise à jour toutes les heures. Nous offrons à nos clients une assistance technique en plusieurs langues.

Si vous avez des questions, vous pouvez les adresser au revendeur ou directement à Kaspersky Lab. Vous bénéficierez toujours de consultations détaillées par téléphone ou courrier électronique. Vous recevrez des réponses complètes à vos questions.

Site Web de Kaspersky Lab :	http://www.kaspersky.com/fr
L'Encyclopédie des virus:	http://www.securelist.com/fr/
Laboratoire antivirus :	newvirus@kaspersky.com (envoi uniquement d'objets suspects sous forme d'archive) http://support.kaspersky.ru/virlab/helpdesk.html?LANG=fr (pour les questions aux experts antivirus)

INFORMATIONS SUR LE CODE TIERS

Le code développé par d'autres éditeurs a été utilisé pour créer l'application.

DANS CETTE SECTION

CODE DE PROGRAMMATION DIFFUSE

Le programme contient un code de programmation indépendant appartenant à d'autres éditeurs au format source ou binaire sans modification.

DANS CETTE SECTION

ADB

Copyright (C) 2005-2008, The Android Open Source Project

Distributed under the terms of the Apache License, version 2.0 of the License

ADBWINAPI.DLL

Copyright (C) 2005-2008, The Android Open Source Project

Distributed under the terms of the Apache License, version 2.0 of the License

ADBWINUSBAPI.DLL

Copyright (C) 2005-2008, The Android Open Source Project

Apache License

Version 2.0, January 2004

http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License. You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any

additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

AUTRES INFORMATIONS

La bibliothèque logicielle de protection des informations (BLPI) Crypto C, développée par CryptoEx intervient dans la formation et la vérification de la signature numérique dans Kaspersky Endpoint Security 8 for Smartphone.

Le site de CryptoEx : http://www.cryptoex.ru

INDEX

M

P

S