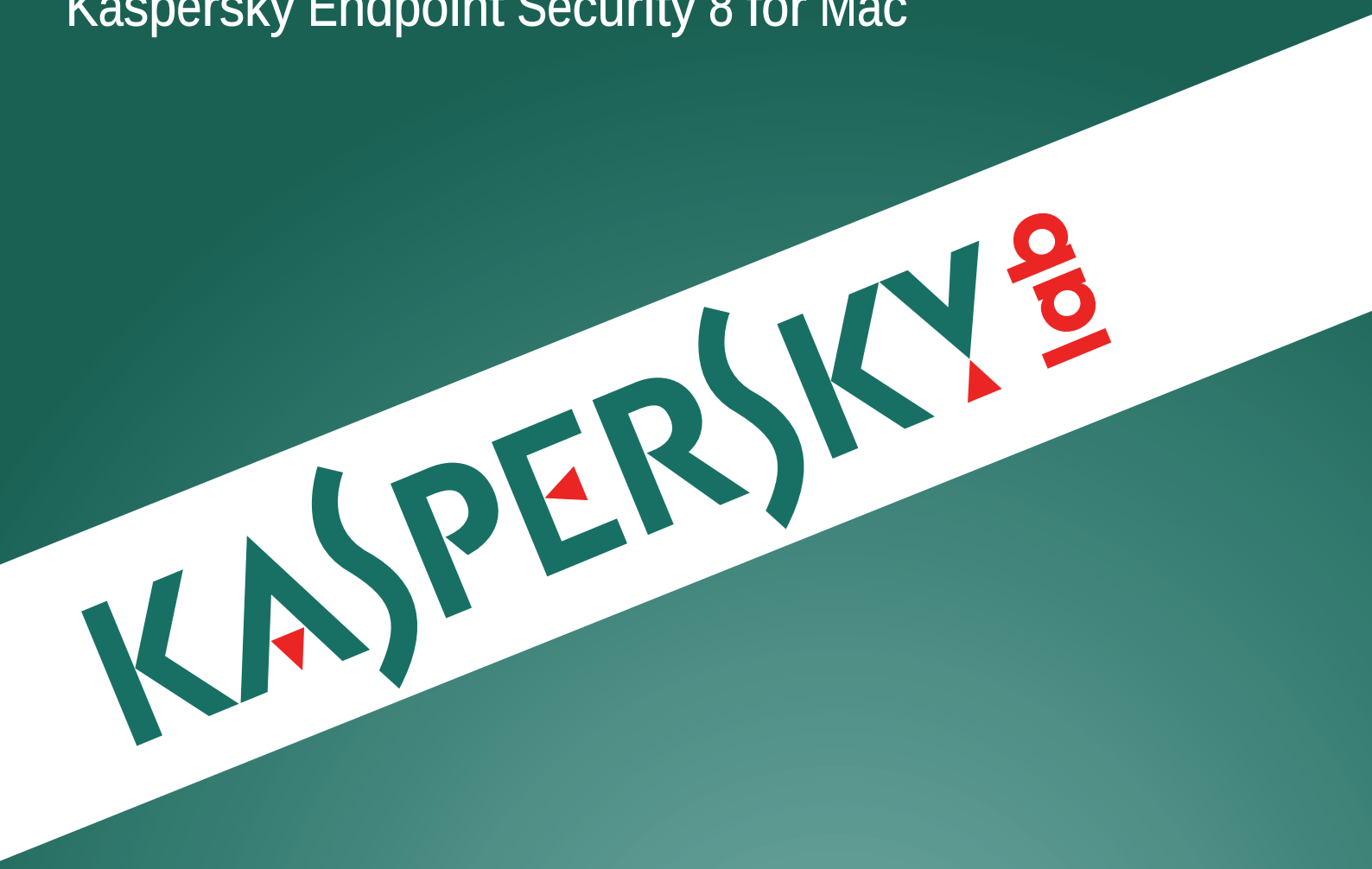
Kaspersky Endpoint Security 8 for Mac



Manuel d'administrateur

VERSION DE L'APPLICATION: 8.0 CRITICAL FIX 2

Cher utilisateur,

Nous vous remercions d'avoir choisi notre logiciel. Nous espérons que ce document vous sera utile et qu'il répondra à la majorité des questions apparaissant.

Ce document peut être modifié sans préavis. La version la plus récente du manuel est disponible sur le site de Kaspersky Lab, à l'adresse suivante : http://www.kaspersky.com/fr/docs.

Date d'édition : 24/12/2010

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

CONTRAT DE LICENCE D'UTILISATEUR FINAL DE KASPERSKY LAB

AVIS JURIDIQUE IMPORTANT À L'INTENTION DE TOUS LES UTILISATEURS : VEUILLEZ LIRE ATTENTIVEMENT LE CONTRAT SUIVANT AVANT DE COMMENCER À UTILISER LE LOGICIEL.

LORSQUE VOUS CLIQUEZ SUR LE BOUTON D'ACCEPTATION DE LA FENÊTRE DU CONTRAT DE LICENCE OU SAISISSEZ LE OU LES SYMBOLES CORRESPONDANTS, VOUS CONSENTEZ À ÊTRE LIÉ PAR LES CONDITIONS GÉNÉRALES DE CE CONTRAT. **CETTE ACTION EST UN SYMBOLE DE VOTRE SIGNATURE, ET VOUS CONSENTEZ PAR LÀ À VOUS SOUMETTRE AUX CONDITIONS DE CE CONTRAT ET À ÊTRE PARTIE DE CELUI-CI, ET CONVENEZ QUE CE CONTRAT A VALEUR EXÉCUTOIRE AU MÊME TITRE QUE TOUT CONTRAT ÉCRIT, NÉGOCIÉ SIGNÉ PAR VOS SOINS.** SI VOUS N'ACCEPTEZ PAS TOUTES LES CONDITIONS GÉNÉRALES DE CE CONTRAT, ANNULEZ L'INSTALLATION DU LOGICIEL ET NE L'INSTALLEZ PAS.

SI UN CONTRAT DE LICENCE OU UN DOCUMENT SIMILAIRE ACCOMPAGNE LE LOGICIEL, LES CONDITIONS D'UTILISATION DU LOGICIEL DÉFINIES DANS CE DOCUMENT PRÉVALENT SUR LE PRÉSENT CONTRAT DE LICENCE D'UTILISATEUR FINAL.

APRÈS AVOIR CLIQUÉ SUR LE BOUTON D'ACCEPTATION DANS LA FENÊTRE DU CONTRAT DE LICENCE OU AVOIR SAISI LE OU LES SYMBOLES CORRESPONDANTS, VOUS POUVEZ VOUS SERVIR DU LOGICIEL CONFORMÉMENT AUX CONDITIONS GÉNÉRALES DE CE CONTRAT.

1. Définitions

1.1. On entend par **Logiciel** le logiciel et toute mise à jour, ainsi que tous les documents associés.
1.2. On entend par **Titulaire des droits** (propriétaire de tous les droits exclusifs ou autres sur le Logiciel) Kaspersky Lab ZAO, une société de droit russe.
1.3. On entend par **Ordinateur(s)** le matériel, en particulier les ordinateurs personnels, les ordinateurs portables, les stations de travail, les assistants numériques personnels, les " téléphones intelligents ", les appareils portables, ou autres dispositifs électroniques pour lesquels le Logiciel a été conçu où le Logiciel sera installé et/ou utilisé.
1.4. On entend par **Utilisateur final (vous/votre)** la ou les personnes qui installent ou utilisent le Logiciel en son ou en leur nom ou qui utilisent légalement le Logiciel ; ou, si le Logiciel est téléchargé ou installé au nom d'une entité telle qu'un employeur, *" Vous "* signifie également l'entité pour laquelle le Logiciel est téléchargé ou installé, et il est déclaré par la présente que ladite entité a autorisé la personne acceptant ce contrat à cet effet en son nom. Aux fins des présentes, le terme *" entité ",* sans limitation, se rapporte, en particulier, à toute société en nom collectif, toute société à responsabilité limitée, toute société, toute association, toute société par actions, toute fiducie, toute société en coparticipation, toute organisation syndicale, toute organisation non constituée en personne morale, ou tout organisme public.
1.5. On entend par **Partenaire(s)** les entités, la ou les personnes qui distribuent le Logiciel conformément à un contrat et une licence concédée par le Titulaire des droits.
1.6. On entend par **Mise(s) à jour** toutes les mises à jour, les révisions, les programmes de correction, les améliorations, les patchs, les modifications, les copies, les ajouts ou les packs de maintenance, etc.
1.7. On entend par **Manuel de l'utilisateur** le manuel d'utilisation, le guide de l'administrateur, le livre de référence et les documents explicatifs ou autres.

2. Concession de la Licence

2.1. Une licence non exclusive d'archivage, de chargement, d'installation, d'exécution et d'affichage (" l'utilisation ") du Logiciel sur un nombre spécifié d'Ordinateurs vous est octroyée pour faciliter la protection de Votre Ordinateur sur lequel le Logiciel est installé contre les menaces décrites dans le cadre du Manuel de l'utilisateur, conformément à toutes les exigences techniques décrites dans le Manuel de l'utilisateur et aux conditions générales de ce Contrat (la " Licence "), et vous acceptez cette Licence :
Version de démonstration. Si vous avez reçu, téléchargé et/ou installé une version de démonstration du Logiciel et si l'on vous accorde par la présente une licence d'évaluation du Logiciel, vous ne pouvez utiliser ce Logiciel qu'à des fins d'évaluation et pendant la seule période d'évaluation correspondante, sauf indication contraire, à compter de la date d'installation initiale. Toute utilisation du Logiciel à d'autres fins ou au-delà de la période d'évaluation applicable est strictement interdite.

Logiciel à environnements multiples ; Logiciel à langues multiples ; Logiciel sur deux types de support ; copies multiples ; packs logiciels. Si vous utilisez différentes versions du Logiciel ou des éditions en différentes langues du Logiciel, si vous recevez le Logiciel sur plusieurs supports, ou si vous recevez plusieurs copies du Logiciel de quelque façon que ce soit, ou si vous recevez le Logiciel dans un pack logiciel, le nombre total de vos Ordinateurs sur lesquels toutes les versions du Logiciel sont autorisées à être installées doit correspondre au nombre d'ordinateurs précisé dans les licences que

vous avez obtenues, *sachant que,* sauf disposition contraire du contrat de licence, chaque licence acquise vous donne le droit d'installer et d'utiliser le Logiciel sur le nombre d'Ordinateurs stipulé dans les Clauses 2.2 et 2.3.

2.2. Si le Logiciel a été acquis sur un support physique, Vous avez le droit d'utiliser le Logiciel pour la protection du nombre d'ordinateurs stipulé sur l'emballage du Logiciel.
2.3. Si le Logiciel a été acquis sur Internet, Vous pouvez utiliser le Logiciel pour la protection du nombre d'Ordinateurs stipulé lors de l'acquisition de la Licence du Logiciel.
2.4. Vous ne pouvez faire une copie du Logiciel qu'à des fins de sauvegarde, et seulement pour remplacer l'exemplaire que vous avez acquis de manière légale si cette copie était perdue, détruite ou devenait inutilisable. Cette copie de sauvegarde ne peut pas être utilisée à d'autres fins et devra être détruite si vous perdez le droit d'utilisation du Logiciel ou à l'échéance de Votre licence ou à la résiliation de celle-ci pour quelque raison que ce soit, conformément à la législation en vigueur dans votre pays de résidence principale, ou dans le pays où Vous utilisez le Logiciel.
2.5. À compter du moment de l'activation du Logiciel ou de l'installation du fichier clé de licence (à l'exception de la version de démonstration du Logiciel), Vous pouvez bénéficier des services suivants pour la période définie stipulée sur l'emballage du Logiciel (si le Logiciel a été acquis sur un support physique) ou stipulée pendant l'acquisition (si le Logiciel a été acquis sur Internet) :
- Mises à jour du Logiciel par Internet lorsque le Titulaire des droits les publie sur son site Internet ou par le biais d'autres services en ligne. Toutes les Mises à jour que vous êtes susceptible de recevoir font partie intégrante du Logiciel et les conditions générales de ce Contrat leur sont applicables ;
- Assistance technique en ligne et assistance technique par téléphone.

3. Activation et durée de validité

3.1. Si vous modifiez Votre Ordinateur ou procédez à des modifications sur des logiciels provenant d'autres vendeurs et installés sur celui-ci, il est possible que le Titulaire des droits exige que Vous procédiez une nouvelle fois à l'activation du Logiciel ou à l'installation du fichier clé de licence. Le Titulaire des droits se réserve le droit d'utiliser tous les moyens et toutes les procédures de vérification de la validité de la Licence ou de la légalité du Logiciel installé ou utilisé sur Votre ordinateur.
3.2. Si le Logiciel a été acquis sur un support physique, le Logiciel peut être utilisé dès l'acceptation de ce Contrat pendant la période stipulée sur l'emballage et commençant à l'acceptation de ce Contrat.
3.3. Si le Logiciel a été acquis sur Internet, le Logiciel peut être utilisé à votre acceptation de ce Contrat, pendant la période stipulée lors de l'acquisition.
3.4. Vous avez le droit d'utiliser gratuitement une version de démonstration du Logiciel conformément aux dispositions de la Clause 2.1 pendant la seule période d'évaluation correspondante (30 jours) à compter de l'activation du Logiciel conformément à ce Contrat, *sachant que* la version de démonstration ne Vous donne aucun droit aux mises à jour et à l'assistance technique par Internet et par téléphone.
3.5. Votre Licence d'utilisation du Logiciel est limitée à la période stipulée dans les Clauses 3.2 ou 3.3 (selon le cas) et la période restante peut être visualisée par les moyens décrits dans le Manuel de l'utilisateur.
3.6. Si vous avez acquis le Logiciel dans le but de l'utiliser sur plus d'un Ordinateur, Votre Licence d'utilisation du Logiciel est limitée à la période commençant à la date d'activation du Logiciel ou de l'installation du fichier clé de licence sur le premier Ordinateur.
3.7. Sans préjudice des autres recours en droit ou équité à la disposition du Titulaire des droits, dans l'éventualité d'une rupture de votre part de toute clause de ce Contrat, le Titulaire des droits sera en droit, à sa convenance et sans préavis, de révoquer cette Licence sans rembourser le prix d'achat en tout ou en partie.
3.8. Vous vous engagez, dans le cadre de votre utilisation du Logiciel et de l'obtention de tout rapport ou de toute information dans le cadre de l'utilisation de ce Logiciel, à respecter toutes les lois et réglementations internationales, nationales, étatiques, régionales et locales en vigueur, ce qui comprend, sans toutefois s'y limiter, les lois relatives à la protection de la vie privée, des droits d'auteur, au contrôle des exportations et à la lutte contre les outrages à la pudeur.
3.9. Sauf disposition contraire spécifiquement énoncée dans ce Contrat, vous ne pouvez transférer ni céder aucun des droits qui vous sont accordés dans le cadre de ce Contrat ou aucune de vos obligations de par les présentes.

4. Assistance technique

4.1. L'assistance technique décrite dans la Clause 2.5 de ce Contrat Vous est offerte lorsque la dernière mise à jour du Logiciel est installée (sauf pour la version de démonstration du Logiciel).
Service d'assistance technique : http://support.kaspersky.com
4.2. Les données de l'utilisateur, spécifiées dans Personal Cabinet/My Kaspersky Account, ne peuvent être utilisées par les spécialistes de l'assistance technique que lors du traitement d'une requête de l'utilisateur.

5. Limitations

5.1. Vous vous engagez à ne pas émuler, cloner, louer, prêter, donner en bail, vendre, modifier, décompiler, ou faire l'ingénierie inverse du Logiciel, et à ne pas démonter ou créer des travaux dérivés reposant sur le Logiciel ou toute portion de celui-ci, à la seule exception du droit inaliénable qui Vous est accordé par la législation en vigueur, et vous ne devez autrement réduire aucune partie du Logiciel à une forme lisible par un humain ni transférer le Logiciel sous licence, ou toute sous-partie du Logiciel sous licence, ni autoriser une tierce partie de le faire, sauf dans la mesure où la restriction précédente est expressément interdite par la loi en vigueur. Ni le code binaire du Logiciel ni sa source ne peuvent être utilisés à des fins d'ingénierie inverse pour recréer le programme de l'algorithme, qui est la propriété

exclusive du Titulaire des droits. Tous les droits non expressément accordés par la présente sont réservés par le Titulaire des droits et/ou ses fournisseurs, suivant le cas. Toute utilisation du Logiciel en violation du Contrat entraînera la résiliation immédiate et automatique de ce Contrat et de la Licence concédée de par les présentes, et pourra entraîner des poursuites pénales et/ou civiles à votre encontre.
5.2. Vous ne devrez transférer les droits d'utilisation du Logiciel à aucune tierce partie.
5.3. Vous vous engagez à ne communiquer le code d'activation et/ou le fichier clé de licence à aucune tierce partie, et à ne permettre l'accès par aucune tierce partie au code d'activation et au fichier clé de licence qui sont considérés comme des informations confidentielles du Titulaire des droits.
5.4. Vous vous engagez à ne louer, donner à bail ou prêter le Logiciel à aucune tierce partie.
5.5. Vous vous engagez à ne pas vous servir du Logiciel pour la création de données ou de logiciels utilisés dans le cadre de la détection, du blocage ou du traitement des menaces décrites dans le Manuel de l'utilisateur.
5.6. Votre fichier clé peut être bloqué en cas de non-respect de Votre part des conditions générales de ce Contrat.
5.7. Si vous utilisez la version de démonstration du Logiciel, Vous n'avez pas le droit de bénéficier de l'assistance technique stipulée dans la Clause 4 de ce Contrat, et Vous n'avez pas le droit de transférer la licence ou les droits d'utilisation du Logiciel à une tierce partie.

6. Garantie limitée et avis de non-responsabilité

6.1. Le Titulaire des droits garantit que le Logiciel donnera des résultats substantiellement conformes aux spécifications et aux descriptions énoncées dans le Manuel de l'utilisateur, *étant toutefois entendu* que cette garantie limitée ne s'applique pas dans les conditions suivantes : (w) des défauts de fonctionnement de Votre Ordinateur et autres non-respects des clauses du Contrat, auquel cas le Titulaire des droits est expressément dégagé de toute responsabilité en matière de garantie ; (x) les dysfonctionnements, les défauts ou les pannes résultant d'une utilisation abusive, d'un accident, de la négligence, d'une installation inappropriée, d'une utilisation ou d'une maintenance inappropriée ; des vols ; des actes de vandalisme ; des catastrophes naturelles ; des actes de terrorisme ; des pannes d'électricité ou des surtensions ; des sinistres ; de l'altération, des modifications non autorisées ou des réparations par toute partie autre que le Titulaire des droits ; ou des actions d'autres tierces parties ou Vos actions ou des causes échappant au contrôle raisonnable du Titulaire des droits ; (y) tout défaut non signalé par Vous au Titulaire dès que possible après sa constatation ; et (z) toute incompatibilité causée par les composants du matériel et/ou du logiciel installés sur Votre Ordinateur.
6.2. Vous reconnaissez, acceptez et convenez qu'aucun logiciel n'est exempt d'erreurs, et nous Vous recommandons de faire une copie de sauvegarde des informations de Votre Ordinateur, à la fréquence et avec le niveau de fiabilité adapté à Votre cas.
6.3. Le Titulaire des droits n'offre aucune garantie de fonctionnement correct du Logiciel en cas de non-respect des conditions décrites dans le Manuel de l'utilisateur ou dans ce Contrat.
6.4. Le Titulaire des droits ne garantit pas que le Logiciel fonctionnera correctement si Vous ne téléchargez pas régulièrement les Mises à jour spécifiées dans la Clause 2.5 de ce Contrat.
6.5. Le Titulaire des droits ne garantit aucune protection contre les menaces décrites dans le Manuel de l'utilisateur à l'issue de l'échéance de la période indiquée dans les Clauses 3.2 ou 3.3 de ce Contrat, ou à la suite de la résiliation pour une raison quelconque de la Licence d'utilisation du Logiciel.
6.6. LE LOGICIEL EST FOURNI " TEL QUEL " ET LE TITULAIRE DES DROITS N'OFFRE AUCUNE GARANTIE QUANT À SON UTILISATION OU SES PERFORMANCES. SAUF DANS LE CAS DE TOUTE GARANTIE, CONDITION, DÉCLARATION OU TOUT TERME DONT LA PORTÉE NE PEUT ÊTRE EXCLUE OU LIMITÉE PAR LA LOI EN VIGUEUR, LE TITULAIRE DES DROITS ET SES PARTENAIRES N'OFFRENT AUCUNE GARANTIE, CONDITION OU DÉCLARATION (EXPLICITE OU IMPLICITE, QUE CE SOIT DE PARLA LÉGISLATION EN VIGUEUR, LA " COMMON LAW ", LA COUTUME, LES USAGES OU AUTRES) QUANT À TOUTE QUESTION DONT, SANS LIMITATION, L'ABSENCE D'ATTEINTE AUX DROITS DE TIERCES PARTIES, LE CARACTÈRE COMMERCIALISABLE, LA QUALITÉ SATISFAISANTE, L'INTÉGRATION OU L'ADÉQUATION À UNE FIN PARTICULIÈRE. VOUS ASSUMEZ TOUS LES DÉFAUTS, ET L'INTÉGRALITÉ DES RISQUES LIÉS À LA PERFORMANCE ET AU CHOIX DU LOGICIEL POUR ABOUTIR AUX RÉSULTATS QUE VOUS RECHERCHEZ, ET À L'INSTALLATION DU LOGICIEL, SON UTILISATION ET LES RÉSULTATS OBTENUS AU MOYEN DU LOGICIEL. SANS LIMITER LES DISPOSITIONS PRÉCÉDENTES, LE TITULAIRE DES DROITS NE FAIT AUCUNE DÉCLARATION ET N'OFFRE AUCUNE GARANTIE QUANT À L'ABSENCE D'ERREURS DU LOGICIEL, OU L'ABSENCE D'INTERRUPTIONS OU D'AUTRES PANNES, OU LA SATISFACTION DE TOUTES VOS EXIGENCES PAR LE LOGICIEL, QU'ELLES SOIENT OU NON DIVULGUÉES AU TITULAIRE DES DROITS.

7. Exclusion et Limitation de responsabilité

7.1. DANS LA MESURE MAXIMALE PERMISE PAR LA LOI EN VIGUEUR, LE TITULAIRE DES DROITS OU SES PARTENAIRES NE SERONT EN AUCUN CAS TENUS POUR RESPONSABLES DE TOUT DOMMAGE SPÉCIAL, ACCESSOIRE, PUNITIF, INDIRECT OU CONSÉCUTIF QUEL QU'IL SOIT (Y COMPRIS, SANS TOUTEFOIS S'Y LIMITER, LES DOMMAGES POUR PERTES DE PROFITS OU D'INFORMATIONS CONFIDENTIELLES OU AUTRES, EN CAS D'INTERRUPTION DES ACTIVITÉS, DE PERTE D'INFORMATIONS PERSONNELLES, DE CORRUPTION, DE DOMMAGE À DES DONNÉES OU À DES PROGRAMMES OU DE PERTES DE CEUX-CI, DE MANQUEMENT À L'EXERCICE DE TOUT DEVOIR, Y COMPRIS TOUTE OBLIGATION STATUTAIRE, DEVOIR DE BONNE FOI OU DE DILIGENCE RAISONNABLE, EN CAS DE NÉGLIGENCE, DE PERTE ÉCONOMIQUE, ET DE TOUTE AUTRE PERTE PÉCUNIAIRE OU AUTRE PERTE QUELLE QU'ELLE SOIT) DÉCOULANT DE OU LIÉ D'UNE MANIÈRE

QUELCONQUE À L'UTILISATION OU À L'IMPOSSIBILITÉ D'UTILISATION DU LOGICIEL, À L'OFFRE D'ASSISTANCE OU D'AUTRES SERVICES OU À L'ABSENCE D'UNE TELLE OFFRE, LE LOGICIEL, ET LE CONTENU TRANSMIS PAR L'INTERMÉDIAIRE DU LOGICIEL OU AUTREMENT DÉCOULANT DE L'UTILISATION DU LOGICIEL, OU AUTREMENT DE PAR OU EN RELATION AVEC TOUTE DISPOSITION DE CE CONTRAT, OU DÉCOULANT DE TOUTE RUPTURE DE CE CONTRAT OU DE TOUT ACTE DOMMAGEABLE (Y COMPRIS LA NÉGLIGENCE, LA FAUSSE DÉCLARATION, OU TOUTE OBLIGATION OU DEVOIR EN RESPONSABILITÉ STRICTE), OU DE TOUT MANQUEMENT À UNE OBLIGATION STATUTAIRE, OU DE TOUTE RUPTURE DE GARANTIE DU TITULAIRE DES DROITS ET/OU DE TOUT PARTENAIRE DE CELUI-CI, MÊME SI LE TITULAIRE DES DROITS ET/OU TOUT PARTENAIRE A ÉTÉ INFORMÉ DE LA POSSIBILITÉ DE TELS DOMMAGES.

VOUS ACCEPTEZ QUE, DANS L'ÉVENTUALITÉ OÙ LE TITULAIRE DES DROITS ET/OU SES PARTENAIRES SONT ESTIMÉS RESPONSABLES, LA RESPONSABILITÉ DU TITULAIRE DES DROITS ET/OU DE SES PARTENAIRES SOIT LIMITÉE AUX COÛTS DU LOGICIEL. LA RESPONSABILITÉ DU TITULAIRE DES DROITS ET/OU DE SES PARTENAIRES NE SAURAIT EN AUCUN CAS EXCÉDER LES FRAIS PAYÉS POUR LE LOGICIEL AU TITULAIRE DES DROITS OU AU PARTENAIRE (LE CAS ÉCHÉANT).

AUCUNE DISPOSITION DE CE CONTRAT NE SAURAIT EXCLURE OU LIMITER TOUTE DEMANDE EN CAS DE DÉCÈS OU DE DOMMAGE CORPOREL. PAR AILLEURS, DANS L'ÉVENTUALITÉ OÙ TOUTE DÉCHARGE DE RESPONSABILITÉ, TOUTE EXCLUSION OU LIMITATION DE CE CONTRAT NE SERAIT PAS POSSIBLE DU FAIT DE LA LOI EN VIGUEUR, ALORS SEULEMENT, CETTE DÉCHARGE DE RESPONSABILITÉ, EXCLUSION OU LIMITATION NE S'APPLIQUERA PAS DANS VOTRE CAS ET VOUS RESTEREZ TENU PAR LES DÉCHARGES DE RESPONSABILITÉ, LES EXCLUSIONS ET LES LIMITATIONS RESTANTES.

8. Licence GNU et autres licences de tierces parties

8.1. Le Logiciel peut comprendre des programmes concédés à l'utilisateur sous licence (ou sous licence) dans le cadre d'une licence publique générale GNU (General Public License, GPL) ou d'autres licences de logiciel gratuites semblables, qui entre autres droits, autorisent l'utilisateur à copier, modifier et redistribuer certains programmes, ou des portions de ceux-ci, et à accéder au code source (" Logiciel libre "). Si ces licences exigent que, pour tout logiciel distribué à quelqu'un au format binaire exécutable, le code source soit également mis à la disposition de ces utilisateurs, le code source sera communiqué sur demande adressée à source@kaspersky.com ou fourni avec le Logiciel. Si une licence de Logiciel libre devait exiger que le Titulaire des droits accorde des droits d'utilisation, de reproduction ou de modification du programme de logiciel libre plus importants que les droits accordés dans le cadre de ce Contrat, ces droits prévaudront sur les droits et restrictions énoncés dans les présentes.

9. Droits de propriété intellectuelle

9.1. Vous convenez que le Logiciel et le contenu exclusif, les systèmes, les idées, les méthodes de fonctionnement, la documentation et les autres informations contenues dans le Logiciel constituent un élément de propriété intellectuelle et/ou des secrets industriels de valeur du Titulaire des droits ou de ses partenaires, et que le Titulaire des droits et ses partenaires, le cas échéant, sont protégés par le droit civil et pénal, ainsi que par les lois sur la protection des droits d'auteur, des secrets industriels et des brevets de la Fédération de Russie, de l'Union européenne et des États-Unis, ainsi que d'autres pays et par les traités internationaux. Ce Contrat ne vous accorde aucun droit sur la propriété intellectuelle, en particulier toute marque de commerce ou de service du Titulaire des droits et/ou de ses partenaires (les " Marques de commerce "). Vous n'êtes autorisé à utiliser les Marques de commerce que dans la mesure où elles permettent l'identification des informations imprimées par le Logiciel conformément aux pratiques admises en matière de marques de commerce, en particulier l'identification du nom du propriétaire de la Marque de commerce. Cette utilisation d'une marque de commerce ne vous donne aucun droit de propriété sur celle-ci. Le Titulaire des droits et/ou ses partenaires conservent la propriété et tout droit, titre et intérêt sur la Marque de commerce et sur le Logiciel, y compris sans limitation, toute correction des erreurs, amélioration, mise à jour ou autre modification du Logiciel, qu'elle soit apportée par le Titulaire des droits ou une tierce partie, et tous les droits d'auteur, brevets, droits sur des secrets industriels, et autres droits de propriété intellectuelle afférents à ce Contrat. Votre possession, installation ou utilisation du Logiciel ne transfère aucun titre de propriété intellectuelle à votre bénéfice, et vous n'acquerrez aucun droit sur le Logiciel, sauf dans les conditions expressément décrites dans le cadre de ce Contrat. Toutes les reproductions du Logiciel effectuées dans le cadre de ce Contrat doivent faire mention des mêmes avis d'exclusivité que ceux qui figurent sur le Logiciel. Sauf dans les conditions énoncées par les présentes, ce Contrat ne vous accorde aucun droit de propriété intellectuelle sur le Logiciel et vous convenez que la Licence telle que définie dans ce document et accordée dans le cadre de ce Contrat ne vous donne qu'un droit limité d'utilisation en vertu des conditions générales de ce Contrat. Le Titulaire des droits se réserve tout droit qui ne vous est pas expressément accordé dans ce Contrat.
9.2. Vous convenez de ne modifier ou altérer le Logiciel en aucune façon. Il vous est interdit d'éliminer ou d'altérer les avis de droits d'auteur ou autres avis d'exclusivité sur tous les exemplaires du Logiciel.

10. Droit applicable ; arbitrage

10.1. Ce Contrat sera régi et interprété conformément aux lois de la Fédération de Russie sans référence aux règlements et aux principes en matière de conflits de droit. Ce Contrat ne sera pas régi par la Conférence des Nations-Unies sur les contrats de vente internationale de marchandises, dont l'application est strictement exclue. Tout litige

auquel est susceptible de donner lieu l'interprétation ou l'application des clauses de ce Contrat ou toute rupture de celui-ci sera soumis à l'appréciation du Tribunal d'arbitrage commercial international de la Chambre de commerce et d'industrie de la Fédération de Russie à Moscou (Fédération de Russie), à moins qu'il ne soit réglé par négociation directe. Tout jugement rendu par l'arbitre sera définitif et engagera les parties, et tout tribunal compétent pourra faire valoir ce jugement d'arbitrage. Aucune disposition de ce Paragraphe 10 ne saurait s'opposer à ce qu'une Partie oppose un recours en redressement équitable ou l'obtienne auprès d'un tribunal compétent, avant, pendant ou après la procédure d'arbitrage.

11. Délai de recours.

11.1. Aucune action, quelle qu'en soit la forme, motivée par des transactions dans le cadre de ce Contrat, ne peut être intentée par l'une ou l'autre des parties à ce Contrat au-delà d'un (1) an à la suite de la survenance de la cause de l'action, ou de la découverte de sa survenance, mais un recours en contrefaçon de droits de propriété intellectuelle peut être intenté dans la limite du délai statutaire maximum applicable.

12. Intégralité de l'accord ; divisibilité ; absence de renoncement.

12.1. Ce Contrat constitue l'intégralité de l'accord entre vous et le Titulaire des droits et prévaut sur tout autre accord, toute autre proposition, communication ou publication préalable, par écrit ou non, relatifs au Logiciel ou à l'objet de ce Contrat. Vous convenez avoir lu ce Contrat et l'avoir compris, et vous convenez de respecter ses conditions générales. Si un tribunal compétent venait à déterminer que l'une des clauses de ce Contrat est nulle, non avenue ou non applicable pour une raison quelconque, dans sa totalité ou en partie, cette disposition fera l'objet d'une interprétation plus limitée de façon à devenir légale et applicable, l'intégralité du Contrat ne sera pas annulée pour autant, et le reste du Contrat conservera toute sa force et tout son effet dans la mesure maximale permise par la loi ou en équité de façon à préserver autant que possible son intention originale. Aucun renoncement à une disposition ou à une condition quelconque de ce document ne saurait être valable, à moins qu'il soit signifié par écrit et signé de votre main et de celle d'un représentant autorisé du Titulaire des droits, étant entendu qu'aucune exonération de rupture d'une disposition de ce Contrat ne saurait constituer une exonération d'une rupture préalable, concurrente ou subséquente. Le manquement à la stricte application de toute disposition ou tout droit de ce Contrat par le Titulaire des droits ne saurait constituer un renoncement à toute autre disposition ou tout autre droit de par ce Contrat.

13. Informations de contact du Titulaire des droits

Si vous souhaitez joindre le Titulaire des droits pour toute question relative à ce Contrat ou pour quelque raison que ce soit, n'hésitez pas à vous adresser à notre service clientèle aux coordonnées suivantes :

Kaspersky Lab ZAO, 10 build. 1, 1st Volokolamsky Proezd
Moscou, 123060
Fédération de Russie
Tél. :+7-495-797-8700
Fax : +7-495-645-7939
E-mail : info@kaspersky.com
Site Internet : www.kaspersky.com

TABLE DES MATIERES

PRESENTATION DU MANUEL

Ce document est le manuel d'installation, de configuration et d'utilisation de l'application Kaspersky Endpoint Security 8 for Mac et décrit également l'administration à distance de l'application via Kaspersky Administration Kit. Il s'adresse aussi bien au grand public qu'aux administrateurs système. Les utilisateurs de l'application doivent avoir le niveau débutant d'utilisation de l'ordinateur Mac : connaître l'interface du système d'exploitation Mac OS X, avoir une pratique de base, savoir utiliser les logiciels pour travailler avec le courrier électronique et dans Internet.

Objectif de ce document :

- aider l'utilisateur à installer lui-même l'application sur l'ordinateur, à l'activer et à réaliser une configuration optimale qui tient compte de ses besoins ;
- aider l'administrateur à réaliser les tâches liées à l'administration de l'application via Kaspersky Administration Kit ;
- offrir un accès rapide aux informations pour répondre aux questions liées à l'application ;
- informer sur les sources complémentaires d'obtention des informations sur l'application, et sur les moyens de contacter le Service d'assistance technique de Kaspersky Lab.

DANS CETTE SECTION

DANS CE DOCUMENT

Le Manuel de l'administrateur de Kaspersky Endpoint Security 8 repend les chapitres suivants :

Sources d'informations complémentaires

Cette section contient des informations sur les sources de complémentaires permettant d'obtenir des l'informations supplémentaires sur l'application, sur Internet où vous pouvez discuter sur l'application, échanger des idées, poser des questions et recevoir des réponses.

Kaspersky Endpoint Security 8

Cette section décrit les fonctionnalités de l'application et offre des informations succinctes sur ses composants et les fonctions principales. Après la lecture de cette section, vous connaîtrez la distribution et l'ensemble des services accessibles aux utilisateurs enregistrés. La section présente la configuration matérielle et logicielle requise pour l'installation de Kaspersky Endpoint Security.

Installation de l'application

Cette rubrique reprend les instructions qui vous aideront à installer l'application localement sur l'ordinateur. Cette section aussi décrit comment supprimer l'application de l'ordinateur.

Gestion des licences

Cette section contient les informations sur les notions générales utilisées dans le contexte de l'octroi de licences de l'application. Cette section vous aidera à activer l'application, à consulter les informations sur la licence actuelle et à acheter la licence et à la renouveler.

Interface de l'application

Cette section contient la description des éléments de base de l'interface graphique de l'application : l'icône et le menu contextuel de l'application, la fenêtre principale, la fenêtre de configuration et les fenêtres des notifications.

Lancement et arrêt de l'application

Cette rubrique explique comment lancer et arrêter l'application.

Etat de la protection de l'ordinateur

Cette rubrique contient des informations qui permettront de confirmer si l'ordinateur est protégé ou si sa sécurité est menacée. Elle explique également comment supprimer les menaces qui se présentent à l'aide de l'Assistant de sécurité.

Résolution des problèmes types

Cette section contient une description des tâches auxquelles est confrontée la majorité des utilisateurs lors de l'utilisation de l'application et les instructions pour les exécuter.

Configuration étendue de l'application

Cette section contient des informations détaillées sur chacun des composants de l'application et une description de l'algorithme de fonctionnement et de la configuration des paramètres du composant.

Utilisation de l'application au départ de la ligne de commande

Cette section fournit une description de l'utilisation de l'application et de ses composants via la ligne de commande.

Administration du logiciel via Kaspersky Administration Kit

Cette rubrique décrit en détails l'installation de Kaspersky Endpoint Security sur l'ordinateur distant de l'utilisateur ainsi que l'installation de l'application requise pour l'administration à distance de l'application via Kaspersky Administration Kit. Après avoir lu ce chapitre, vous connaîtrez la procédure de déploiement de l'application sur le réseau de l'entreprise et l'administration à distance via Kaspersky Administration Kit à l'aide de tâches et de stratégies de groupe.

Contacter le Service d'assistance technique

Cette rubrique regroupe les recommandations pour contacter le service d'assistance technique de Kaspersky Lab.

Applications.

Cette section contient des renseignements qui viennent compléter le contenu principal du document.

Glossaire

Cette section contient la liste des termes qui apparaissent dans le document, et leurs définitions.

CONVENTIONS

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

Tableau 1. Conventions

EXEMPLE DE TEXTE	DESCRIPTION DE LA CONVENTION
N'oubliez pas que ...	Les avertissements apparaissent en rouge et sont encadrés. Les avertissements contiennent les 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 ".
Un virus est ...	Les nouveaux termes sont en italique.
Command-A	Les noms des touches du clavier sont en caractères mi-gras. 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.
`kav update`	Le texte dans la ligne de commande ou le texte 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

Vous pouvez consulter les sources suivantes pour obtenir des informations sur l'application :

- la page sur le site Web de Kaspersky Lab ;
- la page sur le site Web du Service d'assistance technique (banque de solutions) ;
- le forum des utilisateurs des logiciels de Kaspersky Lab ;
- système d'aide électronique.

La page sur le site Web de Kaspersky Lab

La page de l'application (http://www.kaspersky.fr/endpoint-security-mac) offre des informations générales sur Kaspersky Endpoint Security, ses possibilités et les particularités de son fonctionnement. Vous pouvez acheter Kaspersky Endpoint Security 8 ou prolonger sa durée d'utilisation dans notre magasin en ligne.

Page sur le site Web du Service d'assistance technique (banque de solutions)

La banque de solutions est une section du site du Service d'assistance technique (http://support.kaspersky.com/fr/kes8mac) qui contient des recommandations sur l'utilisation des produits de Kaspersky Lab. Cette page propose des articles publiés par les experts du Service d'assistance technique.

Ces articles contiennent des informations utiles, des recommandations et les réponses aux questions les plus souvent posées sur l'achat, l'installation et l'utilisation de Kaspersky Endpoint Security 8. Ils sont regroupés par thèmes tels que "Résolution de problèmes", "Configuration de la mise à jour" ou "Configuration de l'Antivirus Fichiers". Les articles peuvent répondre à des questions concernant non seulement Kaspersky Endpoint Security 8, mais également d'autres logiciels de Kaspersky Lab. Ils peuvent également contenir des nouvelles du Service d'assistance technique dans son ensemble.

Pour accéder à la Banque de solutions, ouvrez le menu principal de l'application (à la page 33), cliquez sur le bouton  et dans la fenêtre qui s'ouvre, cliquez sur le bouton **Service d'assistance technique**.

Forum des utilisateurs

Si votre question n'est pas urgente, vous pouvez en discuter avec les experts de Kaspersky Lab et d'autres utilisateurs sur notre forum (http://forum.kaspersky.fr/). Ce service est une section du site Web du Service d'assistance technique. Il contient les questions, les remarques et les suggestions des utilisateurs de Kaspersky Endpoint Security 8.

Sur le forum, vous pouvez consulter les thèmes publiés, ajouter vos commentaires, créer une nouvelle discussion ou lancer des recherches.

Pour accéder à cette ressource, ouvrez la fenêtre principale de l'application (à la page 33), cliquez sur le bouton  et dans la fenêtre qui s'ouvre, cliquez sur le bouton **Forum**.

Système d'aide électronique

L'application contient les fichiers de l'aide complète et de l'aide contextuelle. L'aide complète explique comment administrer la protection de l'ordinateur, consulter l'état de la protection, analyser différents secteurs de l'ordinateur à la recherche d'éventuels virus, réaliser la mise à jour, utiliser les rapports et les banques. En plus, dans le fichier d'aide contextuelle vous pouvez trouver les informations sur chaque fenêtre de l'application : description des paramètres qui figurent dans chacune d'entre elles et liste des tâches exécutées.

Pour ouvrir l'aide complète, ouvrez la fenêtre principale de l'application (à la page 33) et cliquez sur le bouton  .
Pour ouvrir l'aide contextuelle, ouvrez la fenêtre ou l'onglet de la fenêtre qui vous intéresse et cliquez sur la touche  .

Si vous ne trouvez pas la solution à votre problème dans la banque de solutions, sur le forum des utilisateurs, dans l'aide ou dans la documentation, contactez le Service d'assistance technique de Kaspersky Lab (cf. section "Contacter le Service d'assistance technique" à la page 157).

KASPERSKY ENDPOINT SECURITY 8

Kaspersky Endpoint Security 8 for Mac (ci-après, Kaspersky Endpoint Security) a été développé pour assurer la protection des ordinateurs sous le système d'exploitation Mac OS X contre l'action des virus et des programmes malveillants. L'application offre les possibilités suivantes :

Antivirus Fichiers

Protection en temps réel du système de fichiers de l'ordinateur : interception et analyse des requêtes adressées au système de fichiers, réparation et suppression des fichiers nociceptifs et isolement des objets potentiellement infectés en vue d'une analyse ultérieure.

Analyse

Recherche et neutralisation du code malveillant à la demande de l'utilisateur : recherche et analyse des objets malveillants ou potentiellement infectés dans les zones d'analyse définies, réparation, suppression ou isolement des objets en vue d'une analyse ultérieure.

Kaspersky Endpoint Security est livrée avec les tâches d'analyse de virus les plus souvent utilisées : analyse complète de tous les objets de l'ordinateur et analyse rapide des secteurs critiques.

Mise à jour

Mise à jour des bases et des modules faisant partie de Kaspersky Endpoint Security depuis les serveurs de mise à jour de Kaspersky Lab et depuis le Serveur d'administration Kaspersky Administration Kit, création d'une copie de sauvegarde de tous les fichiers actualisés au cas où il faudrait revenir à la version antérieure de la mise à jour, copie des mises à jour récupérées dans la source locale en vue de la proposer aux autres ordinateurs du réseau (afin de réduire le trafic Internet).

Quarantaine

Mise en quarantaine des objets potentiellement infectés : conservation des objets potentiellement infectés dans le dossier de quarantaine, analyse ultérieure de ceux-ci à l'aide des bases actualisées et restauration des objets de la quarantaine à la demande de l'utilisateur.

Dossier de sauvegarde

Création d'une copie de l'objet infecté dans la sauvegarde avant la réparation ou la suppression afin de pouvoir éventuellement le restaurer à la demande, représentant une valeur informative.

Rapports

Création de rapports détaillés sur le fonctionnement de chaque composant de Kaspersky Endpoint Security.

Notifications

Avertissement de l'utilisateur sur l'occurrence de certains événements dans le travail de Kaspersky Endpoint Security. L'application permet de choisir le mode de notification pour chaque type d'événement : notification sonore ou message contextuel.

Vous pouvez modifier l'apparence de Kaspersky Endpoint Security en utilisant vos propres éléments graphiques et la palette de couleurs sélectionnée.

Vous recevez toutes les informations relatives au fonctionnement de l'application : Kaspersky Endpoint Security affiche des messages sur l'état de la protection et vous propose un fichier d'aide détaillé. L'Assistant de sécurité (à la page 44) inclus dans l'application dresse le tableau complet de la protection actuelle de l'ordinateur et permet de résoudre les problèmes immédiatement.

DANS CETTE SECTION

DISTRIBUTION

Vous pouvez acheter Kaspersky Endpoint Security chez nos partenaires (version en boîte) ou en ligne (par exemple, http://www.kaspersky.fr, section **Boutique en ligne**).

Si vous achetez le logiciel en boîte, vous recevrez :

- Une enveloppe cachetée contenant le cédérom d'installation avec les fichiers du logiciel et la documentation au format PDF.
- Le contrat de licence.

La distribution peut contenir également :

- La version "papier" du guide de l'utilisateur (si cette option avait été incluse dans la commande) ou du guide du logiciel.
- Le fichier de licence de l'application sur une disquette spéciale.
- Une carte d'inscription (reprenant le numéro de série du logiciel).

Avant d'ouvrir l'enveloppe contenant le cédérom, veuillez lire attentivement le contrat de licence. L'ouverture de l'enveloppe contenant le cédérom d'installation marque votre accord avec les termes du contrat de licence.

Si vous achetez Kaspersky Endpoint Security en ligne, vous copiez le logiciel depuis le site Internet de Kaspersky Lab. Cette distribution, outre le logiciel, reprend également ce Manuel. Le fichier de licence ou le code d'activation vous sera envoyé par courrier électronique après le paiement.

CONFIGURATION MATERIELLE ET LOGICIELLE REQUISES

Pour que Kaspersky Endpoint Security puisse fonctionner normalement, l'ordinateur de l'utilisateur doit répondre aux exigences minimales suivantes :

- ordinateur Mac à base de processeur Intel (le processeur PowerPC n'est pas pris en charge) ;
- 1 Go de mémoire vive;
- 500 Mo d'espace disponible sur le disque dur ;
- système d'exploitation Mac OS X 10.4.11 ou plus récent, ou Mac OS X Server 10.6.

Pour installer l'Agent d'administration nécessaire pour l'administration à distance de Kaspersky Endpoint Security via Kaspersky Administration Kit, l'ordinateur de l'utilisateur doit satisfaire les exigences minimales suivantes :

- ordinateur Mac à base de processeur Intel (le processeur PowerPC n'est pas pris en charge) ;
- 512 Mo de mémoire vive;
- 30 Mo d'espace disponible sur le disque dur ;
- système d'exploitation Mac OS X 10.4.11 ou plus récent, ou Mac OS X Server 10.6.

INSTALLATION DE L'APPLICATION

Cette rubrique reprend les instructions qui vous aideront à installer l'application localement sur l'ordinateur. Cette section aussi décrit comment supprimer l'application de l'ordinateur.

Le paquet d'installation de Kaspersky Endpoint Security contient le programme d'installation et le programme de suppression de l'application.

L'administration à distance de Kaspersky Endpoint Security via Kaspersky Administration Kit requiert l'installation du plug-in d'administration Kaspersky Endpoint Security sur le poste de travail de l'administrateur et de l'Agent d'administration sur l'ordinateur de l'utilisateur (cf. section "Installation de l'application indispensable à l'administration à distance de Kaspersky Endpoint Security" à la page 114). Il est également possible de réaliser l'installation à distance de Kaspersky Endpoint Security sur l'ordinateur de l'utilisateur (cf. section "Installation à distance de Kaspersky Endpoint Security" à la page 119).

DANS CETTE SECTION

PREPARATIFS POUR L'INSTALLATION DE L'APPLICATION

Avant d'installer Kaspersky Endpoint Security sur l'ordinateur, il faut exécuter toute une série d'actions de préparation :

- Assurez-vous que votre ordinateur correspond aux exigences du système (cf. section "Configuration matérielle et logicielle requises" à la page 18).
- Vérifiez la connexion de votre ordinateur à Internet. L'accès à Internet est nécessaire pour activer l'application à l'aide du code d'activation et pour recevoir les mises à jour.
- Supprimez les autres applications antivirus de l'ordinateur pour éviter l'apparition des conflits de système et le ralentissement de la rapidité du système d'exploitation.

PROCEDURE D'INSTALLATION DE L'APPLICATION

L'installation de Kaspersky Endpoint Security sur l'ordinateur peut s'opérer d'une des manières suivantes :

- Installation standard (cf. section "Installation standard de Kaspersky Endpoint Security" à la page 21).

  La sélection de composants de l'application par défaut sera installée.

- Installation personnalisée (cf. section "Installation personnalisée de Kaspersky Endpoint Security" à la page 22).

  Cette installation permet de choisir les composants de l'application à installer. Elle est recommandée pour les utilisateurs expérimentés.

INSTALLATION STANDARD DE KASPERSKY ENDPOINT SECURITY

Pour réaliser l'installation standard de Kaspersky Endpoint Security sur l'ordinateur, procédez comme suit :

1. Ouvrez le contenu du fichier d'installation de Kaspersky Endpoint Security. Pour ce faire, introduisez le disque d'installation dans le lecteur.

   Si vous avez acheté Kaspersky Endpoint Security dans un magasin en ligne, alors le fichier d'installation de l'application au format ZIP peut être téléchargé du site de Kaspersky Lab. Décompressez le fichier et ouvrez le fichier .dmg afin de voir le contenu du paquet d'installation.

2. Exécutez le programme d'installation de Kaspersky Endpoint Security. Pour ce faire, ouvrez le paquet d'installation **Kaspersky Endpoint Security** dans la fenêtre du contenu du paquet d'installation.

   Installez l'application en suivant les instructions du programme d'installation.

3. Dans la fenêtre **Introduction**, cliquez sur le bouton **Continuer**.

4. Dans la fenêtre **Lisez-moi**, lisez les informations sur l'application à installer.

   Assurez-vous que votre ordinateur correspond aux exigences de système indiquées. Pour imprimer ces informations, cliquez sur le bouton **Imprimer**. Pour sauvegarder les informations dans un fichier texte, cliquez sur le bouton **Enregistrer**. Pour poursuivre l'installation, cliquez sur **Continuer**.

5. Dans la fenêtre **Licence**, lisez le texte du contrat de licence sur l'utilisation de Kaspersky Endpoint Security, qui a été conclu entre vous et Kaspersky Lab. Le texte du contrat est disponible en plusieurs langues. Pour imprimer le texte du contrat, cliquez sur le bouton **Imprimer**. Pour sauvegarder le contrat dans un fichier texte, cliquez sur le bouton **Enregistrer**.

   Si vous acceptez toutes les conditions du contrat, cliquez sur le bouton **Continuer**. La fenêtre de confirmation de l'acceptation des termes du contrat de licence s'ouvrira. Vous pouvez exécuter les opérations suivantes :

   - Poursuivre l'installation de Kaspersky Endpoint Security. Pour ce faire, cliquez sur **Accepter**.
   - Revenir au texte du contrat. Pour ce faire, cliquez sur le bouton **Lire la licence**.
   - Interrompre l'installation de l'application. Pour ce faire, cliquez sur **Refuser**.

6. Dans la fenêtre **Type d'installation**, étudiez les informations sur le disque sur lequel l'application sera installée, et sur l'espace minimal requis sur le disque pour l'installation.

   Pour installer l'application en utilisant les paramètres d'installation standards proposés, cliquez sur le bouton **Installer** et saisissez le mot de passe de l'administrateur pour confirmer.

   Pour sélectionner un autre disque pour installer l'application, cliquez sur le bouton **Modifier l'emplacement de l'installation** et sélectionnez un autre disque, puis cliquez sur le bouton **Continuer**.

   Le disque d'amorçage est requis pour l'installation de l'application. Le système d'exploitation de la version non pas inférieure à celle indiquée dans les exigences de système (cf. section "Configuration matérielle et logicielle requises" à la page 18) doit être installé sur le disque.

   Attendez la fin de l'installation des composants par le programme d'installation de Kaspersky Endpoint Security.

7. Dans la fenêtre **Résumé**, lisez les informations sur la fin du processus d'installation et cliquez sur le bouton **Fermer** pour quitter le programme d'installation.

   Kaspersky Endpoint Security démarre automatiquement à l'issue de l'installation. Le redémarrage de l'ordinateur n'est pas requis.

INSTALLATION PERSONNALISEE DE KASPERSKY ENDPOINT SECURITY

Pour réaliser l'installation personnalisée de Kaspersky Endpoint Security sur l'ordinateur, procédez comme suit :

1. Ouvrez le contenu du fichier d'installation de Kaspersky Endpoint Security. Pour ce faire, introduisez le disque d'installation dans le lecteur.

   Si vous avez acheté Kaspersky Endpoint Security dans un magasin en ligne, alors le fichier d'installation de l'application au format ZIP peut être téléchargé du site de Kaspersky Lab. Décompressez le fichier et ouvrez le fichier .dmg afin de voir le contenu du paquet d'installation.

2. Exécutez le programme d'installation de Kaspersky Endpoint Security. Pour ce faire, ouvrez le paquet d'installation **Kaspersky Endpoint Security** dans la fenêtre du contenu du paquet d'installation.

   Installez l'application en suivant les instructions du programme d'installation.

3. Dans la fenêtre **Introduction**, cliquez sur le bouton **Continuer**.

4. Dans la fenêtre **Lisez-moi**, lisez les informations sur l'application à installer.

   Assurez-vous que votre ordinateur correspond aux exigences de système indiquées. Pour imprimer ces informations, cliquez sur le bouton **Imprimer**. Pour sauvegarder les informations dans un fichier texte, cliquez sur le bouton **Enregistrer**. Pour poursuivre l'installation, cliquez sur **Continuer**.

5. Dans la fenêtre **Licence**, lisez le texte du contrat de licence sur l'utilisation de Kaspersky Endpoint Security, qui a été conclu entre vous et Kaspersky Lab. Le texte du contrat est disponible en plusieurs langues. Pour imprimer le texte du contrat, cliquez sur le bouton **Imprimer**. Pour sauvegarder le contrat dans un fichier texte, cliquez sur le bouton **Enregistrer**.

   Si vous acceptez toutes les conditions du contrat, cliquez sur le bouton **Continuer**. La fenêtre de confirmation de l'acceptation des termes du contrat de licence s'ouvrira. Vous pouvez exécuter les opérations suivantes :

   - Poursuivre l'installation de Kaspersky Endpoint Security. Pour ce faire, cliquez sur **Je confirme**.
   - Revenir au texte du contrat. Pour ce faire, cliquez sur le bouton **Lire la licence**.
   - Interrompre l'installation de l'application. Pour ce faire, cliquez sur **Ne confirme pas**.

6. Dans la fenêtre **Type d'installation**, étudiez les informations sur le disque sur lequel l'application sera installée, et sur l'espace minimal requis sur le disque pour l'installation.

   Pour sélectionner un autre disque pour installer l'application, cliquez sur le bouton **Modifier l'emplacement de l'installation** et sélectionnez un autre disque, puis cliquez sur le bouton **Continuer**.

   Le disque d'amorçage est requis pour l'installation de l'application. Le système d'exploitation de la version non pas inférieure à celle indiquée dans les exigences de système (cf. section "Configuration matérielle et logicielle requises" à la page 18) doit être installé sur le disque.

   Cliquez sur le bouton **Paramètres** afin de sélectionner les composants à installer.

7. Dans la fenêtre ouverte, indiquez les composants de l'application à installer sur l'ordinateur. Décochez les cases à côté des noms des composants à ne pas installer.

   - **Analyse**. Assure l'analyse des objets dans les zones définies par l'utilisateur.

     Ce composant de Kaspersky Endpoint Security est toujours installé.

- **Antivirus Fichiers**. Effectue l'analyse de tous les objets ouverts, lancés et enregistrés en temps réel.
- **Menu contextuel Finder**. Permet d'analyser les virus d'objets affichés dans Finder. Le lancement de l'analyse s'effectue à partir du menu contextuel de l'objet.
- **Connecteur pour l'Agent d'administration**. Indispensable à l'administration à distance de l'application via Kaspersky Administration Kit.

Après avoir sélectionné les composants, cliquez sur le bouton **Installer** et saisissez le mot de passe de l'administrateur pour confirmer. Pour revenir aux paramètres standards d'installation (cf. section "Installation standard de Kaspersky Endpoint Security" à la page 21), cliquez sur le bouton **Installation standard**.

Attendez la fin de l'installation des composants sélectionnés par le programme d'installation de Kaspersky Endpoint Security.

8. Dans la fenêtre **Résumé**, lisez les informations sur la fin du processus d'installation et cliquez sur le bouton **Fermer** pour quitter le programme d'installation.

Kaspersky Endpoint Security démarre automatiquement à l'issue de l'installation. Le redémarrage de l'ordinateur n'est pas requis.

PREPARATION AU TRAVAIL

Après l'installation de Kaspersky Endpoint Security, nous vous recommandons d'exécuter les actions suivantes :

- Activer Kaspersky Endpoint Security (cf. section "Activation de Kaspersky Endpoint Security" à la page 28). L'utilisation d'une version sous licence vous donne la possibilité d'actualiser régulièrement les bases antivirus et d'accéder au service d'assistance technique.
- Evaluer l'état actuel de la protection (cf. section "Evaluation de l'état de la protection de l'ordinateur" à la page 43) pour s'assurer que Kaspersky Endpoint Security offre le niveau de sécurité souhaité.
- Mettre à jour Kaspersky Endpoint Security (cf. section "Procédure de mise à jour des bases et des modules de l'application" à la page 47). Il est indispensable de maintenir les bases de Kaspersky Endpoint Security à jour pour que l'application soit toujours en mesure d'identifier et de neutraliser les programmes malveillants.
- Lancer une analyse complète de l'ordinateur sur les virus (cf. section "Recherche d'éventuels virus dans tout l'ordinateur" à la page 45).

En cas de problèmes ou d'erreurs pendant l'utilisation de l'application, ouvrez la fenêtre des rapports sur le fonctionnement de Kaspersky Endpoint Security (cf. section "Rapports" à la page 98). Le rapport contiendra peut-être la description de la cause de l'échec. Si vous ne parvenez pas à résoudre vous-même le problème, contactez le Service d'assistance technique de Kaspersky Lab (cf. section "Contacter le Service d'assistance technique" à la page 157).

SUPPRESSION DE L'APPLICATION

La suppression de Kaspersky Endpoint Security expose votre ordinateur à de sérieux risques d'infection.

Avant de commencer la suppression, nous vous recommandons de traiter tous les objets en quarantaine et dans le dossier de sauvegarde. Tous les objets non traités dans les stockages seront supprimés sans possibilité de les restaurer.

Pour supprimer Kaspersky Endpoint Security, procédez comme suit :

1. Ouvrez le contenu du fichier d'installation de Kaspersky Endpoint Security. Pour ce faire, introduisez le disque d'installation dans le lecteur

   Si vous avez acheté Kaspersky Endpoint Security dans un magasin en ligne, alors le fichier d'installation de l'application au format ZIP peut être téléchargé du site de Kaspersky Lab. Décompressez le fichier et ouvrez le fichier .dmg afin de voir le contenu du paquet d'installation.

2. Exécutez le programme de suppression de Kaspersky Endpoint Security. Pour ce faire, ouvrez le paquet d'installation **Suppression de Kaspersky Endpoint Security** dans la fenêtre du contenu du paquet d'installation.

   Suivez ses étapes pour supprimer l'application.

3. Dans la fenêtre **Introduction**, cliquez sur le bouton **Poursuivre**.

4. Dans la fenêtre **Informations**, lisez les informations importantes. Pour lancer la procédure de suppression, cliquez sur le bouton **Supprimer** et saisissez le mot de passe de l'administrateur pour confirmer. Attendez pendant la suppression de l'application.

5. Dans la fenêtre **Fin**, lisez les informations sur la fin du processus de suppression et cliquez sur le bouton **Terminer** pour quitter le programme de suppression.

   Il n'est pas nécessaire de redémarrer l'ordinateur après la suppression de Kaspersky Endpoint Security.

GESTION DES LICENCES

Cette section contient les informations sur les notions générales utilisées dans le contexte de l'octroi de licences de l'application. Cette section vous aidera à activer l'application, à consulter les informations sur la licence actuelle et à acheter la licence et à la renouveler.

DANS CETTE SECTION

PRESENTATION DE LA LICENCE

Licence : le droit d'utilisation de Kaspersky Endpoint Security et des services complémentaires liés à l'application. Ces services sont offerts par Kaspersky Lab et ses partenaires.

Chaque licence se caractérise par la durée de validité et le type.

La durée de validité d'une licence est la période au cours de laquelle vous pouvez bénéficier des services complémentaires :

- l'assistance technique ;
- mise à jour des bases et des modules de l'application.

Le volume des services offerts dépend du type de licence.

Les types suivants de licences sont prévus :

- *Evaluation* : une licence gratuite avec la durée de validité limitée, par exemple, de 30 jours. Cette licence est conçue pour faire connaissance avec Kaspersky Endpoint Security.

  La licence d'évaluation ne peut être utilisée qu'une seule fois.

  Etant donné la licence d'évaluation, vous pouvez contacter le Service d'assistance technique uniquement pour les questions sur l'activation de l'application ou sur l'achat d'une licence commerciale. A la fin de la durée de validité de la licence d'évaluation, Kaspersky Endpoint Security arrête l'exécution de toutes les fonctions. Pour continuer à utiliser l'application, il faut l'activer (cf. section "Procédure d'activation de Kaspersky Endpoint Security" à la page 28).

- *Commerciale* : licence payante à durée de validité limitée (par exemple, un an).

Pendant l'action de la licence commerciale, toutes les fonctions de l'application et les services complémentaires sont accessibles.

Une fois la licence commerciale expirée, Kaspersky Endpoint Security continue à exécuter toutes ses fonctions. Cependant, la mise à jour des bases antivirus ne se passe pas. Vous pouvez comme toujours analyser votre ordinateur sur les virus et utilisez les composants de la protection, mais uniquement à l'aide des bases antivirus actuelles à la date de fin de validité de la licence. Afin que votre ordinateur ne soit pas contaminé par de nouveaux virus, nous vous conseillons de prolonger la validité de la licence de l'application.

Après avoir activé l'application avec la licence commerciale, vous pouvez acheter la licence supplémentaire pour Kaspersky Endpoint Security et l'activer. Dans ce cas, à l'expiration de la licence active, la licence supplémentaire deviendra automatiquement active, et l'application poursuivra son fonctionnement sans modification. Kaspersky Endpoint Security peut avoir qu'une seule licence supplémentaire.

CONSULTATION DES INFORMATIONS SUR LA LICENCE

Pour consulter les informations sur la licence utilisée,

ouvrez la fenêtre principale de l'application (à la page 33) et cliquez sur le bouton  .

Dans la fenêtre qui s'ouvre (cf. ill. ci-après), vous trouverez le numéro de licence, son type (commerciale ou évaluation), les restrictions sur le nombre d'ordinateurs sur lesquels la licence peut être utilisée, la date et l'heure de fin de validité de la licence, ainsi que le nombre de jours restant avant cette date.

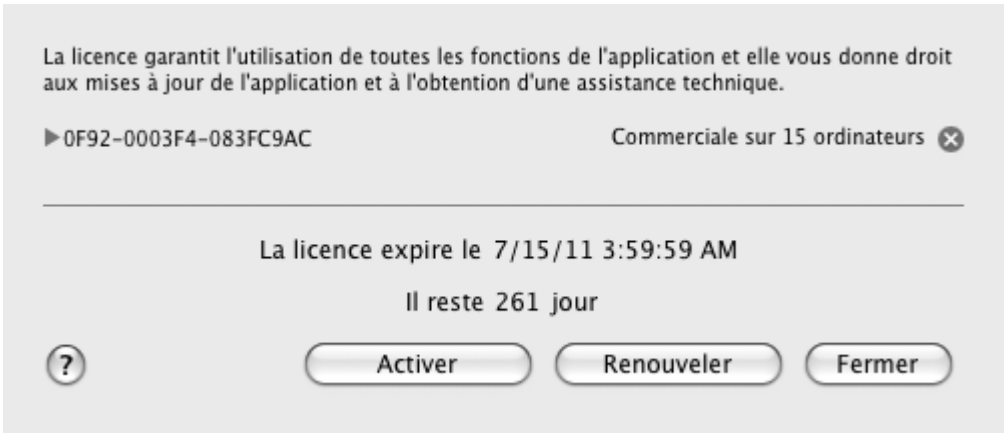


Illustration 1. Gestion des licences

Si la licence est introuvable, Kaspersky Endpoint Security vous le signale. Si l'application n'est pas activée, vous pouvez lancer la procédure d'activation (cf. section "Activation de Kaspersky Endpoint Security" à la page 28). Si la version d'évaluation de l'application est activée, vous pouvez acheter une licence commerciale (cf. section "Achat d'une licence" à la page 26). Si la licence commerciale expire, vous pouvez la renouveler (cf. section "Renouveler la licence" à la page 27).

ACHAT D'UNE LICENCE

Pour acheter une nouvelle licence, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (à la page 33) et cliquez sur le bouton  .
2. Dans la fenêtre ouverte (cf. ill. ci-après), cliquez sur le bouton **Acheter**.

Dans la page Web qui s'ouvre, vous pourrez saisir toutes les informations relatives à l'achat de la licence par la boutique en ligne de Kaspersky Lab ou auprès des partenaires de la société. En cas d'achat par la boutique en ligne, vous

recevrez, après confirmation du paiement, le code d'activation de Kaspersky Endpoint Security (cf. section "Présentation du code d'activation" à la page 28) dans un message envoyé à l'adresse indiquée dans le bon de commande.

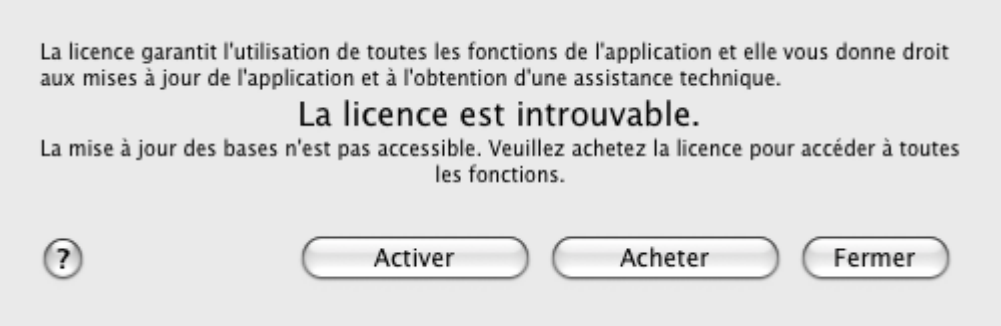


Illustration 2. Achat d'une licence

RENOUVELER LA LICENCE

La nécessité à renouveler la licence sur l'utilisation de l'application surgit à l'expiration de la licence existante. Dans ce cas, Kaspersky Endpoint Security continue son fonctionnement. Cependant, la mise à jour des bases antivirus n'est pas réalisée.

Pour renouveler le droit d'utilisation de la licence disponible, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (à la page 33) et cliquez sur le bouton .
2. Dans la fenêtre ouverte (cf. ill. ci-après), cliquez sur le bouton **Renouveler**.

Dans la page Web qui s'ouvre, vous pourrez saisir toutes les informations relatives au renouvellement de la licence par la boutique en ligne de Kaspersky Lab ou auprès des partenaires de la société. En cas de renouvellement par la boutique en ligne, vous recevrez, après confirmation du paiement, le code d'activation de Kaspersky Endpoint Security (cf. section "Présentation du code d'activation" à la page 28) dans un message envoyé à l'adresse indiquée dans le bon de commande.

Kaspersky Lab organise régulièrement des campagnes qui permettent aux utilisateurs actuels de renouveler leur licence en profitant de remises. Tenez-vous au cours de ces campagnes dans la section **Produits → Promotions et offres spéciales** de Kaspersky Lab.

Illustration 3. Gestion des licences

PRESENTATION DU CONTRAT DE LICENCE

Le contrat de licence est un accord conclu entre une personne physique ou morale détenant une copie légale de Kaspersky Endpoint Security et Kaspersky Lab. Ce contrat figure dans chaque application de Kaspersky Lab. Il reprend des informations détaillées sur les droits et les restrictions d'utilisation de Kaspersky Endpoint Security.

PRESENTATION DU CODE D'ACTIVATION

Le code d'activation est un code que vous recevez après l'achat de la licence commerciale de Kaspersky Endpoint Security. Ce code est indispensable pour activer l'application.

Il se présente sous la forme d'une succession de chiffres et de lettres, séparés par des tirets en groupe de quatre caractères, par exemple : AA111-AA111-AA111-AA111.

PRESENTATION DU FICHIER CLE

Kaspersky Endpoint Security fonctionne grâce à une *fichier clé*. Le fichier clé est délivré sur la base du code d'activation (cf. section "Présentation du fichier clé" à la page 28), obtenu à l'achat de l'application, et permet d'utiliser l'application à partir du jour de l'activation. Le fichier clé contient les informations relatives à la licence : type, durée de validité, nombre d'ordinateurs couverts par la licence.

ACTIVATION DE KASPERSKY ENDPOINT SECURITY

Avant d'activer Kaspersky Endpoint Security, assurez-vous que la date et l'heure système de l'ordinateur correspondent à la date et à l'heure réelles.

La procédure d'activation consiste à installer le fichier clé (cf. section "Présentation du fichier clé" à la page 28) qui permet à Kaspersky Endpoint Security de vérifier les autorisations d'utilisation de l'application et de déterminer la durée de validité.

L'activation de l'application s'opère à l'aide de l'Assistant d'activation. Suivez ses étapes pour activer l'application.

A chaque étape de l'Assistant, vous pouvez cliquer sur le bouton **Annuler** et par cela même interrompre l'activation de l'application. Le fonctionnement de l'Assistant sera terminé. Si l'application n'est pas activée, toutes les fonctions de Kaspersky Endpoint Security vous seront accessibles sauf l'obtention des mises à jour. Il est possible d'actualiser l'application uniquement une fois après son installation.

DANS CETTE SECTION

ACTIVATION DE L'APPLICATION A L'AIDE DU CODE D'ACTIVATION

Utilisez cette option si vous avez reçu le code d'activation. Ce code vous permet d'obtenir le fichier clé qui donne accès à toutes les fonctions de Kaspersky Endpoint Security pendant la durée de validité de la licence.

Si vous avez reçu le code d'activation pour une version d'évaluation de l'application, vous recevez une clé gratuite dont la validité sera limitée par la licence d'évaluation. L'activation de la version d'évaluation de l'application est possible uniquement si cette version de Kaspersky Endpoint Security n'a jamais été installée sur l'ordinateur.

Lors de la sélection de l'activation à l'aide du code d'activation, la connexion à Internet est requise. Si au moment présent la connexion à Internet est absente, vous pouvez activer l'application plus tard.

Pour activer l'application à l'aide du code d'activation, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (à la page 33) et cliquez sur le bouton  .
2. Dans la fenêtre qui s'affiche, cliquez sur **Activer**. L'Assistant d'activation sera lancé. Suivez ses étapes pour activer l'application.
3. Dans la fenêtre **Mode d'activation**, sélectionnez le mode d'activation de l'application **Activer à l'aide du code d'activation**.
4. Dans la fenêtre **Saisie du code d'activation**, saisissez le code d'activation reçu à l'achat de Kaspersky Endpoint Security.

   Le code d'activation se présente sous la forme d'une série de chiffres et de lettres séparés par des traits d'union en 4 groupes de cinq chiffres, sans espace, par exemple : 11AA1-11AAA-1AA11-1A111. Le code doit être saisi en caractères latins.
5. Dans la fenêtre **Réception de fichier clé**, attendez pendant que l'Assistant d'activation établit la connexion avec les serveurs de Kaspersky Lab et envoie le code d'analyse pour vérification. Si le code d'activation est correct, l'Assistant obtiendra et installera le fichier clé.

   Kaspersky Endpoint Security ne reçoit pas du serveur un fichier physique avec l'extension key, mais les informations renfermées dans le système d'exploitation. Pour obtenir le fichier clé réel, il faut s'enregistrer en tant qu'utilisateur sur le site de Kaspersky Lab (http://support.kaspersky.com/fr/).

   Si le code d'activation n'est pas reconnu, un message vous le signalera. Dans ce cas, contactez la société où vous avez acheté Kaspersky Endpoint Security pour obtenir des informations.
6. Dans la fenêtre **Informations relatives au fichier clé**, l'Assistant d'activation vous informe sur la fin réussie de la procédure d'activation. De plus, vous pouvez voir les informations relatives à la clé installée : numéro de clé, type (commerciale ou évaluation) et fin de validité de la licence. Cliquez sur le bouton **Terminer** afin de quitter l'Assistant d'activation.

ACTIVATION DE L'APPLICATION A L'AIDE DU FICHIER CLE

Utilisez cette option pour activer l'application à l'aide du fichier de licence obtenu ultérieurement.

Lors de la sélection d'activation avec le fichier clé, la connexion à Internet n'est pas requise. Il est recommandé d'utiliser ce mode d'activation de l'application, si la connexion de l'ordinateur à Internet est impossible ou temporairement inaccessible.

Pour activer l'application à l'aide d'un fichier clé déjà en votre possession, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (à la page 33) et cliquez sur le bouton  .
2. Dans la fenêtre qui s'affiche, cliquez sur **Activer**. L'Assistant d'activation sera lancé. Suivez ses étapes pour activer l'application.
3. Dans la fenêtre **Mode d'activation**, choisissez le mode d'activation de l'application **Utiliser le fichier clé obtenu antérieurement**.
4. Dans la fenêtre **Sélection du fichier clé**, cliquez sur le bouton **Sélectionner** et dans la fenêtre standard, sélectionnez le fichier clé portant l'extension .key. La partie inférieure de la fenêtre reprendra les informations relatives à la licence utilisée : numéro de licence, type (commerciale ou évaluation) et date de la fin de validité de la licence.
5. Dans la fenêtre **Informations relatives au fichier clé**, l'Assistant d'activation vous informe sur la fin réussie de la procédure d'activation. De plus, vous pouvez voir les informations relatives à la clé installée : numéro de clé, type et fin de validité de la clé. Cliquez sur le bouton **Terminer** afin de quitter l'Assistant d'activation.

INTERFACE DE L'APPLICATION

Cette section contient la description des éléments de base de l'interface graphique de l'application : l'icône et le menu contextuel de l'application, la fenêtre principale, la fenêtre de configuration et les fenêtres des notifications.

DANS CETTE SECTION

ICONE KASPERSKY ENDPOINT SECURITY

L'icône de Kaspersky Endpoint Security apparaît dans la barre de menus directement après son installation. L'icône indique le fonctionnement de l'application. Si l'icône est active, cela signifie que la protection du système de fichiers de l'ordinateur contre les programmes malveillants en temps réel est activée. L'icône inactive témoigne que la protection est désactivée. En outre, le menu contextuel de l'icône assure l'accès aux commandes principales de Kaspersky Endpoint Security telles que : la désactivation ou le rétablissement de la protection du système de fichiers de l'ordinateur, le lancement des tâches de mises à jour et d'analyse rapide de l'ordinateur sur la présence de virus, le passage à la fenêtre de configuration de l'application, etc.

Par défaut, l'icône se trouve sur la barre de menus. Vous pouvez configurer l'application de telle sorte que l'icône de Kaspersky Endpoint Security apparaisse dans le Dock ou n'apparaisse pas du tout.

- *Pour sélectionner l'affichage de l'icône de l'application sur la barre de lancement rapide Dock, procédez comme suit :*

  1. Ouvrez la fenêtre de configuration de l'application (à la page 35) et sélectionnez l'onglet **Apparence** (cf. ill. ci-après).

  2. Dans le groupe **Afficher l'icône de l'application**, sélectionnez l'option **Dans le Dock**.

- *Pour désactiver l'affichage de l'icône de l'application, procédez comme suit :*

  1. Ouvrez la fenêtre de configuration de l'application (à la page 35) et sélectionnez l'onglet **Apparence** (cf. ill. ci-après).

  2. Dans le groupe **Afficher l'icône de l'application**, sélectionnez l'option **Ne pas afficher**.

N'oubliez pas que la modification de ce paramètre n'entrera en vigueur qu'après le redémarrage de Kaspersky Endpoint Security.

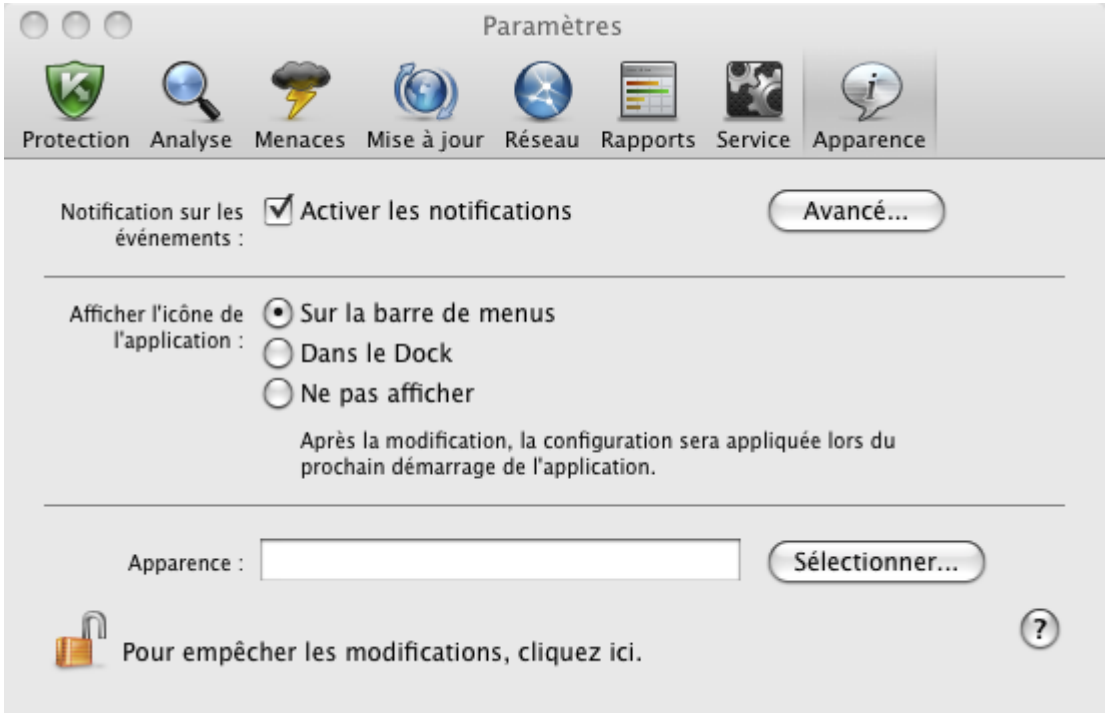


Illustration 4. Fenêtre de configuration de l'application. Apparence

Si vous avez sélectionné l'affichage de l'icône sur la barre de menus, alors lors du lancement de l'application ou lors de l'ouverture de la fenêtre principale, l'icône ne s'affiche pas dans Dock. De même, il ne sera pas possible de changer d'application en utilisant une combinaison de touches **Command-Tab**.

Si l'affichage de l'icône de l'application est désactivé, l'application est exécutée en arrière-plan. Pour ouvrir la fenêtre principale de l'application (à la page 33), il faut cliquer sur le label Kaspersky Endpoint Security dans la liste des applications installées sur l'ordinateur.

Illustration 5. Menu contextuel de l'icône de Kaspersky Endpoint Security dans la barre de menus.

Illustration 6. Menu contextuel de l'icône de Kaspersky Endpoint Security dans le Dock

FENETRE PRINCIPALE DE L'APPLICATION

- *Pour ouvrir la fenêtre principale de l'application,*

  cliquez sur l'icône Kaspersky Endpoint Security dans la barre de menus ou dans le Dock (cf. ill. ci-dessus)et dans le menu contextuel qui s'ouvre, choisissez l'option **Kaspersky Endpoint Security**.

La fonction principale de la fenêtre principale de Kaspersky Endpoint Security (cf. ill. ci-après) est d'informer l'utilisateur sur l'état de la protection de l'ordinateur et de signaler d'éventuels problèmes, ainsi que de fournir des informations sur le fonctionnement des composants de l'application (Antivirus Fichiers, analyse et mise à jour) ainsi qu'offrir un accès aux principales tâches et à la fenêtre de configuration de l'application.

Illustration 7. Fenêtre principale de Kaspersky Endpoint Security 8

Il existe trois types d'états de la protection (cf. section "Etat de la protection de l'ordinateur" à la page 43), et chacun est indiqué par une couleur identique à celle d'un feu rouge. La couleur de l'indicateur de la fenêtre principale de l'application indique l'état de la protection. Le vert indique que la protection de l'ordinateur est assurée au niveau requis. Le jaune et le rouge indique la présence de problèmes dans la configuration ou le fonctionnement de Kaspersky Endpoint Security. Pour obtenir des informations détaillées sur ces problèmes et pour les résoudre, utilisez l'Assistant de sécurité (cf. section "Assistant de sécurité" à la page 44), qui s'ouvre quand vous cliquez sur un indicateur de couleur.

La partie gauche de la fenêtre contient un texte sur l'état de la protection (explication du signal en couleur) et affiche également les menaces pour la sécurité si celles-ci ont été repérées par l'Assistant de sécurité. Si une analyse ou une mise à jour est en cours d'exécution à ce moment donné, la progression de celle-ci (exprimée en pour cent) apparaît également dans la partie gauche de la fenêtre.

La partie inférieure de la fenêtre affiche des statistiques de synthèse sur la fonction d'Antivirus Fichiers, ainsi que des informations relatives aux bases antivirus utilisées par l'application.

Vous pouvez lancer une mise à jour de Kaspersky Endpoint Security, lancer l'analyse dans les zones définies, ou passer à la gestion des licences depuis la fenêtre principale. Pour ce faire, utilisez les boutons suivants :

Lancer la mise à jour de Kaspersky Endpoint Security. A la fin d'une mise à jour, les informations détaillées sur l'exécution de la tâche seront présentées dans la fenêtre des rapports (cf. section "Rapports" à la page 98).

Passez aux tâches de recherche de virus : **Analyse express**, **Analyse complète** et **Analyse** dans la zone indiquée par l'utilisateur, et aux toutes tâches de recherche d'utilisateur, si de telles ont été créées. A la fin d'une recherche de virus, les informations détaillées sur l'exécution de la tâche seront présentées dans la fenêtre des rapports (cf. section "Rapports" à la page 98).

Passer à la fenêtre reprenant les informations sur la licence utilisée.

La partie supérieure de la fenêtre principale abrite le volet de navigation qui contient les boutons suivants :

Ouvrir la fenêtre des rapports (cf. section "Rapports" à la page 98) Kaspersky Endpoint Security, ainsi que pouvoir accéder à la quarantaine (cf. section "Quarantaine" à la page 94) et au dossier de sauvegarde (cf. section "Dossier de sauvegarde" à la page 97).

Ouvre la fenêtre de configuration de l'application (à la page 35).

Ouvrir l'aide électronique de Kaspersky Endpoint Security.

Ouvre la fenêtre contenant les informations sur les moyens d'obtenir l'assistance technique (cf. section "Contacter le Service d'assistance technique" à la page 157).

FENETRE DE CONFIGURATION DE L'APPLICATION

Les méthodes suivantes s'offrent à vous pour ouvrir la fenêtre de configuration de Kaspersky Endpoint Security (cf. ill. ci-après) :

- en cliquant sur le bouton  dans la fenêtre principale de l'application (cf. section "Fenêtre principale de l'application" à la page 33);
- en sélectionnant le point **Paramètres** dans le menu contextuel qui s'ouvre lorsque vous cliquez sur l'icône de Kaspersky Endpoint Security (à la page 31) dans Dock ou sur la barre de menus.

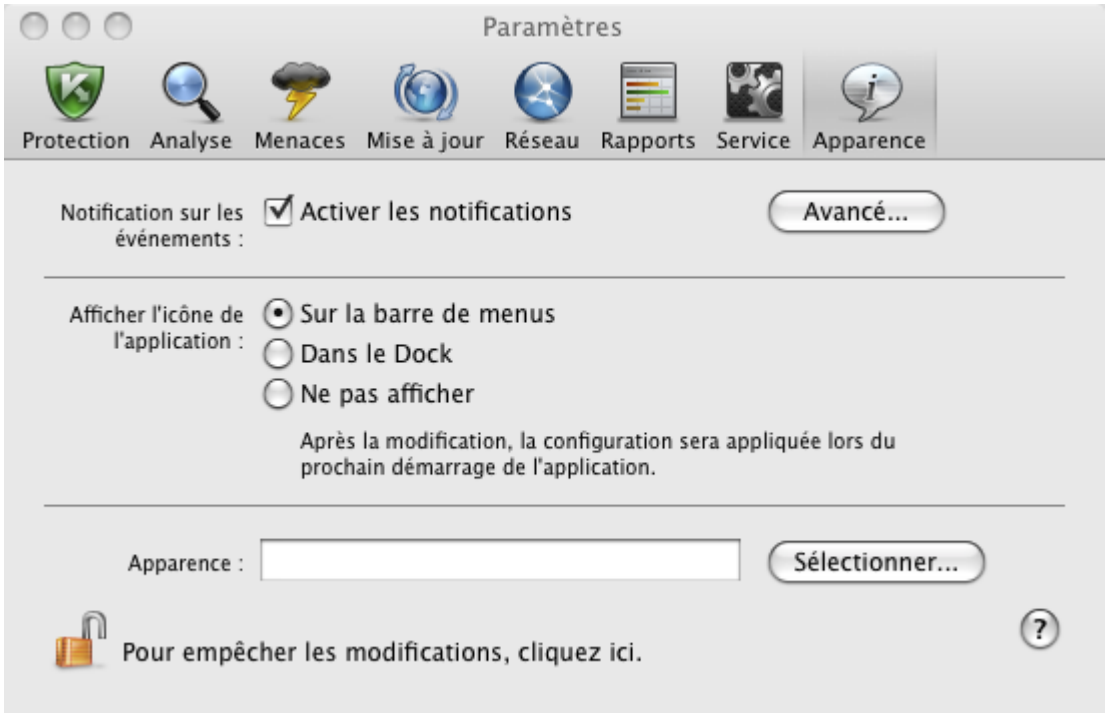


Illustration 8. Fenêtre de configuration de l'application. Apparence

Les onglets situés dans la partie supérieure de la fenêtre permettent d'accéder rapidement aux fonctions suivantes de l'application :

- configuration de l'Antivirus Fichiers ;
- configuration des tâches de recherche de virus ;
- configuration de la mise à jour de l'application ;
- sélection des applications malveillantes contrôlées et formation de la zone de confiance ;

- paramètres de service Kaspersky Endpoint Security.

La configuration détaillée de certains paramètres nécessitera l'ouverture d'une fenêtre de configuration de deuxième ou de troisième niveau.

Pour interdire la modification des paramètres de fonctionnement de Kaspersky Endpoint Security par des utilisateurs qui n'ont pas de privilèges d'administrateur, cliquez sur le bouton  situé dans la partie inférieure de la fenêtre. Dans ce cas, il faudra saisir les paramètres de l'administrateur de l'ordinateur pour pouvoir introduire des modifications.

Le bouton  permet d'accéder à l'aide de Kaspersky Endpoint Security et plus exactement à la description des paramètres de la fenêtre ouverte.

FENETRES DE NOTIFICATION ET FENETRES CONTEXTUELLES

Divers événements peuvent survenir pendant l'utilisation de Kaspersky Endpoint Security. Ils peuvent avoir un caractère informatif ou contenir les informations importantes. Par exemple, un événement peut vous signaler la réussite de la mise à jour ou indiquer une erreur de fonctionnement de l'Antivirus Fichiers ou de la tâche d'analyse qu'il faut corriger de toute urgence. Les *fenêtres de notification* et les *fenêtres contextuelles* sont les méthodes utilisées par l'application pour vous signaler les événements qui se produisent.

DANS CETTE SECTION

A PROPOS DES NOTIFICATIONS

Kaspersky Endpoint Security signale à l'utilisateur les événements des types suivants :

- **Evénements critiques** : événements critiques au sujet desquels il est vivement conseillé d'être averti, car ils indiquent un problème dans le fonctionnement de Kaspersky Endpoint Security ou une vulnérabilité dans la protection de l'ordinateur. Par exemple, *les bases de l'application sont dépassées* ou *le délai de validité de la clé est écoulé*.

- **Refus de fonctionnement** : événements qui empêchent le fonctionnement de Kaspersky Endpoint Security : par exemple, *les bases de l'application sont corrompues*.

- **Evénements importants** : événements auxquels il faut absolument prêter attention, car ils indiquent une situation importante dans le fonctionnement de Kaspersky Endpoint Security. Par exemple, *protection désactivée* ou *l'analyse antivirus de l'ordinateur a été réalisée il y a longtemps*.

- **Événements informatifs** : événements à caractère informatif, par exemple : *tous les objets dangereux ont été réparés*.

Si vous souhaitez être informé de ce qui se passe pendant le fonctionnement de Kaspersky Endpoint Security, utilisez le service de notification.

MOENS DE RECEPTION DES NOTIFICATIONS

Les notifications peuvent être réalisées par un des moyens suivants ou par les deux en même temps :

- Fenêtre contextuelle ;
- Notification sonore.

Kaspersky Endpoint Security est compatible avec la technologie Growl pour l'affichage des notifications. Si le système Growl est activé, les messages s'affichent sur l'écran en utilisant cette technologie.

CONFIGURATION DE RECEPTION DES NOTIFICATIONS

Pour recevoir les notifications sur les événements, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (à la page 35) et sélectionnez l'onglet **Apparence** (cf. ill. ci-après).

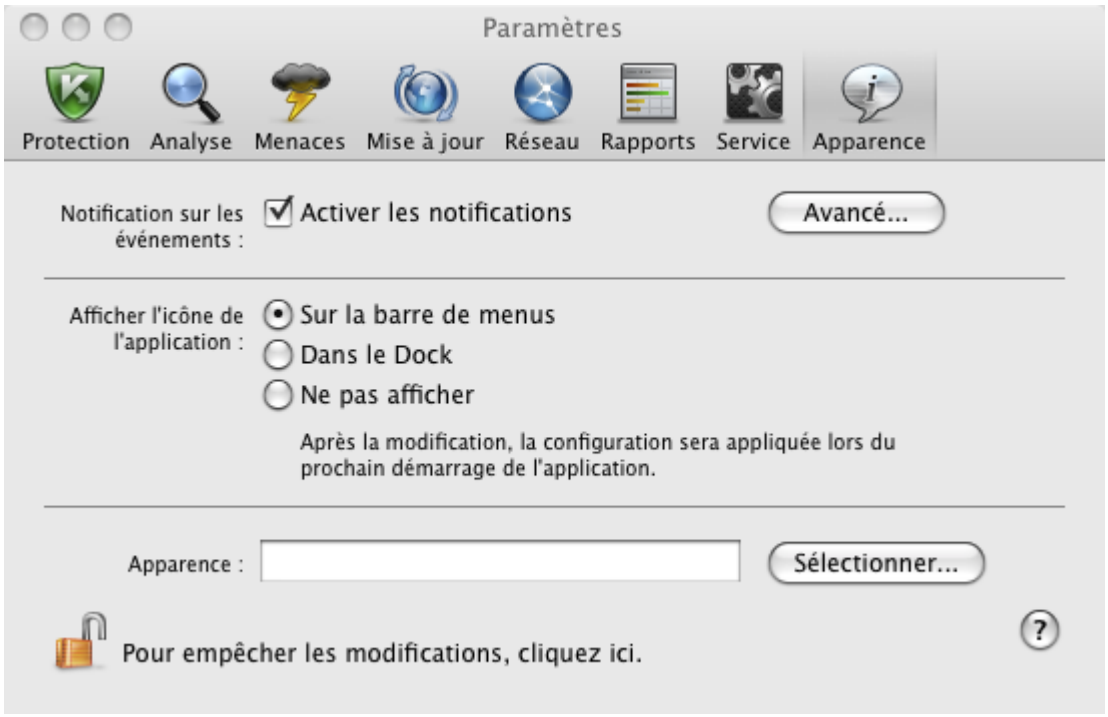


Illustration 9. Fenêtre de configuration de l'application. Apparence

2. Cochez la case **Activer les notifications** dans le groupe **Notifications sur les événements** et passez à la configuration détaillée. Pour ce faire, cliquez sur **Avancé**.

La fenêtre qui s'ouvre (cf. ill. ci-après) vous permet de configurer les modes suivants d'envoi des notifications sur les événements mentionnés ci-dessus :

- *Fenêtre contextuelle*, contenant des informations sur l'événement survenu.

  Pour utiliser ce type de notification, cochez la case dans la colonne **Ecran** en regard des événements au sujet desquels vous souhaitez être alerté.

- *Notification sonore*.

Si vous voulez accompagner cette infobulle d'un effet sonore, cochez la case **Son** en regard de l'événement.

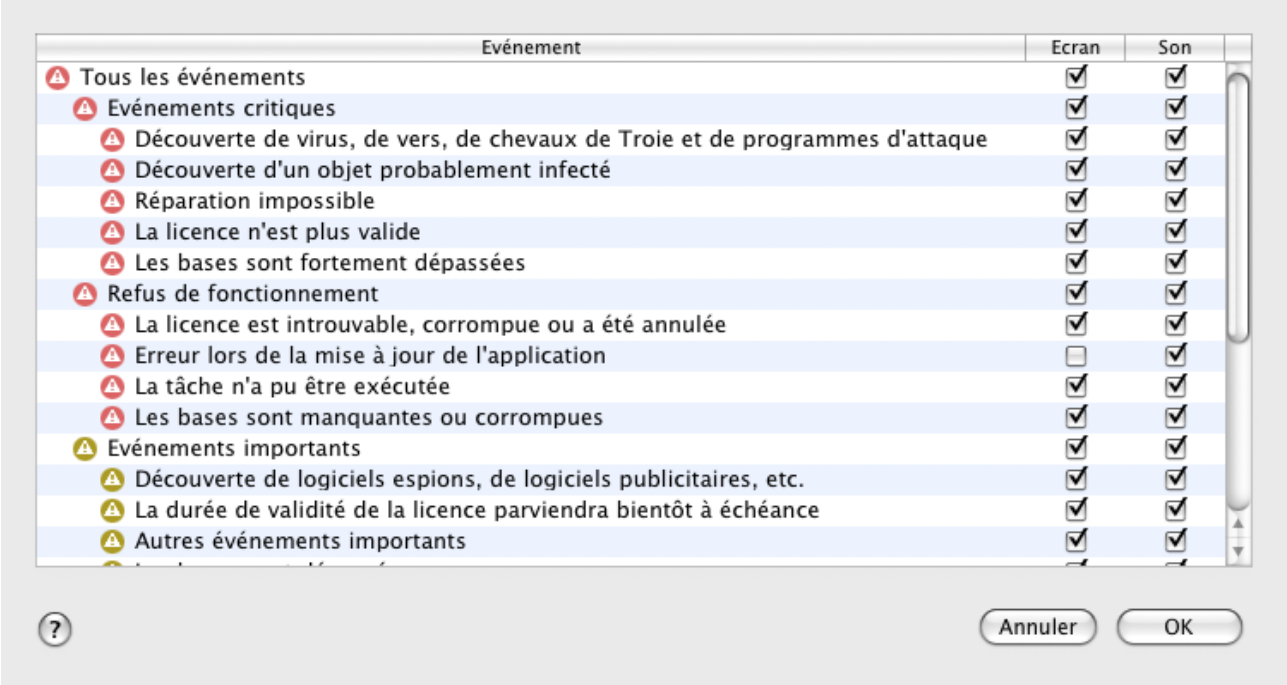


Illustration 10. Configuration de réception des notifications

PRESENTATION DES FENETRES CONTEXTUELLES

Kaspersky Endpoint Security utilise des *fenêtres contextuelles* pour signaler les événements qui ne requièrent pas nécessairement une intervention de l'utilisateur. Les fenêtres contextuelles apparaissent sous l'icône de l'application dans la barre de menus et disparaissent automatiquement après un certain temps.

CONFIGURATION DE L'INTERFACE DE KASPERSKY ENDPOINT SECURITY

Vous pouvez également modifier l'apparence de Kaspersky Endpoint Security en créant et en utilisant divers éléments graphiques et la palette de couleurs. Toutes les couleurs, polices de caractères, images et textes utilisés dans l'interface de l'application peuvent être modifiés.

➡ *Pour activer l'apparence, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application (à la page 35) et sélectionnez l'onglet **Apparence** (cf. ill. ci-après).

2. Dans le groupe **Apparence**, cliquez sur le bouton **Sélectionner** et dans la fenêtre standard ouverte, sélectionnez le dossier contenant les fichiers de l'environnement graphique.

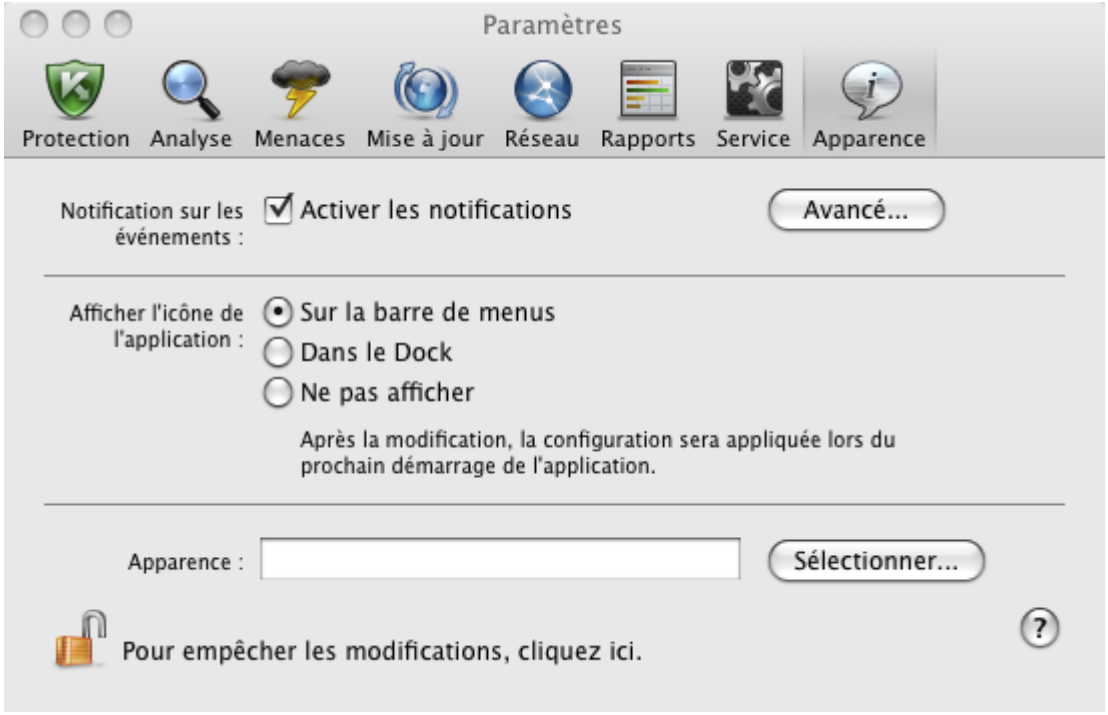


Illustration 11. Fenêtre de configuration de l'application. Apparence

LANCEMENT ET ARRET DE L'APPLICATION

Cette rubrique explique comment lancer et arrêter l'application.

L'application est lancée automatiquement après l'installation et l'icône de Kaspersky Endpoint Security (cf. page 31) apparaît dans la barre de menus.

DANS CETTE SECTION

ARRET DE KASPERSKY ENDPOINT SECURITY

Si pour une raison quelconque, vous devez complètement arrêter Kaspersky Endpoint Security, cliquez sur l'icône de Kaspersky Endpoint Security (à la page 31) sur la barre de menus Mac OS ou dans Dock, et dans le menu qui s'ouvre, sélectionnez la commande **Quitter**. Le fonctionnement de l'application sera arrêté et le processus sera supprimé depuis la mémoire vive de l'ordinateur.

Quand Kaspersky Endpoint Security est arrêté, l'ordinateur continue à fonctionner sans protection et il risque d'être infecté.

CONFIGURATION DU LANCEMENT AUTOMATIQUE DE KASPERSKY ENDPOINT SECURITY

Par défaut, Kaspersky Endpoint Security est lancé automatiquement au démarrage de l'ordinateur ou après le redémarrage du système d'exploitation.

Pour activer le mode de démarrage, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (à la page 35) sélectionnez l'onglet **Service** (cf. ill. ci-après).

2. Dans le groupe **Chargement automatique**, décochez la case **Lancer l'application au démarrage de l'ordinateur**.

Illustration 12. Fenêtre de configuration de l'application. Service

Si vous désactivez le mode de lancement automatique de Kaspersky Endpoint Security, alors après le prochain démarrage de l'ordinateur ou redémarrage du système d'exploitation, votre ordinateur ne sera plus protégé et il risque d'être infecté.

CONFIGURATION DU MODE D'ECONOMIE DE LA CONSOMMATION ELECTRIQUE

Par défaut, Kaspersky Endpoint Security fonction en mode d'économie de la consommation électrique. Dans ce mode, les tâches d'analyse dont le lancement est programmé ne seront pas exécutées si l'ordinateur est alimenté par la batterie.

Pour désactiver le mode d'économie de la consommation électrique, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (à la page 35) sélectionnez l'onglet **Service** (cf. ill. ci-après).

2. Dans le groupe **Batterie**, décochez la case **Ne pas lancer les tâches prévues si le portable est débranché**.

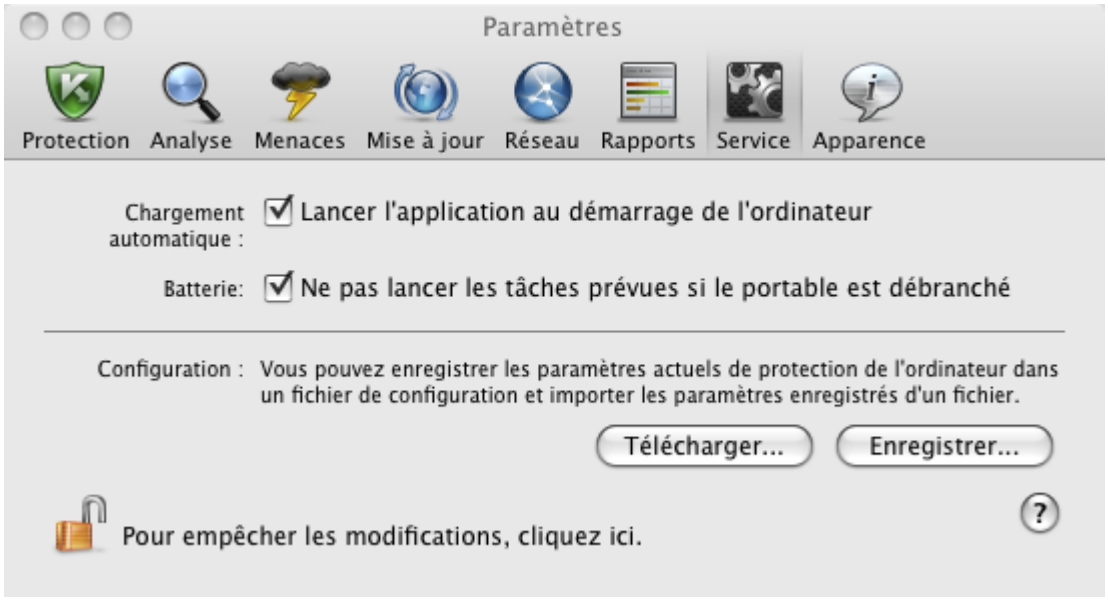


Illustration 13. Fenêtre de configuration de l'application. Service

ETAT DE LA PROTECTION DE L'ORDINATEUR

L'état de la protection de votre ordinateur reflète la présence ou l'absence de menaces qui influencent le niveau général de sécurité du système. Dans ce cas, les menaces sont non seulement les programmes malveillants découverts, mais aussi l'utilisation de bases antivirus dépassées, la désactivation de l'Antivirus Fichiers, l'utilisation des paramètres minimum de fonctionnement de Kaspersky Endpoint Security.

L'Assistant de sécurité aidera à examiner les menaces existantes et à les éliminer.

DANS CETTE SECTION

EVALUATION DE L'ETAT DE LA PROTECTION DE L'ORDINATEUR

L'état de la protection de l'ordinateur est affiché dans la fenêtre principale de l'application (cf. section "Fenêtre principale de l'application" à la page 33) et il est exprimé par des couleurs identiques à celles des feux de circulation. La couleur de l'indicateur change en fonction de la situation. Si une menace est présente dans le système, l'indicateur de couleur sera accompagné d'un texte d'informations.

L'indice de couleur peut prendre une des valeurs suivantes :

- **Vert**. La protection de l'ordinateur est assurée au niveau adéquat.

  Cet état indique que vous avez actualisé les bases antivirus en temps voulu, que l'Anti-Virus Fichiers est activé, que Kaspersky Endpoint Security fonctionne selon les paramètres recommandés par les spécialistes de Kaspersky Lab et que l'analyse complète de l'ordinateur n'a décelé aucun objet malveillant ou que les objets malveillants découverts ont été neutralisés.

- **Jaune**. Le niveau de protection de votre ordinateur est inférieur au niveau précédent.

  Il y a plusieurs problèmes au niveau du fonctionnement ou de la configuration de Kaspersky Endpoint Security. Par exemple, l'écart par rapport au mode de fonctionnement recommandé est négligeable, les bases de Kaspersky Endpoint Security n'ont pas été mises à niveau pendant quelques jours.

- **Rouge**. Votre ordinateur est exposé à un risque d'infection.

  Cet état signale l'existence de problèmes qui pourraient entraîner l'infection de l'ordinateur ou la perte de données. Par exemple, une erreur s'est produite dans le fonctionnement de l'Antivirus Fichiers, Kaspersky Endpoint Security n'a plus été actualisée depuis longtemps, des programmes malveillants qu'il faut absolument neutraliser ont été découverts ou l'application n'est pas activée.

Il est conseillé de résoudre les problèmes du système de protection dès qu'ils se présentent. Pour ce faire, cliquer sur l'indice de couleur de la fenêtre principale pour lancer l'Assistant de sécurité (à la page 44).

ASSISTANT DE SECURITE

L'Assistant de sécurité est un service permettant d'analyser les menaces existantes et de passer à leur suppression immédiate (cf. ill. ci-après).

Pour lancer l'Assistant de sécurité,

cliquez sur l'indicateur de couleur de la fenêtre principale de l'application (cf. section "Fenêtre principale de l'application" à la page 33).

Illustration 14. Interface de l'Assistant de sécurité

Pour prendre connaissance de la liste des menaces existantes, cliquez sur les boutons **Poursuivre** et **Précédent**. Chaque menace est accompagnée d'une description et les actions suivantes sont proposées :

- **Supprimer la menace immédiatement**.

  Pour supprimer une menace, cliquez sur le bouton reprenant le nom de l'action recommandée. Par exemple, si des objets infectés ont été découverts sur l'ordinateur, alors l'action **Réparer les objets infectés** est recommandée. Si les bases antivirus sont dépassées, alors l'action **Mettre à jour les bases** est recommandée. Les informations détaillées sur la menace sont présentes dans la fenêtre des rapports (cf. section "Rapports" à la page 98).

- **Reporter la suppression d'une menace**.

  Si pour une raison quelconque vous ne voulez pas supprimer la menace directement, reportez cette action à plus tard. Pour ce faire, cliquez sur **Reporter**. N'oubliez pas que cette option n'est pas disponible pour les menaces sérieuses telles que la présence d'objets malveillants non réparés, un échec de fonctionnement de l'Antivirus Fichiers ou l'endommagement des fichiers des bases de Kaspersky Endpoint Security.

Si vous avez terminé le fonctionnement de l'Assistant de sécurité sans exclure des menaces sérieuses, la couleur de l'indice dans la fenêtre principale vous avertira des problèmes de sécurité. Si vous avez reporté l'exclusion de certaines menaces, alors lors de l'ouverture réitérée de l'Assistant de sécurité, les menaces reportées ne seront pas présentes dans la liste des menaces actives. Néanmoins, vous pouvez revenir à l'examen et à la suppression des anciennes menaces en cliquant sur le bouton **Consulter les menaces reportées** dans la dernière fenêtre de l'Assistant de sécurité.

RESOLUTION DES PROBLEMES TYPES

Cette section contient une description des tâches auxquelles est confrontée la majorité des utilisateurs lors de l'utilisation de l'application et les instructions pour les exécuter.

DANS CETTE SECTION

PROCEDURE D'EXECUTION D'UNE ANALYSE COMPLETE DE L'ORDINATEUR

La tâche d'analyse complète (créée par défaut) de l'ordinateur fait partie de Kaspersky Endpoint Security. Dans le cadre de cette tâche, l'application recherche la présence éventuelle de virus sur tous les disques durs.

Pour lancer la tâche d'analyse complète de l'ordinateur, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (à la page 33) et cliquez sur le bouton  .
2. Dans la fenêtre ouverte, sélectionnez la tâche  **Analyse complète**.

Les résultats de l'exécution de la tâche seront affichés dans la fenêtre des rapports (cf. section "Statistiques de la recherche de virus" à la page 82).

REALISATION D'UNE ANALYSE RAPIDE DE L'ORDINATEUR

La tâche d'analyse rapide (créée par défaut) de l'ordinateur fait partie de Kaspersky Endpoint Security. Dans le cadre de cette tâche, l'application recherche la présence éventuelle de virus dans les secteurs critiques de l'ordinateur, dans les dossiers contenant les fichiers du système d'exploitation et les bibliothèques système dont l'infection par des programmes malveillants pourrait endommager le système d'exploitation de l'ordinateur.

Pour lancer la tâche d'analyse rapide de l'ordinateur, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (à la page 33) et cliquez sur le bouton  .
2. Dans la fenêtre ouverte, sélectionnez la tâche  **Analyse express**.

Les résultats de l'exécution de la tâche seront affichés dans la fenêtre des rapports (cf. section "Statistiques de la recherche de virus" à la page 82).

COMMENT RECHERCHER D'EVENTUELS VIRUS DANS UN FICHIER, UN REPERTOIRE OU UN DISQUE

Si vous devez rechercher la présence éventuelle de virus dans un objet distinct (un des disques durs, un dossier ou un fichier en particulier ou un périphérique amovible), utilisez la tâche préconfigurée **Analyse**.

Pour rechercher la présence d'éventuels virus dans un objet en particulier, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (à la page 33) et cliquez sur le bouton  .
2. Dans le menu qui s'ouvre, sélectionnez la tâche  **Analyse**. La fenêtre de sélection des objets d'analyse s'ouvrira.
3. Formez la liste des objets d'analyse (cf. section "Composition de la liste des objets à analyser" à la page 72) et cliquez sur le bouton **Démarrer** pour démarrer une tâche de recherche de virus.

Les résultats de l'exécution de la tâche seront affichés dans la fenêtre des rapports (cf. section "Statistiques de la recherche de virus" à la page 82).

La recherche d'éventuels virus dans n'importe quel objet de votre ordinateur peut être lancée depuis le Finder, pour autant que le composant **Menu contextuel Finder** (cf. section "**Installation personnalisée de Kaspersky Endpoint Security**" à la page 22) ait été installé. Pour ce faire, ouvrez le menu contextuel de l'objet et choisissez l'option **Rechercher d'éventuels virus**[1].

PLANIFICATION DE L'ANALYSE DE L'ORDINATEUR

L'analyse opportune de votre ordinateur est le garant de la sécurité des données. Vous pouvez programmer le lancement des tâches de recherche de virus **Analyse express** et **Analyse complète**. Conformément au mode indiqué, l'application lancera automatiquement la tâche et exécutera l'analyse de tout l'ordinateur et des zones les plus critiques du système de fichiers.

*Pour programmer le lancement des tâches **Analyse express** et **Analyse complète**, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application (à la page 35) et sélectionnez l'onglet **Analyse**.

[1] Le lancement peut être différent sous les systèmes d'exploitation Mac OS X de version en dessous 10.6.

2. Dans la liste de gauche, sélectionnez le nom de la tâche, puis dans le groupe **Mode d'exécution**, activez le lancement de la tâche programmée. Pour modifier les horaires du lancement de la tâche, cliquez sur le bouton **Modifier**.

3. Dans la fenêtre ouverte, indiquez la fréquence de lancement de la tâche de recherche de virus.

Les résultats de l'exécution des tâches seront affichés dans la fenêtre des rapports (cf. section "Statistiques de la recherche de virus" à la page 82).

PROCEDURE D'ACHAT OU DE RENOUVELLEMENT DE LA LICENCE

Si vous avez installé Kaspersky Endpoint Security sans licence, vous pourrez acheter celle-ci après l'installation de l'application. Quand la durée de validité de la licence approche de son échéance, vous pouvez la renouveler. Lors de l'achat de la licence et du son renouvellement, vous recevez le code d'activation qui vous permet d'activer l'application (cf. section "Activation de Kaspersky Endpoint Security" à la page 28).

- *Pour acheter une licence, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application (à la page 33) et cliquez sur le bouton  .

2. Dans la fenêtre qui s'affiche, cliquez sur **Acheter**.

   La page de la boutique en ligne où vous pouvez acheter la licence s'ouvre.

- *Pour renouveler une licence, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application (à la page 33) et cliquez sur le bouton  .

2. Dans la fenêtre qui s'affiche, cliquez sur **Renouveler**.

   La page Web de la boutique en ligne où vous pouvez renouveler la licence s'ouvrira.

PROCEDURE DE MISE A JOUR DES BASES ET DES MODULES DE L'APPLICATION

Kaspersky Lab actualise les bases antivirus et les modules de Kaspersky Endpoint Security par des serveurs de mises à jour spéciaux et le Serveur d'administration Kaspersky Administration Kit. *Les serveurs de mises à jour de Kaspersky Lab* sont les sites Internet que Kaspersky Lab utilise pour diffuser régulièrement les mises à jour de Kaspersky Endpoint Security.

Pour réussir le téléchargement des mises à jour depuis les serveurs, la connexion de l'ordinateur à Internet est requise.

Par défaut, Kaspersky Endpoint Security recherche périodiquement la présence du paquet des mises à jour sur les serveurs de Kaspersky Lab. Lorsque Kaspersky Endpoint Security découvre de nouvelles mises à jour, il les télécharge en arrière-plan et les installe sur l'ordinateur.

- *Pour lancer manuellement la mise à jour de Kaspersky Endpoint Security,*

  ouvrez la fenêtre principale de l'application (à la page 33) et cliquez sur le bouton  .

Les résultats de l'exécution de la tâche de mise à jour seront affichés dans la fenêtre des rapports (cf. section "Statistiques de la mise à jour" à la page 92).

PROCEDURE DE TRANSFERT DES PARAMETRES DE L'APPLICATION DANS UNE VERSION DE KASPERSKY ENDPOINT SECURITY INSTALLE SUR UN AUTRE ORDINATEUR

Kaspersky Endpoint Security vous permet d'exporter et d'importer les paramètres de fonctionnement. Cela est utile si vous avez installé l'application sur un ordinateur chez vous et au bureau. Vous pouvez configurer l'application selon un mode qui vous convient pour le travail à domicile, conserver ces paramètres sur le disque et les importer rapidement sur votre ordinateur au travail. Les paramètres sont enregistrés dans un fichier de configuration spécial.

- *Pour enregistrer les paramètres actuels de fonctionnement de Kaspersky Endpoint Security dans un fichier, procédez comme suit :*

  1. Ouvrez la fenêtre de configuration de l'application (à la page 35) et sélectionnez l'onglet **Service**.
  2. Dans le groupe **Configuration**, cliquez sur le bouton **Enregistrer**. La fenêtre **Enregistrer** s'ouvrira.
  3. Dans le champ **Enregistrer sous**, saisissez le nom du fichier et sélectionnez le dossier où il sera enregistrer.

- *Pour importer les paramètres de fonctionnement de Kaspersky Endpoint Security depuis le fichier de configuration, procédez comme suit :*

  1. Ouvrez la fenêtre de configuration de l'application (à la page 35) et sélectionnez l'onglet **Service**.
  2. Dans le groupe **Configuration**, cliquez sur le bouton **Télécharger** et dans la fenêtre standard ouverte sélectionnez le fichier contenant les paramètres de Kaspersky Endpoint Security.

QUE FAIRE SI L'APPLICATION A BLOQUEE L'ACCES AU FICHIER

Kaspersky Endpoint Security bloque l'accès au fichier ou au programme si l'Antivirus Fichiers (cf. page 56) soupçonne l'objet sollicité d'être infecté ou potentiellement infecté par une application malveillante et si l'action **Bloquer l'accès** a été sélectionnée.

- *Pour traiter les objets dangereux repris sous l'onglet **Détectés** de la fenêtre des rapports, procédez comme suit :*

  1. Ouvrez la fenêtre principale de l'application (à la page 33) et cliquez sur le bouton  . La fenêtre des rapports de Kaspersky Endpoint Security s'ouvre.
  2. Dans la partie gauche de la fenêtre des rapports, sélectionnez **Détectés**. La liste des objets dangereux détectés avec leurs états sera affichée dans la partie droite de la fenêtre.
  3. Cliquez sur le bouton **Réparer tous**. Le traitement de chaque objet s'accompagne d'un message qui vous permet de choisir les actions ultérieures à appliquer à cet objet. Si vous cochez la case **Appliquer à tous les cas similaires** dans le message, alors l'action sélectionnée sera appliquée à tous les objets au statut identique.

- *Pour traiter les objets potentiellement infectés placés en quarantaine, procédez comme suit :*

  1. Ouvrez la fenêtre principale de l'application (à la page 33) et cliquez sur le bouton  . La fenêtre des rapports de Kaspersky Endpoint Security s'ouvre.
  2. Dans la partie gauche de la fenêtre des rapports, sélectionnez **Quarantaine**. La partie droite de la fenêtre affichera le contenu de la quarantaine.

3. Cliquez sur le bouton **Analyser tout** pour analyser et réparer tous les objets potentiellement infectés de la quarantaine en utilisant la version actuelle des bases de Kaspersky Endpoint Security.

4. Cliquez sur le bouton **Restaurer** pour restaurer les fichiers dans le dossier défini par l'utilisateur, ou le dossier depuis lequel ils ont été déplacés dans la quarantaine (par défaut).

   Nous vous conseillons de restaurer uniquement les objets dont l'état correspond à *faux positif*. La restauration d'autres types d'objets pourrait entraîner l'infection de votre ordinateur.

5. Cliquez sur le bouton **Supprimer** ou **Purger tout** afin de supprimer l'objet sélectionné de la quarantaine ou de purger complètement la quarantaine.

Si vous êtes convaincu que les objets bloqués par l'Antivirus Fichiers ne présentent aucun danger, vous pouvez les ajouter à la zone de confiance en créant une règle d'exclusion (cf. section "Constitution de la zone de confiance" à la page 53).

QUE FAIRE SI VOUS PENSEZ QUE L'OBJET EST INFECTE PAR UN VIRUS

Si vous pensez qu'un objet est infecté, soumettez-le à la recherche de la présence éventuelle de virus (cf. section "Comment rechercher d'éventuels virus dans un fichier, un répertoire ou un disque" à la page 46).

Si Kaspersky Endpoint Security signale à l'issue de l'analyse que l'objet est sain, mais que vous pensez le contraire, placez-le en *quarantaine*. Les objets placés en quarantaine sont compactés et ne présentent aucune menace pour votre ordinateur. Il se peut, après la mise à jour des bases, que Kaspersky Endpoint Security puisse identifier la menace et la supprimer.

➧ *Pour placer l'objet en quarantaine, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application (à la page 33) et cliquez sur le bouton  . La fenêtre des rapports de Kaspersky Endpoint Security s'ouvre.

2. Dans la partie gauche de la fenêtre des rapports, sélectionnez **Quarantaine**. La partie droite de la fenêtre affichera le contenu de la quarantaine.

3. Cliquez sur le bouton **Ajouter** et sélectionnez le fichier souhaité dans la fenêtre standard ouverte. Il sera ajouté à la liste sous le signe *ajouté par l'utilisateur*.

PROCEDURE DE RESTAURATION D'UN OBJET SUPPRIME OU REPARE PAR L'APPLICATION

Il est déconseillé, sauf urgence, de restaurer les objets supprimés et réparés car ils pourraient constituer une menace pour votre ordinateur.

Il n'est pas toujours possible de préserver l'intégrité des objets infectés lors de la réparation. Si le fichier réparé contenait des informations importantes et que celles-ci ne sont plus accessibles (complètement ou partiellement) suite à la réparation, il est possible de le restaurer à partir de sa copie de sauvegarde.

➧ *Pour restaurer un objet supprimé ou modifié lors de la réparation, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application (à la page 33) et cliquez sur le bouton  . La fenêtre des rapports de Kaspersky Endpoint Security s'ouvre.

2. Dans la partie gauche de la fenêtre des rapports, sélectionnez **Dossier de sauvegarde**. La partie droite de la fenêtre présente le contenu de la sauvegarde sous forme de la liste des copies de sauvegarde des objets.

3. Sélectionnez la copie de sauvegarde de l'objet nécessaire dans la liste et cliquez sur le bouton **Restaurer**. Confirmez l'action dans la fenêtre ouverte. L'objet sera restauré dans l'emplacement d'origine avec le même nom qu'avant la réparation ou la suppression. Si l'emplacement d'origine contient un objet portant le même nom (cette situation est possible en cas de restauration d'un objet dont la copie avait déjà été créée avant la réparation), un avertissement apparaîtra à l'écran. Vous pouvez modifier l'emplacement de l'objet restauré ainsi que son nom.

   Nous recommandons d'analyser les objets tout de suite après la restauration. Il sera possible de le réparer avec les bases antivirus les plus récentes tout en préservant son intégrité.

EMPLACEMENT DU RAPPORT SUR LE FONCTIONNEMENT DE L'APPLICATION

Les informations relatives aux événements survenus pendant le fonctionnement de l'Antivirus Fichiers (cf. section "Antivirus Fichiers" à la page 56), lors de l'exécution des tâches de recherche de virus (cf. section "Analyse" à la page 68) ou de la mise à jour (cf. section "Mise à jour de l'application" à la page 84) s'affichent dans la fenêtre des rapports (cf. section "Rapports" à la page 98).

- *Pour ouvrir la fenêtre des rapports,*

  ouvrez la fenêtre principale de l'application (à la page 33) et cliquez sur le bouton  .

QUE FAIRE EN CAS D'AFFICHAGE DE NOTIFICATIONS

Les notifications de l'application (cf. section "Fenêtres de notifications et fenêtres contextuelles" à la page 36) sous la forme de fenêtre de notification contextuelle signalent les événements qui surviennent pendant l'utilisation de l'application et qui requièrent votre attention.

Quand un tel message apparaît, il faut sélectionner une des actions proposées. La version optimale, à savoir celle recommandée par les experts de Kaspersky Lab, est choisie par défaut.

CONFIGURATION ETENDUE DE L'APPLICATION

Cette section contient des informations détaillées sur chacun des composants de l'application et une description de l'algorithme de fonctionnement et de la configuration des paramètres du composant.

DANS CETTE SECTION

CONSTITUTION DE LA ZONE DE PROTECTION

La zone de protection de l'ordinateur est formée à l'aide de la configuration des paramètres suivants :

- la liste des programmes malveillants, contre lesquels l'application assure la protection ;
- les objets de la zone de confiance qui seront exclus de la protection.

DANS CETTE SECTION

SELECTION DES PROGRAMMES MALVEILLANTS CONTROLES

Kaspersky Endpoint Security vous protège contre divers types de programmes malveillants. Quelle que soit la configuration de l'application, votre ordinateur sera protégé contre les types de programmes malveillants les plus dangereux tels que les virus, les chevaux de Troie et les outils de piratage. Il s'agit des programmes qui peuvent occasionner les dégâts les plus graves. Pour offrir une plus grande sécurité de votre ordinateur, vous pouvez élargir la liste des menaces à identifier en activant le contrôle d'un autre type de programme présentant un risque potentiel.

Les programmes malveillants et indésirables contre lesquels Kaspersky Endpoint Security vous protège sont regroupés de la manière suivante :

- **Virus, vers, chevaux de Troie et utilitaires d'attaque**. Ce groupe reprend les programmes malveillants les plus répandus et les plus dangereux. Cette protection est le niveau minimum admissible. Sur la recommandation des experts de Kaspersky Lab, Kaspersky Endpoint Security surveille toujours ce groupe de programmes malveillants.
- **Logiciel espions et publicitaires**. Ce groupe reprend les applications indésirables qui peuvent nuire à l'utilisateur ou entraîner de dommages.

- **Numéroteurs**. Ce groupe inclut les applications qui établissent des liaisons téléphoniques par modem en mode masqué (y compris les numéroteurs vers les services téléphoniques pornographiques).

- **Autres applications**. Ce groupe reprend les logiciels qui ne sont pas malveillants ou dangereux, mais qui dans certaines circonstances peuvent nuire à votre ordinateur.

Pour sélectionner du groupe le programme malveillant, contre lequel Kaspersky Endpoint Security va protéger votre ordinateur, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (à la page 35) et sélectionnez l'onglet **Menaces** (cf. ill. ci-après).

2. Cochez, dans le groupe **Catégories de programmes malicieux**, la case en regard des groupes de programmes malveillants contre lesquels Kaspersky Endpoint Security doit protéger l'ordinateur.

Kaspersky Endpoint Security assure toujours la protection de votre ordinateur contre les virus, les vers, les chevaux de Troie et les utilitaires d'attaque. Pour cette raison, il est impossible de décocher la case à côté de ce groupe.

Selon les groupes sélectionnés, Kaspersky Endpoint Security va utiliser entièrement ou partiellement les bases antivirus lors du fonctionnement de l'Antivirus Fichiers (cf. section "Antivirus Fichiers" à la page 56) et lors de la recherche de virus (cf. section "Analyse" à la page 68).

Si tous les groupes de programmes malveillants ont été sélectionnés, la protection de l'ordinateur offerte par Kaspersky Endpoint Security est à son niveau maximum. Si la protection uniquement contre les virus, les vers, les chevaux de Troie et les utilitaires d'attaque a été sélectionnée, Kaspersky Endpoint Security n'analyse pas les programmes indésirables et d'autres programmes malveillants qui peuvent être installés sur votre ordinateur et qui peuvent amener des dégâts moraux ou matériels.

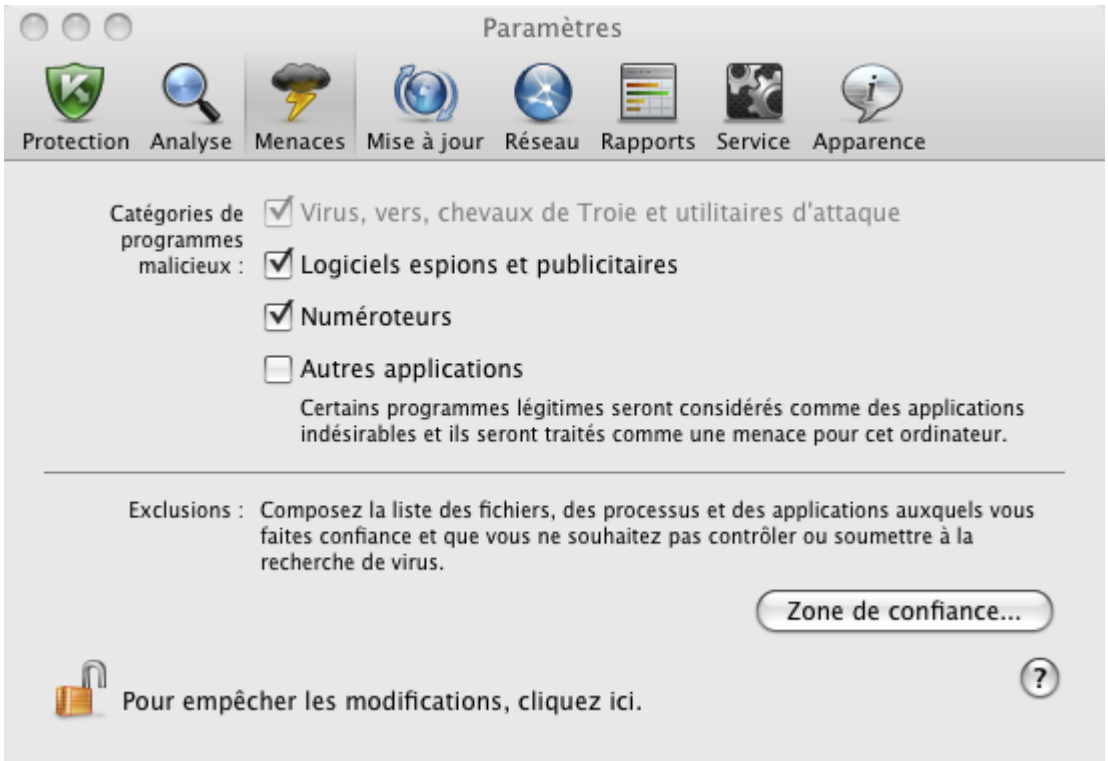


Illustration 15. Fenêtre de configuration de l'application. Menaces

Les experts de Kaspersky Lab vous recommandent de ne pas désactiver le contrôle des logiciels espions, adwares et numéroteurs automatiques. Lorsque Kaspersky Endpoint Security considère un programme qui d'après vous n'est pas dangereux comme un programme de cette catégorie, il est conseillé de configurer une règle d'exclusion (cf. section "Constitution de la zone de confiance" à la page 53).

CONSTITUTION DE LA ZONE DE CONFIANCE

La *Zone de confiance* est en réalité une liste d'objets composée par l'utilisateur. Ces objets seront ignorés par Kaspersky Endpoint Security.

Cette zone de confiance peut être définie par l'utilisateur, sur la base des particularités des objets qu'il manipule et des programmes installés sur l'ordinateur. La constitution de cette liste d'exclusions peut s'avérer utile si Kaspersky Endpoint Security bloque l'accès à un objet ou un programme quelconque, alors que vous êtes convaincu que celui-ci est tout à fait sain.

Les règles d'exclusions sont des ensembles de conditions qui permettent à Kaspersky Endpoint Security de savoir qu'il ne doit pas analyser un objet. Vous pouvez exclure de l'analyse des fichiers de format défini (cf. section "Liste des objets analysés en fonction de l'extension" à la page 159), des fichiers selon un masque (cf. section "Masques autorisés pour l'exclusion des fichiers" à la page 161), certains secteurs (par exemple, un répertoire ou un programme), des processus ou des objets selon un type de menace conforme à la classification de l'Encyclopédie des virus (http://www.securelist.com/fr/).

Les objets exclus ne seront pas analysés lors de l'analyse du disque ou du dossier où ils se trouvent. Toutefois, en cas de sélection de l'analyse de cet objet précis, la règle d'exclusion ne sera pas appliquée.

Type de menace : est l'état assigné par Kaspersky Endpoint Security à un objet au cours de l'analyse. Le type de menace est rendu sur la base du classement des programmes malveillants et indésirables présentés dans l'encyclopédie des virus de Kaspersky Lab.

Les programmes indésirables n'ont aucune fonction malicieuse, mais ils peuvent être exploités par un individu malintentionné en guise de soutien à un programme malicieux, en raison des failles ou des erreurs qu'il contient. Cette catégorie regroupe par exemple les programmes d'administration à distance, les clients IRC, les serveurs FTP, tous les utilitaires pour l'arrêt des processus ou la dissimulation de leur activité, les enregistreurs de frappes, les programmes d'identification des mots de passe, les numéroteurs automatiques vers des sites payants. Ce genre de programme n'est pas considéré comme un virus (not-a-virus). Mais il peut être malgré tout scindé entre les types Adware, Joke, Riskware, etc. (pour en savoir plus sur les programmes indésirables détectés par Kaspersky Endpoint Security, consultez l'Encyclopédie des virus (http://www.securelist.com/fr)). Ces programmes peuvent être bloqués suite à l'analyse. Sachant que certains d'entre eux sont largement utilisés, il est possible de les exclure de l'analyse.

Pour créer une nouvelle règle d'exclusion ou consulter et modifier les règles d'exclusion déjà créées, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (à la page 35) et sélectionnez l'onglet **Menaces** (cf. ill. ci-après).

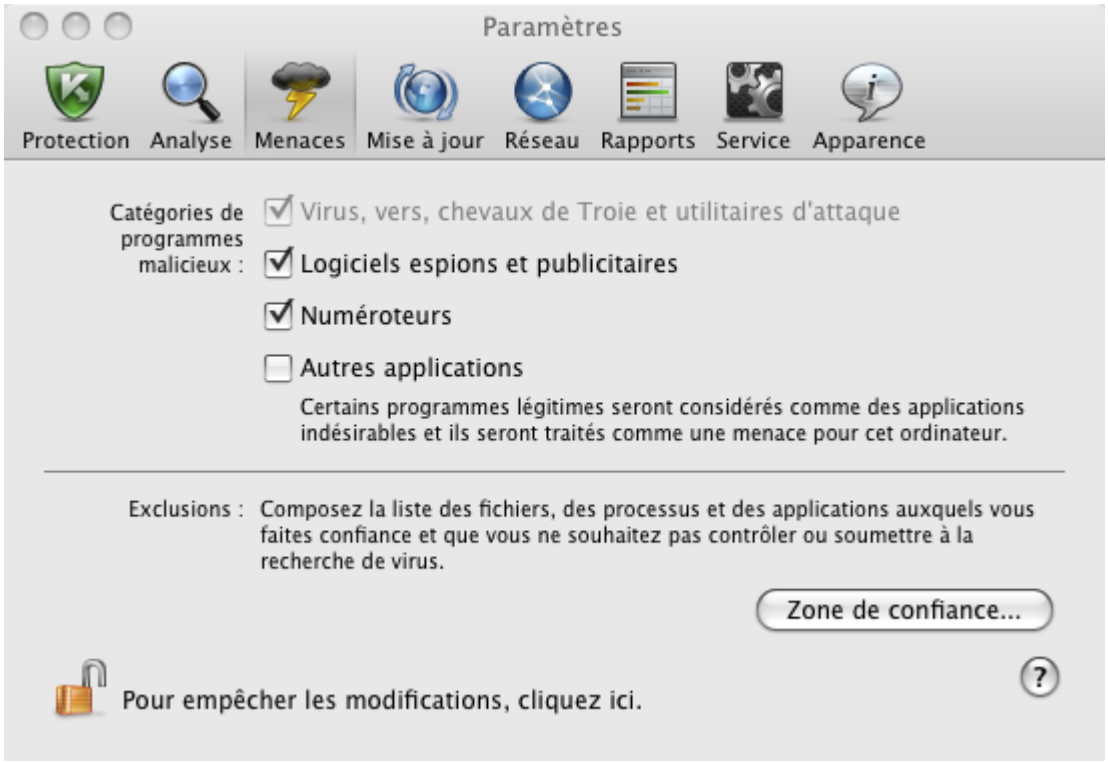


Illustration 16. Fenêtre de configuration de l'application. Menaces

2. Dans le groupe **Exclusions**, cliquez sur le bouton **Zone de confiance** (cf. ill. ci-dessus). Une fenêtre (cf. ill. ci-après) contenant la liste des objets qui ne seront pas analysés par Kaspersky Endpoint Security s'ouvre.

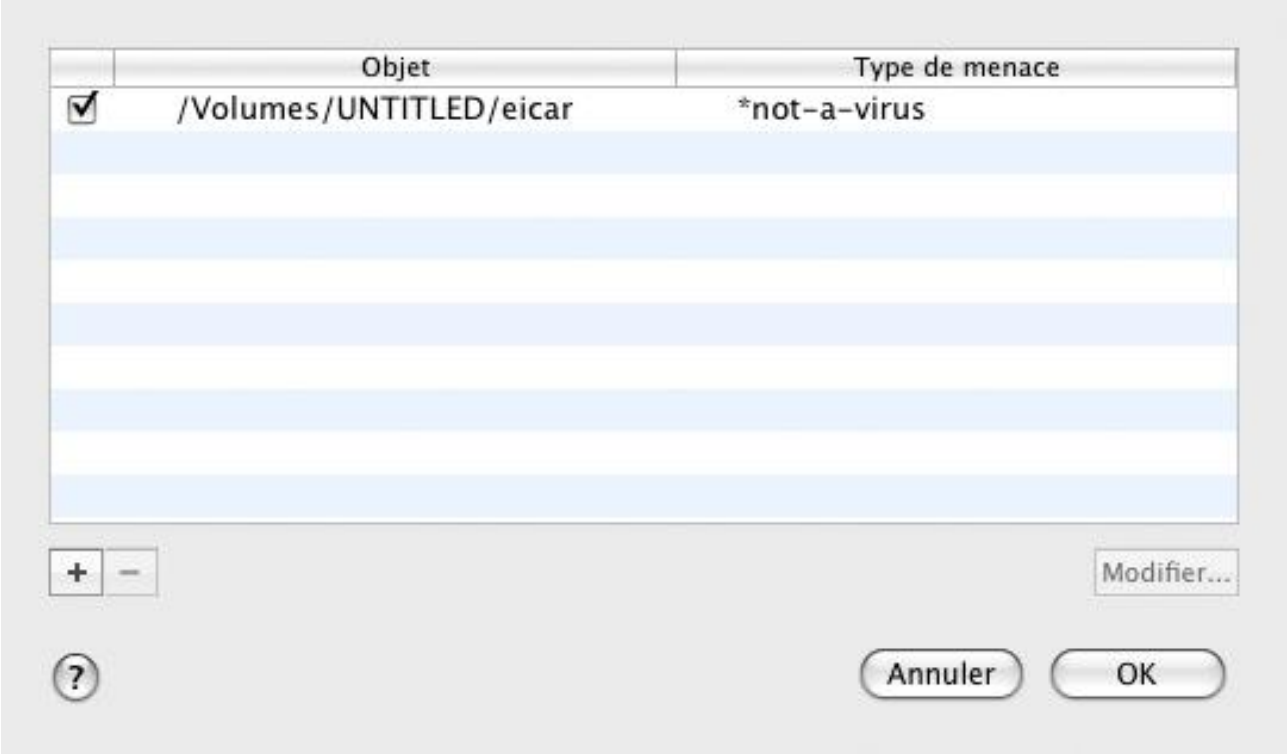


Illustration 17. Liste des objets exclus

Vous pouvez exécuter les opérations suivantes :

- Créer une nouvelle règle d'exclusion.

  Cliquez sur le bouton [+], et dans la fenêtre ouverte **Règle d'exclusion** (cf. ill. ci-après), définissez ses conditions.

- Modifier une règle d'exclusion déjà créée.

  Sélectionnez une règle d'exclusion dans la liste et cliquez sur le bouton **Modifier**. Dans la fenêtre ouverte **Règle d'exclusion** (cf. ill. ci-après), apportez les modifications dans ses conditions.

- Refuser temporairement l'utilisation d'une règle d'exclusion.

  Sélectionnez la règle d'exclusion dans la liste et décochez la case à côté de cette règle. La règle d'exclusion ne va pas être appliquée jusqu'à ce que la case ne soit pas cochée.

- Supprimer une règle d'exclusion.

  Sélectionnez une règle d'exclusion dans la liste et cliquez sur le bouton [−].

Création d'une règle d'exclusion

Dans la fenêtre **Règle d'exclusion** qui s'ouvre, définissez les conditions de la règle d'exclusion à l'aide des paramètres suivants :

- **Objet/Tous les objets**. Désignez le fichier, le dossier ou le masque de fichier (cf. section "Masques autorisés pour l'exclusion des fichiers" à la page 161) comme l'objet d'exclusion. Vous pouvez saisir à la main le nom/le

masque de nom de l'objet dans le champ ou cliquer sur le bouton **Sélectionner** et sélectionner l'objet dans la fenêtre standard ouverte.

La valeur **Tous les objets** suppose l'exclusion de l'analyse de tous les objets de votre ordinateur, correspondants au type de menace défini dans le champ inférieur.

- **Types de menaces/Toutes les menaces**. Le paramètre permet d'exclure de l'analyse les objets, sur la base du type de la menace attribuée selon la classification de l'encyclopédie des virus. Pour saisir un nom de menace, utilisez les valeurs de la liste déroulante : **commençant par**, **terminant par**, **contient**, **un mot entier**, et dans le champ à droite, désignez la partie correspondante du nom. Par exemple, si vous avez choisi la valeur **commençant par not-a-virus**, alors les applications légitimes, mais indésirables, seront exclues. Il est également possible de désigner le nom de la menace selon un masque (cf. section "Masques d'exclusion autorisés selon le classement de l'encyclopédie des virus" à la page 162).

  Si vous choisissez l'option **Toutes les menaces**, les objets repris dans le champ **Objet** supérieur seront exclus de l'analyse quel que soit le type de menace qui leur aura été attribuée.

  En cas de sélection simultanée d'un objet à exclure et d'un type de menace, la règle fonctionnera de la manière suivante :

  - Si un fichier quelconque a été défini en tant qu'Objet et qu'un état particulier a été sélectionné pour le Type de menace, cela signifie que le fichier sélectionné sera exclu uniquement si l'état défini lui est attribué pendant l'analyse.

  - Si un secteur ou un répertoire quelconque a été défini en tant qu'Objet et qu'un état (ou masque de type de menace) a été défini en tant que Type de menace, cela signifie que les objets correspondant à cet état, mais découverts uniquement dans ce secteur/répertoire, seront exclus.

- **Composant/Tous les composants**. Sélectionnez les composants de Kaspersky Endpoint Security qui devront appliquer la règle créée : **Antivirus Fichiers** ou **Analyse**.

  Le choix de l'option **Tous les composants** signifie que la règle sera utilisée par toutes les tâches de recherche de virus, ainsi que par Antivirus Fichiers.

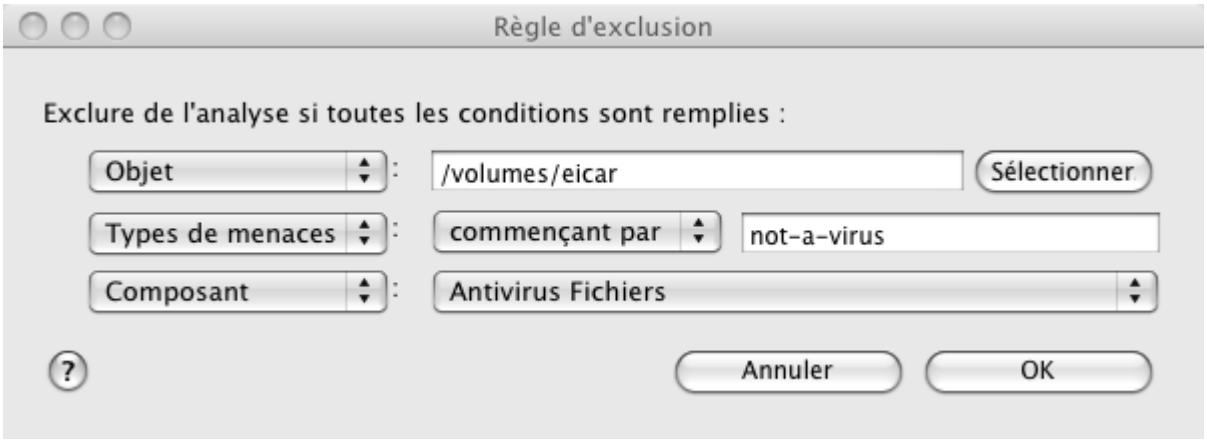


Illustration 18. Création d'une règle d'exclusion

ANTIVIRUS FICHIERS

Le système de fichiers de l'ordinateur peut contenir des virus ou d'autres programmes malveillants qui peuvent être conservés des années après leur intrusion par un disque amovible ou par Internet sans jamais se manifester.

Antivirus Fichiers est le composant qui contrôle le système de fichiers de l'ordinateur en temps réel. Il est lancé par défaut au démarrage du système d'exploitation, reste en permanence dans la mémoire vive de l'ordinateur et analyse tous les fichiers ouverts, exécutés ou enregistrés sur l'ordinateur, ainsi que les disques connectés.

L'Antivirus Fichiers fonctionne avec les fichiers selon l'algorithme suivant :

1. Intercepte les requêtes de l'utilisateur ou d'une application quelconque adressés à chaque fichier.

2. Vérifie la présence des informations sur le fichier intercepté dans la base iSwift (cf. section "Configuration des paramètres avancés" à la page 64). En vertu des informations reçues, une décision sur l'analyse du fichier est prise.

3. Est soumis à la recherche d'éventuels virus. L'identification des objets malveillants s'opère à l'aide des bases antivirus de Kaspersky Endpoint Security. Les bases contiennent la définition de tous les programmes malveillants connus à ce jour et de leur mode d'infection.

Kaspersky Endpoint Security peut adopter un des comportements suivants en fonction des résultats de l'analyse :

- Si aucun code malveillant n'a été découvert dans le fichier, le destinataire pourra l'utiliser immédiatement.

- Si le fichier contient un code malveillant, Antivirus Fichiers le bloque, place une copie dans le dossier de sauvegarde et tente de le réparer. Si la réparation réussit, l'utilisateur peut utiliser le fichier. Dans le cas contraire, le fichier est supprimé. La copie du fichier est placée dans le dossier de sauvegarde (cf. page 97).

- Si le fichier contient un code semblable à un code malveillant, le fichier est placé en quarantaine (à la page 94). Il est possible de le réparer plus tard en utilisant les bases antivirus actualisées.

Kaspersky Endpoint Security est lancé par défaut au démarrage du système d'exploitation et protège votre ordinateur pendant la session. L'icône de Kaspersky Endpoint Security (cf. page 31) témoigne du fonctionnement de l'Antivirus Fichiers. Si l'icône est active, cela signifie que la protection de votre ordinateur est activée. Si l'icône n'est pas active, cela signifie que la protection est désactivée.

DANS CETTE SECTION

DESACTIVATION DE LA PROTECTION DES FICHIERS

Les experts de Kaspersky Lab vous recommandent vivement de ne pas désactiver la protection offerte par l'Antivirus Fichiers en temps réel, car cela pourrait entraîner l'infection de votre ordinateur et la perte de données.

Notez que dans ce cas, la protection est envisagée dans le contexte de fonctionnement d'Antivirus Fichiers (cf. section "Antivirus Fichiers" à la page 56). La désactivation ou la suspension du fonctionnement d'Antivirus Fichiers n'a pas d'influence sur la recherche de virus (cf. section "Analyse" à la page 68) et la mise à jour (cf. section "Mise à jour de l'application" à la page 84).

Il est possible d'activer l'Antivirus Fichiers par plusieurs moyens. Toutefois, avant de faire quoi que ce soit, nous vous conseillons de définir la raison pour laquelle vous souhaitez désactiver la protection des fichiers.

En effet, il est peut-être possible de résoudre le problème d'une autre façon : modifier le niveau de protection (cf. section "Sélection du niveau de protection" à la page 60) ou désactiver la protection uniquement de certains fichiers en créant une règle d'exclusion (cf. section "Constitution de la zone de confiance" à la page 53). Ainsi, si vous utilisez une base de données qui, selon vous, ne peut contenir de virus, il suffit d'ajouter ce dossier et les fichiers qu'il contient dans la zone de confiance. Probablement, il vous faudra suspendre le fonctionnement de l'Antivirus Fichiers si Kaspersky Endpoint Security est en conflit avec d'autres applications installées sur votre ordinateur.

Pour désactiver l'Antivirus Fichiers, utilisez un des moyens suivants :

- Cliquez sur l'icône de Kaspersky Endpoint Security (à la page 31) et dans le menu contextuel ouvert, sélectionnez la commande **Désactiver Protection** (cf. ill. ci-après).

Illustration 19. Désactivation de l'Antivirus Fichiers

- Ouvrez la fenêtre de configuration de l'application (à la page 35), sélectionnez l'onglet **Protection** et décochez la case **Activer Antivirus Fichiers** (cf. ill. ci-après).

Illustration 20. Fenêtre de configuration de l'application. Protection

Si vous avez désactivé l'Antivirus Fichiers, alors il ne sera pas activé automatiquement après le redémarrage de Kaspersky Endpoint Security. Il est nécessaire de restaurer la protection du système de fichier de l'ordinateur à la main (cf. section "Rétablissement de la protection de l'ordinateur" à la page 59).

RETABLISSEMENT DE LA PROTECTION DE L'ORDINATEUR

Si l'Antivirus Fichiers a été désactivé, alors il sera possible de restaurer la protection du système de fichiers de l'ordinateur uniquement à la main à la demande de l'utilisateur. L'activation automatique de l'Antivirus Fichiers après le redémarrage du système d'exploitation ou de Kaspersky Endpoint Security n'aura pas lieu.

Pour activer l'Antivirus Fichiers, utilisez un des moyens suivants :

- Cliquez sur l'icône de Kaspersky Endpoint Security (à la page 31) et dans le menu contextuel ouvert, sélectionnez la commande **Activer Protection** (cf. ill. ci-après).

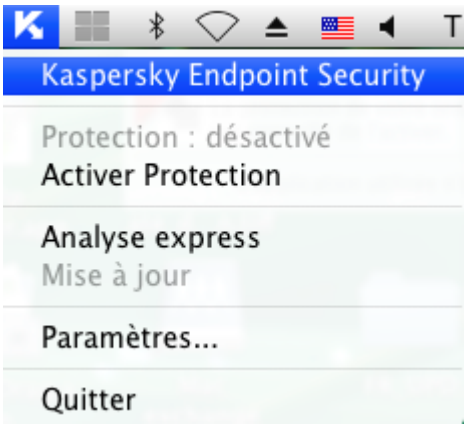


Illustration 21. Activation de l'Antivirus Fichiers

- Ouvrez la fenêtre de configuration de l'application (à la page 35), sélectionnez l'onglet **Protection** et décochez la case **Activer Antivirus Fichiers** (cf. ill. ci-après).

Illustration 22. Fenêtre de configuration de l'application. Protection

- Utilisez l'Assistant de sécurité (cf. section "Assistant de sécurité" à la page 44). La suspension ou l'arrêt de la protection augmente sensiblement le risque d'infection de l'ordinateur. Par conséquent, cette menace est immédiatement consignée par l'Assistant de protection.

CONFIGURATION DE L'ANTIVIRUS FICHIERS

Le fonctionnement de l'Antivirus Fichiers est contrôlé à l'aide des paramètres suivants :

- **Niveau de protection**.

  Le niveau de protection est l'ensemble de paramètres qui définissent la relation entre le détail et la vitesse de l'analyse des objets sur les virus. Il existe trois niveaux prédéfinis de protection (cf. section "Sélection du niveau de protection" à la page 60) mis au point par les experts de Kaspersky Lab.

- **Action à réaliser sur l'objet identifié**.

  L'action (cf. section "Sélection de l'action exécutée sur les objets" à la page 65) détermine le comportement de Endpoint Security en cas de découverte d'un objet infecté ou potentiellement infecté.

SELECTION DU NIVEAU DE PROTECTION

L'Antivirus Fichiers assure la protection du système de fichiers de l'ordinateur sur un des niveaux suivants :

- **Protection maximale** : le contrôle de tous les fichiers ouverts, enregistrés et modifiés est total.
- **Recommandé** : le niveau dont les paramètres sont recommandés par les experts de Kaspersky Lab.
- **Vitesse maximale** : les paramètres de ce niveau vous permettent d'utiliser confortablement des applications à usage intensif de ressources systèmes, dans la mesure où l'ensemble des fichiers analysés est réduit.

Par défaut, l'Antivirus Fichiers fonctionne sur le niveau de protection **Recommandé**. Vous pouvez augmenter ou réduire le niveau de protection du système de fichiers en sélectionnant le niveau **Protection maximale** ou **Vitesse maximale** ou en modifiant les paramètres du niveau actuel.

Afin de modifier le niveau de protection, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (à la page 35) et sélectionnez l'onglet **Protection** (cf. ill. ci-après).
2. Dans le groupe **Niveau de protection**, déplacez simplement le curseur. Ce faisant, vous modifiez le rapport entre la vitesse de l'analyse et la quantité des fichiers analysés : plus le nombre de fichiers soumis à l'analyse sera réduit, plus la vitesse de l'analyse sera élevée.

Si aucun des niveaux prédéfinis ne répond à vos attentes, vous pouvez procéder à une configuration avancée des paramètres de la protection. Pour ce faire, il est conseillé de choisir le niveau de protection le plus proche de vos besoins en guise de point de départ et d'en modifier les paramètres. Dans ce cas, le nom du niveau de sécurité devient **Utilisateur**.

Pour modifier les paramètres du niveau de protection actuel, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (à la page 35) et sélectionnez l'onglet **Protection** (cf. ill. ci-après).
2. Dans le groupe **Niveau de protection**, cliquez sur le bouton **Paramètres**.
3. Dans la fenêtre ouverte, modifiez les paramètres de la protection des fichiers :
   - sous l'onglet **Général** (cf. section "**Définition du type de fichiers analysés**" à la page 61), définissez les types de fichiers analysés ;

- sous l'onglet **Zone de protection** (cf. section "**Constitution de la couverture de protection**" à la page 62), indiquez les disques ou les dossiers qui doivent être contrôlés par l'Antivirus Fichiers ;

- sous l'onglet **Avancé** (cf. section "**Configuration des paramètres avancés**" à la page 64), configurez le mode de fonctionnement du composant.

4. Cliquez sur le bouton **OK** pour enregistrer les modifications.

Illustration 23. Fenêtre de configuration de l'application. Protection

DEFINITION DU TYPE DE FICHIERS ANALYSES

La définition du type de fichiers analysés vous permet de déterminer le format et la taille des fichiers qui seront soumis à l'analyse antivirus par l'Antivirus Fichiers à l'ouverture, l'exécution et l'enregistrement. Vous pouvez également configurer les performances de l'analyse.

Pour désigner les types d'objets analysés par l'Antivirus Fichiers et configurer les performances de l'analyse, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (à la page 35) et sélectionnez l'onglet **Protection**.

2. Dans le groupe **Niveau de protection**, cliquez sur le bouton **Paramètres**.

3. Dans la fenêtre ouverte, sélectionnez l'onglet **Général** (cf. ill. ci-après) et configurez les paramètres suivants :

   - Indiquez, dans le groupe **Types de fichiers**, les formats d'objet qui seront analysés par Kaspersky Endpoint Security à la recherche d'éventuels virus à l'ouverture, à l'exécution et à l'enregistrement.

   - Dans le groupe **Optimisation**, configurez les performances de l'analyse.

- Dans le groupe **Fichiers composés**, sélectionnez les fichiers composés à soumettre à la recherche d'éventuels virus et définissez la restriction sur l'analyse des gros objets.

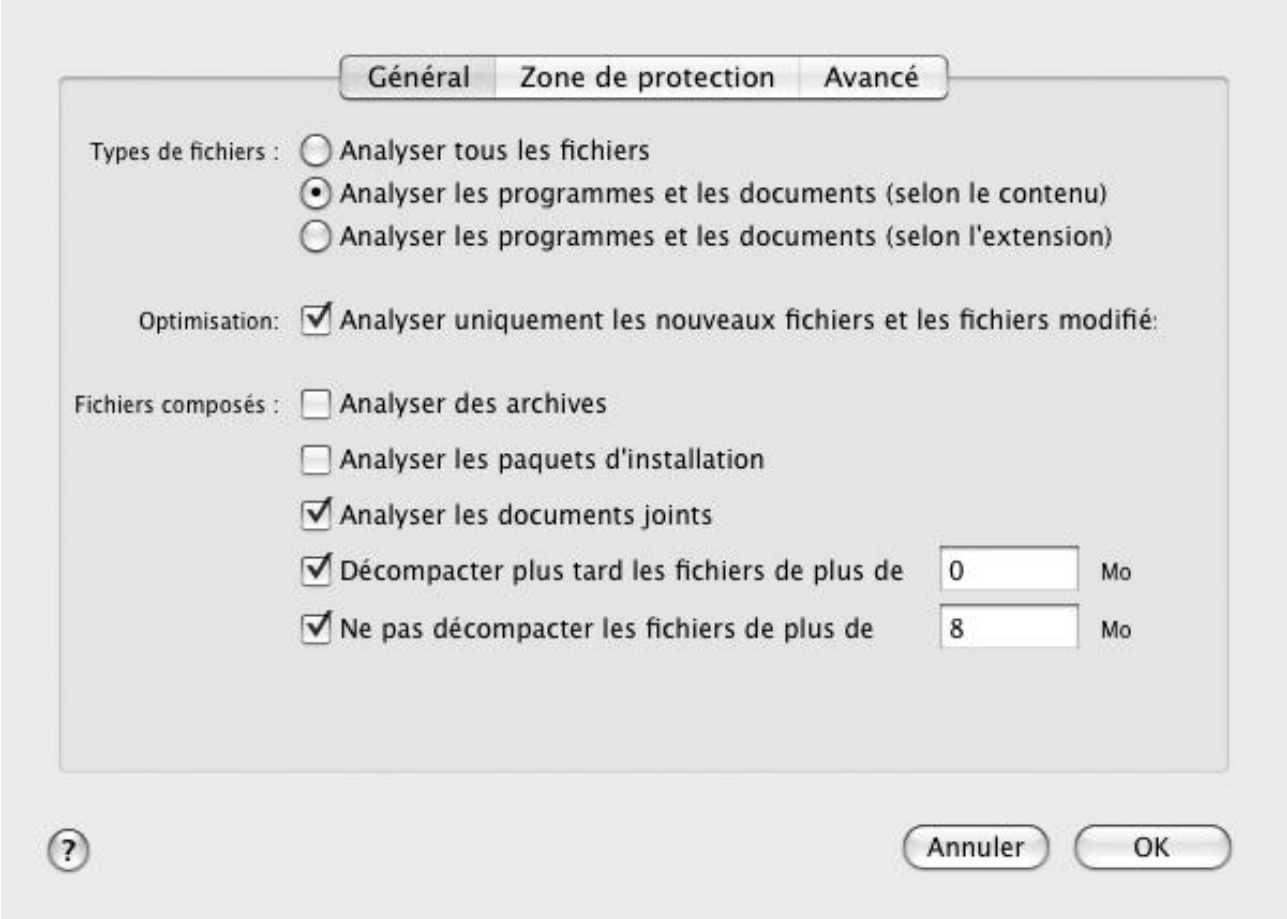


Illustration 24. Antivirus Fichiers. Configuration de l'analyse

CONSTITUTION DE LA ZONE DE PROTECTION

Par défaut, Antivirus Fichiers analyse tous les fichiers dès qu'une requête lui est adressée, quel que soit le support sur lequel ils se trouvent (disque dur, CD/DVD-ROM ou carte Flash).

Pour former une liste des objets inclus dans la zone de confiance, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (à la page 35) et sélectionnez l'onglet **Protection**.
2. Dans le groupe **Niveau de protection**, cliquez sur le bouton **Paramètres**.
3. Dans la fenêtre qui s'ouvre, sélectionnez l'onglet **Zone de protection** (cf. ill. ci-après). La liste des objets qui seront analysés par l'Antivirus Fichiers est présentée sous la liste. La protection est active par défaut pour tous les objets se trouvant sur des disques fixes, des supports amovibles et les unités réseau connectées à l'ordinateur.

Vous pouvez exécuter les opérations suivantes :

- Ajouter en objet à analyser.

  Cliquez sur le bouton [+] et dans la fenêtre standard ouverte, sélectionnez le dossier ou le fichier.

- Modifier l'objet de la liste (accessible uniquement pour les objets ajoutés par l'utilisateur).

Sélectionnez l'objet et cliquez sur le bouton **Modifier**. Saisissez vos modifications dans la fenêtre standard ouverte.

- Suspendre temporairement l'analyse d'un objet de la liste.

  Sélectionnez un objet et décochez la case à côté de cet objet. L'Antivirus Fichier ne va pas contrôler cet objet jusqu'à ce que la case ne soit pas cochée de nouveau.

- Supprimer l'objet (accessible uniquement pour les objets ajoutés par l'utilisateur).

  Sélectionnez l'objet et cliquez sur le bouton  .

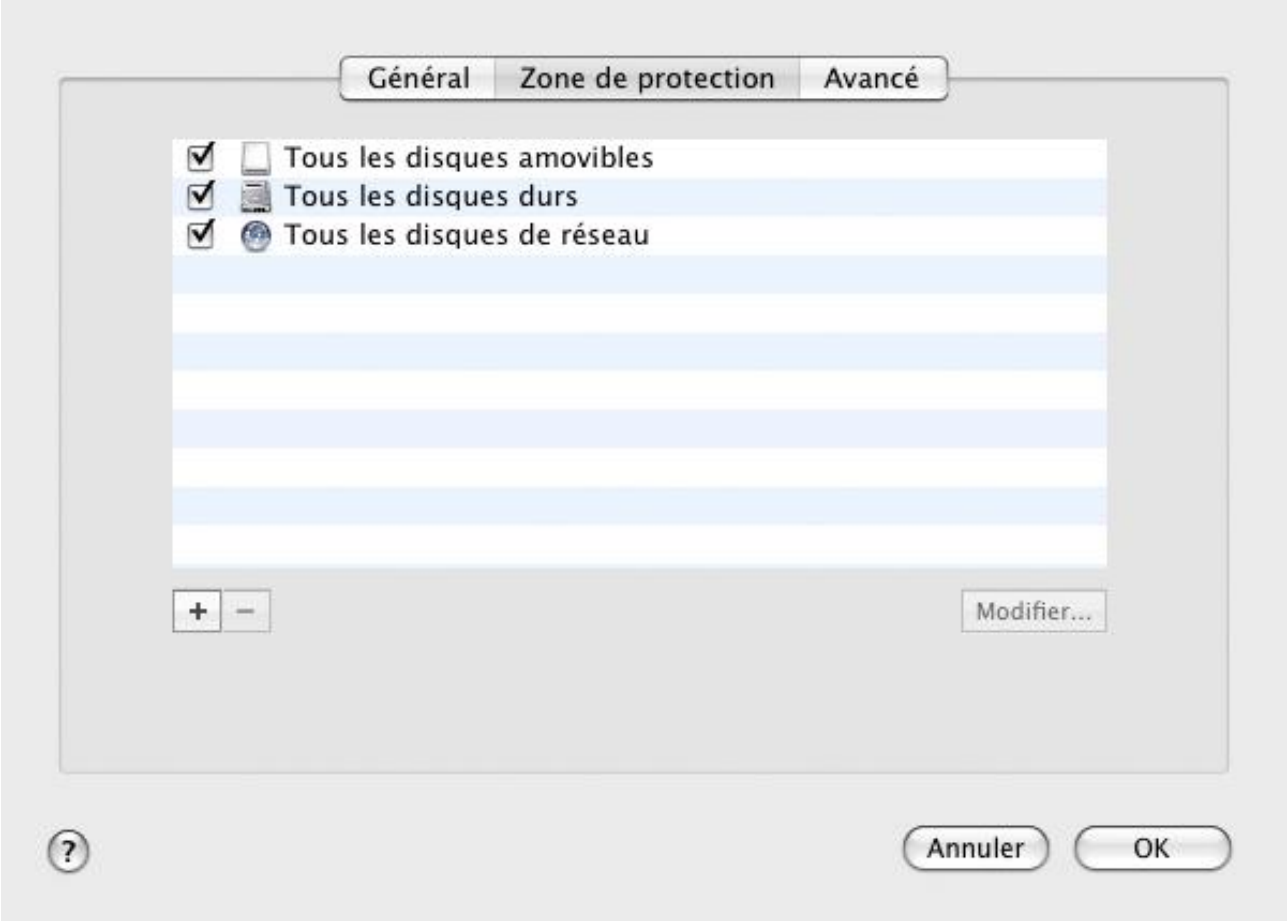


Illustration 25. Antivirus Fichiers. Constitution de la couverture de protection

Si vous souhaitez restreindre le nombre d'objets protégés, vous pouvez suivre une des méthodes suivantes :

- indiquer uniquement les répertoires, disques ou fichiers qui doivent être protégés ;
- constituer une liste des objets qui ne doivent pas être protégés (cf. section "Constitution de la zone de confiance" à la page 53) ;
- utiliser simultanément la première et la deuxième méthode, c.-à-d. définir une zone de protection dont sera exclue une série d'objets.

CONFIGURATION DES PARAMETRES AVANCES

En tant que paramètres complémentaires du fonctionnement de l'Antivirus Fichiers vous configurez le mode d'analyse des objets du système fichier, activer la technologie iSwift qui augmente la productivité du traitement des objets et programmer le fonctionnement du composant.

Pour configurer les paramètres avancés d'Antivirus Fichiers, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (à la page 35) et sélectionnez l'onglet **Protection**.
2. Dans le groupe **Niveau de protection**, cliquez sur le bouton **Paramètres**.
3. Dans la fenêtre ouverte, sélectionnez l'onglet **Avancé** (cf. ill. ci-après) et configurez les paramètres suivants :
   - Dans le groupe **Mode d'analyse**, définissez les conditions d'activation d'Antivirus Fichiers.
   - Sélectionnez la technologie d'analyse dans le groupe **Productivité**.
   - Dans le groupe **Suspension de la tâche**, activez la suspension programmée du fonctionnement de l'Antivirus Fichiers et configurez les paramètres de la programmation.
   - Dans le groupe **Analyseur heuristique**, configurez l'utilisation de l'analyseur heuristique par l'Antivirus Fichiers.

Illustration 26. Antivirus Fichiers. Configuration des paramètres avancés

SELECTION DES ACTIONS A REALISER SUR LES OBJETS

Si l'analyse d'un fichier détermine une infection ou une possibilité d'infection, la suite du fonctionnement de l'Antivirus Fichiers dépendra de l'état de l'objet et de l'action sélectionnée.

A la fin de l'analyse, chaque objet peut se voir attribuer un des statuts suivants :

- état de l'un des programmes malveillants (exemple, *virus*, *cheval de Troie*) ;
- état *probablement infecté* lorsqu'il est impossible d'affirmer avec certitude si l'objet est infecté ou non. Cela signifie que le fichier contient la séquence du code d'un virus inconnu ou le code modifié d'un virus connu.

Par défaut, tous les objets malveillants sont réparés et tous les objets probablement infectés sont placés en quarantaine (cf. section "Quarantaine" à la page 94).

Pour sélectionner une action à effectuer par l'Antivirus Fichiers lors de la détection d'un objet infecté ou potentiellement infecté, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (à la page 35) et sélectionnez l'onglet **Protection** (cf. ill. ci-après).
2. Dans le groupe **Action**, sélectionnez l'action de l'Antivirus Fichiers.

Illustration 27. Fenêtre de configuration de l'application. Protection

Avant toute réparation ou suppression d'un objet, Kaspersky Endpoint Security crée une copie de sauvegarde et la place dans le dossier de sauvegarde (à la page 97) au cas où il faudrait restaurer l'objet ou s'il devenait possible de le réparer.

RESTAURATION DES PARAMETRES DE PROTECTION DU COURRIER PAR DEFAUT

A tout moment, vous pouvez revenir aux paramètres de la configuration de l'Antivirus Fichiers par défaut. Il s'agit des paramètres optimaux pour assurer la protection de votre ordinateur contre les programmes malveillants. Ces paramètres sont recommandés par les experts de Kaspersky Lab et sont réunis dans le niveau de protection **Recommandé**.

Pour restaurer les paramètres de l'Antivirus Fichiers par défaut, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (à la page 35) et sélectionnez l'onglet **Protection** (cf. ill. ci-après).

2. Dans le groupe **Niveau de protection**, cliquez sur le bouton **Par défaut**.

Illustration 28. Fenêtre de configuration de l'application. Protection

STATISTIQUES DE LA PROTECTION DES FICHIERS

Les statistiques de synthèse sur le fonctionnement actuel de l'Antivirus Fichiers (nombre d'objets analysés depuis le dernier lancement du composant, nombre d'objets détectés et réparés, nom du fichier qui a été analysé en dernier) sont présentées dans la partie inférieure de la fenêtre principale de l'application (cf. section "Fenêtre principale de l'application" à la page 33).

Kaspersky Endpoint Security propose également un rapport détaillé sur le fonctionnement de l'Antivirus Fichiers.

Pour parcourir le rapport, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (à la page 33) et cliquez sur le bouton  .

2. Dans la section **Tâches exécutées** de la fenêtre qui s'ouvre, choisissez **Antivirus Fichiers**.

Si l'Antivirus Fichiers est désactivé actuellement, vous pouvez consulter le rapport détaillé sur les résultats de l'exécution antérieure dans la section **Tâches terminées**.

Si le fonctionnement d'Antivirus Fichiers s'est soldé par une erreur, consultez le rapport et tentez de relancer le composant. Si vous ne parvenez pas à résoudre vous-même le problème, contactez le Service d'assistance technique de Kaspersky Lab (cf. section "Contacter le Service d'assistance technique" à la page 157).

Les informations détaillées sur le fonctionnement de l'Antivirus Fichiers sont présentées dans la fenêtre des rapports à droite, sous les onglets suivants :

- L'onglet **Détectés** reprend tous les objets détectés pendant la protection du système de fichiers de l'ordinateur. Pour chaque objet, le nom et le chemin d'accès au dossier (où l'objet a été enregistré) sont indiqués, ainsi que l'état attribué à cet objet par l'Antivirus Fichiers. Si le programme a pu définir exactement le programme malveillant qui a infecté l'objet, il recevra l'état, par exemple : *virus*, *cheval de Troie*, etc. S'il est impossible de définir avec exactitude le type de programme malveillant, l'objet recevra le statut *suspect*. En plus de l'état, le rapport reprend également les informations relatives à l'action exécutée sur l'objet (*découvert*, *réparé*).

- L'onglet **Evénements** reprend la liste entière des événements survenus pendant l'utilisation de l'Antivirus Fichiers avec l'heure de survenance de l'événement, son nom, état et causes d'apparition. Les événements prévus sont :

  - *événement informatif* (par exemple : l'objet n'a pas été traité : ignoré selon le type) ;

  - *avertissement* (par exemple : découverte d'un virus) ;

  - *remarque* (par exemple : archive protégée par un mot de passe).

- L'onglet **Statistiques** reprend les informations sur le nombre total d'objets analysés, et dans les colonnes séparées vous retrouverez le nombre d'objets parmi le nombre total d'objets en cours d'analyse étant les archives, les objets dangereux, réparés, placés en quarantaine, etc.

- L'onglet **Paramètres** reprend les paramètres principaux conformément auxquels l'Antivirus Fichiers fonctionne. Pour passer rapidement à la configuration du composant, cliquez sur le bouton **Modifier les paramètres**.

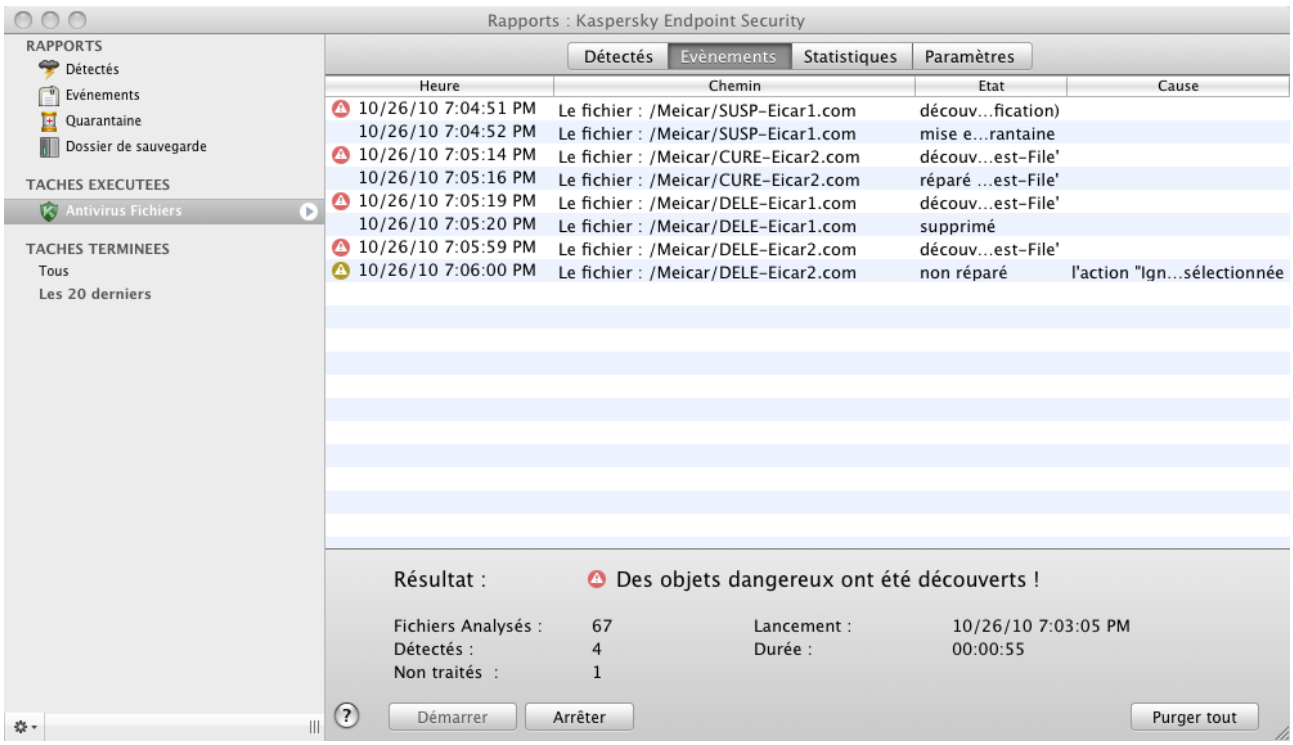


Illustration 29. Fenêtre des rapports. Antivirus Fichiers

ANALYSE

Outre la protection en temps réel du système de fichiers de l'ordinateur par l'Antivirus Fichiers (cf. section "Antivirus Fichiers" à la page 56), il est primordial de rechercher la présence éventuelle de virus sur l'ordinateur à intervalles réguliers. Cette activité est indispensable afin d'éviter la propagation de programmes malveillants qui n'auraient pas été interceptés par les composants de la protection en raison, par exemple, d'un niveau de protection trop bas ou de tout autre motif.

Kaspersky Endpoint Security propose les tâches de recherche de virus prédéfinies suivantes :

-  **Analyse**

  Recherche de virus sur un objet spécifique (fichiers, dossier, disques, disques amovibles).

-  **Analyse complète**

  Recherche de virus sur l'ordinateur avec une analyse minutieuse de tous les disques durs.

-  **Analyse express**

  Recherche de virus éventuels uniquement dans les secteurs critiques de l'ordinateur : dossiers contenant les fichiers du système d'exploitation et les bibliothèques système.

Par défaut, ces tâches sont exécutées selon les paramètres recommandés. Vous pouvez modifier ces paramètres (cf. section "Configuration des tâches liées à la recherche de virus" à la page 74) et même indiquer le mode du lancement de la tâche d'analyse (cf. section "Programmation du lancement des tâches de recherche de virus" à la page 78).

DANS CETTE SECTION

ADMINISTRATION DES TACHES LIEES A LA RECHERCHE DE VIRUS

Les tâches liées à la recherche de virus peuvent être lancées manuellement (cf. section "Lancement/arrêt des tâches liées à la recherche de virus" à la page 68) ou automatiquement selon la programmation (cf. section "Programmation du lancement des tâches de recherche de virus" à la page 78). Il est également possible de créer des tâches d'utilisateur (cf. section "Création de tâches liées à la recherche de virus" à la page 70).

LANCEMENT/ARRET DES TACHES LIEES A LA RECHERCHE DE VIRUS

Pour lancer la tâche de recherche de virus manuellement, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (à la page 33) et cliquez sur le bouton .

2. Dans la fenêtre qui s'ouvre (cf. ill. ci-après), sélectionnez la tâche nécessaire : **Analyse complète**, **Analyse express** ou **Analyse**. Si vous avez sélectionné la tâche **Analyse**, Kaspersky Endpoint Security vous proposera d'indiquer la zone d'analyse. Excepté des tâches énumérées comprises dans l'application, les tâches utilisateurs d'analyse s'affichent dans le menu (cf. section "Création de tâches liées à la recherche de virus" à la page 70), si de telles tâches ont été créées.

Illustration 30. Tâches de recherche de virus

Les informations relatives aux tâches en cours d'exécution apparaissent dans la partie gauche de la fenêtre principale, ainsi que dans la section **Tâches exécutées** de la fenêtre du rapport (cf. section "Rapports" à la page 98). Les informations sur les tâches exécutées sont reprises dans la section **Tâches terminées** de la fenêtre des rapports (cf. ill. ci-après).

Pour arrêter l'exécution de la tâche de recherche de virus, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (à la page 33) et cliquez sur le bouton . La fenêtre des rapports de Kaspersky Endpoint Security s'ouvre.

2. Dans la section **Tâches exécutées** (cf. ill. ci-après), sélectionnez le nom de la tâche d'analyse et cliquez sur le bouton **Arrêter**. L'analyse sera suspendue jusqu'à ce que la tâche soit à nouveau relancée manuellement ou selon la programmation. Pour relancer l'analyse, cliquez sur le bouton **Démarrer.** Dans la fenêtre qui s'ouvre, Kaspersky Endpoint Security proposera de reprendre la recherche là où elle a été interrompue, soit d'en lancer une nouvelle.

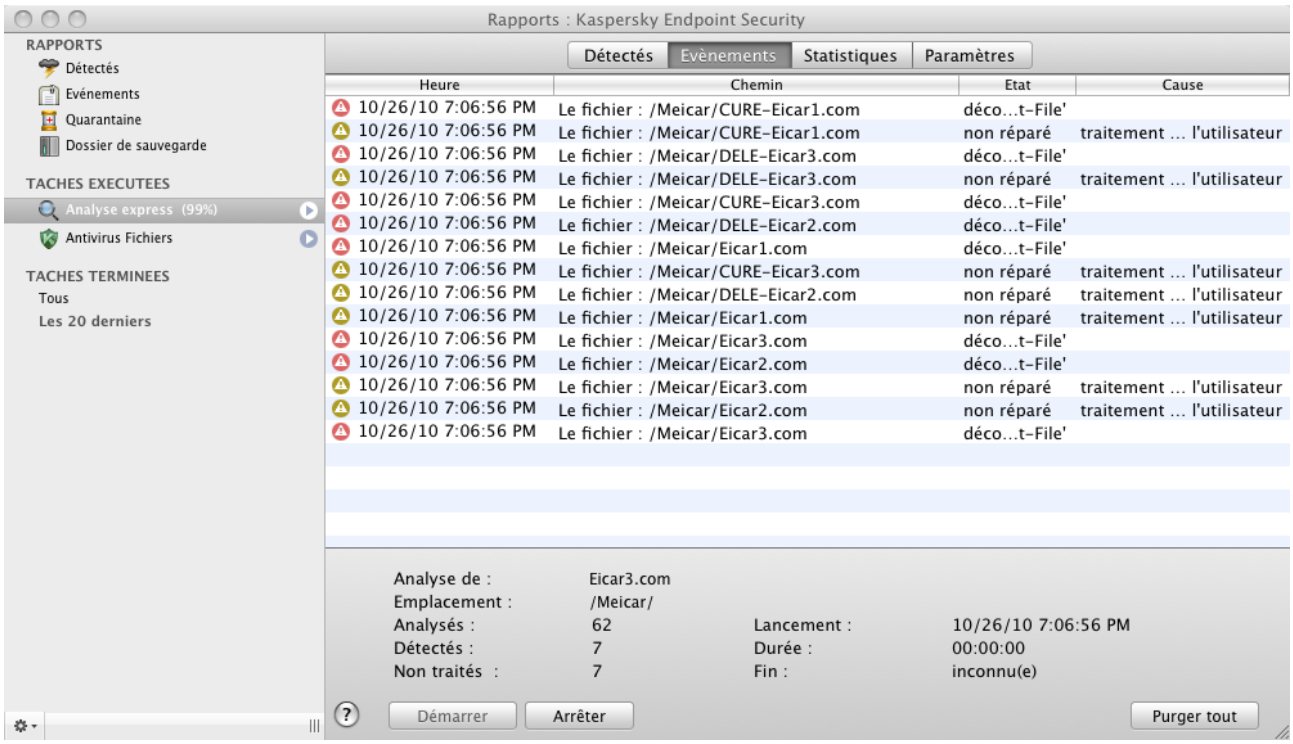


Illustration 31. Fenêtre des rapports. Analyse

CREATION DE TACHES LIEES A LA RECHERCHE DE VIRUS

Afin de rechercher la présence éventuelle de virus parmi les objets de l'ordinateur, vous pouvez utiliser non seulement les tâches d'analyse intégrées livrées avec Kaspersky Endpoint Security, mais aussi des tâches personnalisées. La création de chaque nouvelle tâche s'opère sur la base des tâches existantes.

Pour créer une tâche de recherche de virus, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (à la page 35).

2. Sélectionnez l'onglet **Analyse** et dans la liste à gauche (cf. ill. ci-après), sélectionnez la tâche **Analyse express** ou **Analyse complète** dont les paramètres sont les plus proches à vos exigences.

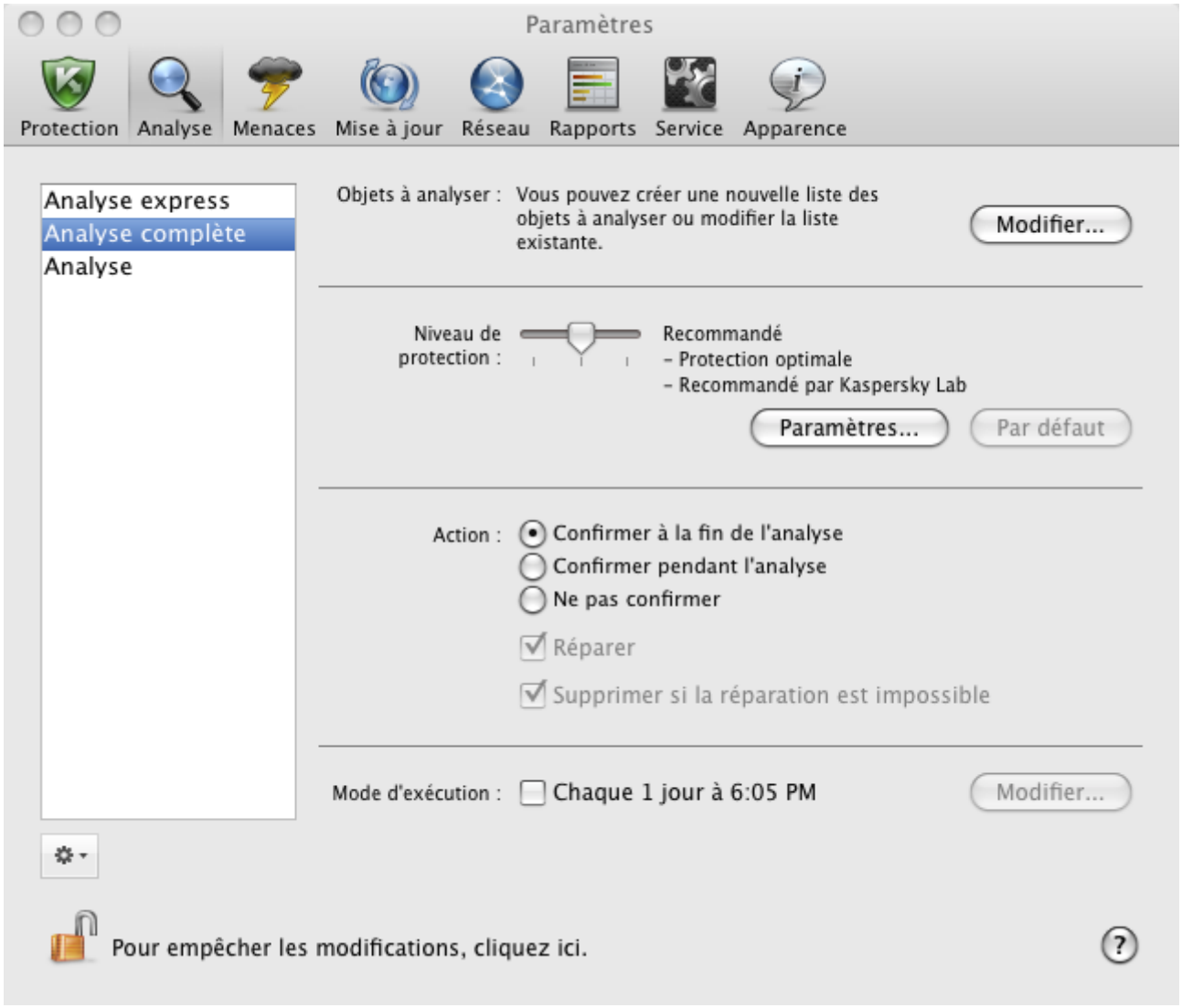


Illustration 32. Fenêtre de configuration de l'application. Tâche Analyse complète

3. Cliquez sur le bouton  situé sous la liste des tâches de recherche de virus, et dans la fenêtre ouverte, sélectionnez la commande **Copier**.

4. Saisissez le nom de la nouvelle tâche dans la fenêtre qui s'ouvre, puis cliquez sur **OK**. La tâche portant le nom indiqué apparaîtra dans la liste.

La nouvelle tâche possède des paramètres identiques à ceux de la tâche qui lui a servi de base. Vous devrez par conséquent réaliser une configuration complémentaire :

- modifier la liste des objets à analyser (cf. section "Composition de la liste des objets à analyser" à la page 72) ;
- indiquer les paramètres (cf. section "Configuration des tâches liées à la recherche de virus" à la page 74) utilisés pour l'exécution de la tâche ;
- configurer la planification du lancement automatique (cf. section "Programmation du lancement des tâches de recherche de virus" à la page 78).

Suite aux tâches intégrées de recherche de virus, Kaspersky Endpoint Security permet de créer pas plus de six tâches utilisateurs de recherche.

Vous pouvez renommer et supprimer les tâches d'analyse.

Vous pouvez renommer ou supprimer uniquement les tâches de recherche créées par l'utilisateur.

- *Pour renommer une tâche créée, procédez comme suit :*

  1. Ouvrez la fenêtre de configuration de l'application (à la page 35).
  2. Dans la liste de gauche, sélectionnez la tâche (cf. ill. ci-dessus).
  3. Cliquez sur le bouton  situé sous la liste des tâches d'analyse, et dans la fenêtre ouverte, sélectionnez la commande **Renommer**.
  4. Modifiez le nom de la tâche dans la fenêtre qui s'affiche puis cliquez sur **OK**. La tâche sera renommée.

- *Pour supprimer une tâche, procédez comme suit :*

  1. Ouvrez la fenêtre de configuration de l'application (à la page 35).
  2. Dans la liste de gauche, sélectionnez la tâche (cf. ill. ci-dessus).
  3. Cliquez sur le bouton  situé sous la liste des tâches d'analyse, et dans la fenêtre ouverte, sélectionnez la commande **Supprimer**. Confirmez l'action dans la fenêtre ouverte. La tâche sera supprimée de la liste.

COMPOSITION DE LA LISTE DES OBJETS A ANALYSER

Les tâches **Analyse complète** et **Analyse express** incluses dans Kaspersky Endpoint Security possèdent déjà des listes formées des objets à analyser. La tâche **Analyse complète** permet d'effectuer l'analyse de tous les fichiers situés sur les disques durs de l'ordinateur. Dans le cadre de l'**Analyse express**, Kaspersky Endpoint Security analyse uniquement les objets vulnérables du point de vue de la sécurité : les dossiers contenant les fichiers du système d'exploitation et les bibliothèques système.

La tâche **Analyse** requiert une formation de la liste des objets à analyser (sélection du fichier, dossier, disque, disques amovibles).

- *Pour faire connaissance avec la liste des objets à analyser, lors de l'exécution des tâches **Analyse complète** et **Analyse express**, ou pour modifier cette liste, procédez comme suit :*

  1. Ouvrez la fenêtre de configuration de l'application (à la page 35) et sélectionnez l'onglet **Analyse**.
  2. Dans la liste de gauche, sélectionnez le nom de la tâche : **Analyse complète** ou **Analyse express**.
  3. A droite, dans le groupe **Objets à analyser**, cliquez sur le bouton **Modifier**. La fenêtre avec la liste des objets s'ouvrira (cf. ill. ci-après). Modifiez-la, si nécessaire.

     Vous pouvez exécuter les opérations suivantes :

     - Ajouter l'objet dans la liste.

       Déplacez l'objet dans la fenêtre ou cliquez sur le bouton  et sélectionnez de la liste déroulante l'option qui vous convient le mieux (**Fichier ou dossier**, **Tous les disques**, **Quarantaine**, etc.). Si l'objet ajouté contient des sous-dossiers qui doivent aussi être analysés, cochez la case **Sous-répertoires compris** dans la fenêtre de la sélection du fichier. Si l'objet ajouté contient les liens symboliques vers d'autres objets

qui requièrent l'analyse, dans la fenêtre ouverte de sélection du fichier, cochez la case **Liens symboliques inclus**.

- Modifier l'objet de la liste (accessible uniquement pour les objets ajoutés par l'utilisateur).

  Sélectionnez l'objet et cliquez sur le bouton **Modifier**. Saisissez vos modifications dans la fenêtre standard ouverte.

- Suspendre temporairement l'analyse d'un objet de la liste.

  Sélectionnez un objet et décochez la case à côté de cet objet. La tâche de recherche de virus ne sera pas exécutée pour cet objet jusqu'à ce que la case ne soit pas cochée de nouveau.

- Supprimer l'objet (accessible uniquement pour les objets ajoutés par l'utilisateur).

  Sélectionnez l'objet et cliquez sur le bouton  .

Lors de la création des tâches d'utilisateur (cf. section "Création de tâches liées à la recherche de virus" à la page 70), la liste des objets à analyser est formée ou modifiée d'une manière analogue.

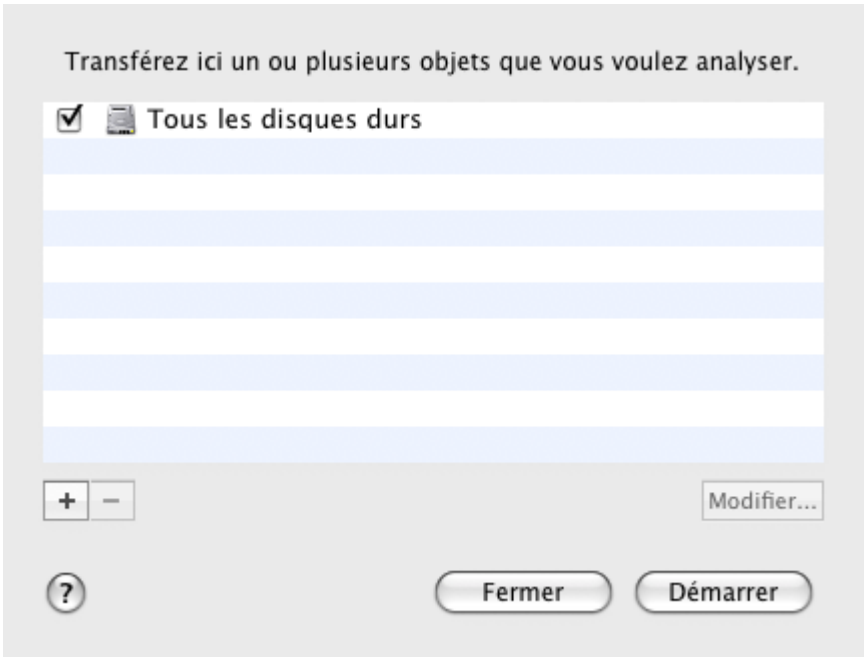


Illustration 33. Composition de la liste des objets à analyser

*Pour sélectionner un ou plusieurs objets à analyser lors de l'exécution de la tâche **Analyse**, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application (à la page 33) et cliquez sur le bouton  .

2. Dans le menu qui s'ouvre, sélectionnez la tâche **Analyse**. La fenêtre de formation de la liste des objets s'ouvrira (cf. ill. ci-dessus). Modifiez la liste par le mode décrit ci-dessus.

CONFIGURATION DES TACHES LIEES A LA RECHERCHE DE VIRUS

L'exécution des tâches de recherche de virus sur votre ordinateur est définie par les paramètres suivants :

- **Niveau de protection**

  Le niveau de protection est l'ensemble de paramètres qui définissent la relation entre le détail et la vitesse de l'analyse des objets sur la présence de virus. Il existe trois niveaux prédéfinis de protection (cf. section "Sélection du niveau de protection" à la page 74) mis au point par les experts de Kaspersky Lab.

- **Action à réaliser sur l'objet identifié**

  L'action (cf. section "Sélection de l'action exécutée sur les objets" à la page 77) détermine le comportement de Kaspersky Endpoint Security en cas de découverte d'un objet infecté ou potentiellement infecté.

- **Mode d'exécution**

  Le lancement automatique de la tâche d'analyse selon un horaire défini (cf. section "Programmation du lancement des tâches de recherche de virus" à la page 78) permet de rechercher la présence éventuelle de virus sur l'ordinateur en temps opportuns. Accessible uniquement pour les tâches **Analyse express**, **Analyse complète** et les tâches d'utilisateur.

- **Lancement de la tâche au nom de l'utilisateur**

  Lancement de la tâche au nom de l'utilisateur privilégié (cf. section "Lancement des tâches d'analyse au nom de l'utilisateur" à la page 79) assure une analyse à temps peut importe les privilèges de l'utilisateur travaillant sur l'ordinateur au moment actuel. Accessible uniquement pour les tâches **Analyse express**, **Analyse complète** et les tâches d'utilisateur.

Outre cela, vous pouvez installer les valeurs uniques des paramètres **Niveau de protection** ou **Action** sur l'objet détecté pour toutes les tâches de recherche de virus (cf. section "Définition de paramètres d'analyse uniques pour toutes les tâches de recherche de virus" à la page 80).

SELECTION DU NIVEAU DE PROTECTION

Chaque tâche d'analyse antivirus s'exécute sur les objets en fonction des niveaux suivants :

- **Protection maximale** pour l'analyse complète en profondeur de votre ordinateur ou d'un disque, d'un répertoire ou d'un dossier particulier. Nous recommandons d'utiliser ce niveau, si vous soupçonner votre ordinateur d'être infecté par un virus.

- **Recommandé** : le niveau dont les paramètres sont recommandés par les experts de Kaspersky Lab.

- **Vitesse maximale** : les paramètres de ce niveau vous permettent d'utiliser confortablement des applications à usage intensif de ressources systèmes, dans la mesure où l'ensemble des fichiers analysés est réduit.

Par défaut, l'exécution des tâches de recherche de virus est réalisée sur le niveau de protection **Recommandé**. Vous pouvez augmenter ou diminuer le fini de l'analyse des objets en sélectionnant conformément le niveau **Protection maximale** ou **Vitesse maximale**, ou en modifiant les paramètres du niveau actuel.

➧ *Pour modifier le niveau de protection de la tâche de recherche de virus, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application (à la page 35) et sélectionnez l'onglet **Analyse** (cf. ill. ci-après).

2. Sélectionnez une tâche dans la liste à gauche.

3. Dans le groupe **Niveau de protection**, déplacez simplement le curseur. Ce faisant, vous modifiez le rapport entre la vitesse de l'analyse et la quantité des fichiers analysés : plus le nombre de fichiers soumis à l'analyse sera réduit, plus la vitesse de l'analyse sera élevée.

Si aucun des niveaux prédéfinis ne répond à vos attentes, vous pouvez procéder à une configuration avancée des paramètres de la protection. Pour ce faire, il est conseillé de choisir le niveau de protection le plus proche de vos besoins en guise de point de départ et d'en modifier les paramètres. Dans ce cas, le nom du niveau de sécurité devient **Utilisateur**.

Pour modifier les paramètres du niveau de protection actuel, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (à la page 35) et sélectionnez l'onglet **Analyse** (cf. ill. ci-après).

2. Sélectionnez une tâche dans la liste à gauche.

3. Dans le groupe **Niveau de protection**, cliquez sur le bouton **Paramètres**.

4. Dans la fenêtre qui s'ouvre, modifiez les paramètres (cf. section "Définition du type d'objet analysé" à la page 76) du niveau de protection et cliquez **OK** pour enregistrer les modifications.

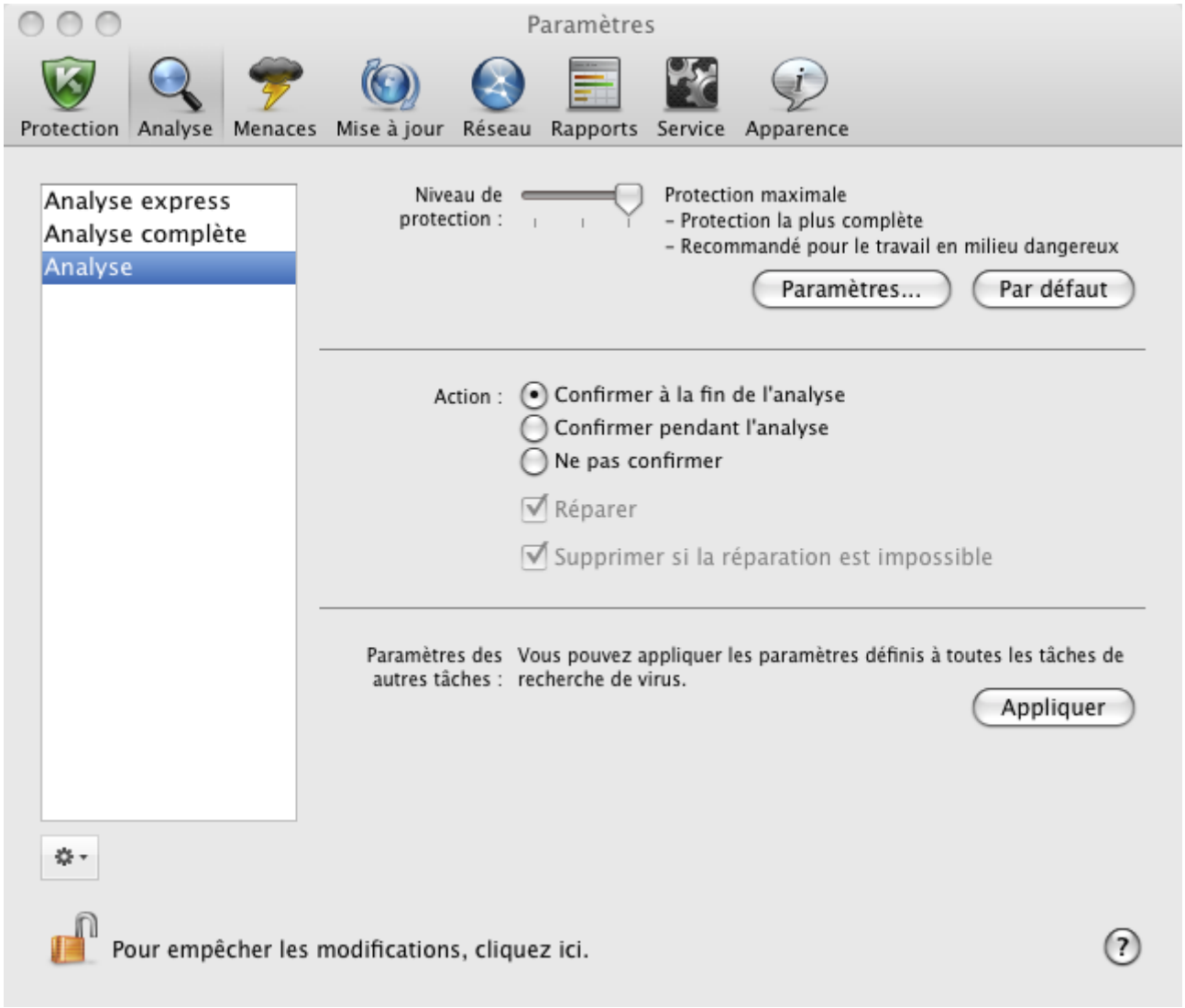


Illustration 34. Fenêtre de configuration de l'application. Tâche Analyse

DEFINITION DU TYPE D'OBJET ANALYSE

La définition du type d'objet à analyser précise le format et la taille des fichiers qui seront analysés par Kaspersky Endpoint Security lors de l'exécution de cette tâche.

Pour indiquer le type d'objets analysés lors de l'exécution de la tâche de recherche de virus, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (à la page 35) et sélectionnez l'onglet **Analyse**.
2. Sélectionnez une tâche dans la liste à gauche.
3. Dans le groupe **Niveau de protection**, cliquez sur le bouton **Paramètres**. Dans la fenêtre qui s'ouvre (cf. ill. ci-après), configurez les paramètres suivants :
   - Indiquez, dans le groupe **Types de fichiers**, le format des fichiers qui seront analysés par Kaspersky Endpoint Security dans le cadre de la tâche de recherche de virus.
   - Dans le groupe **Optimisation**, configurez les performances de l'analyse et l'utilisation des technologies d'analyse.
   - Dans le groupe **Fichiers composés**, sélectionnez quels sont les fichiers composés à analyser.
   - Dans le groupe **Analyseur heuristique**, configurez l'utilisation de l'analyseur heuristique dans les tâches d'analyse.

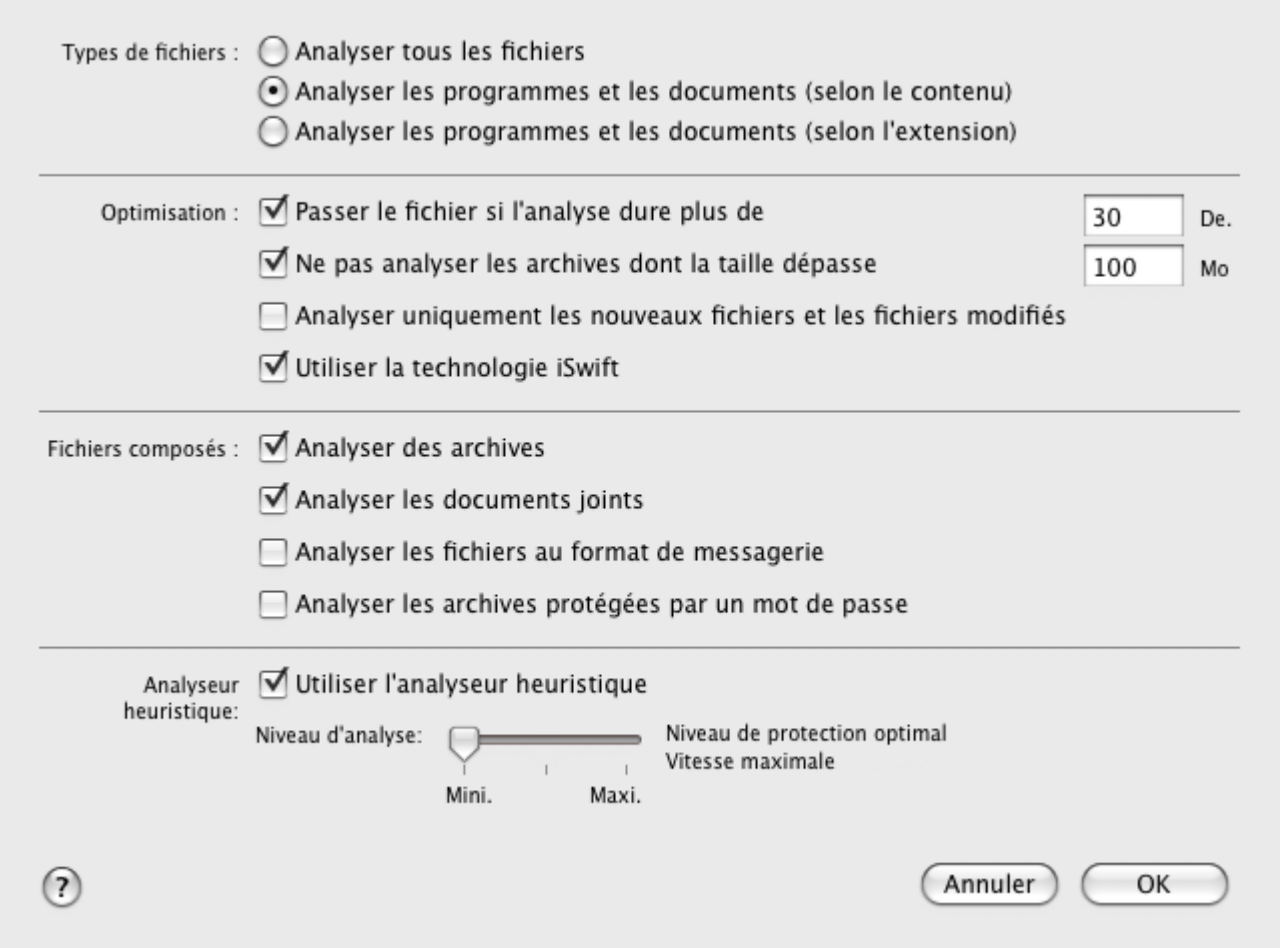


Illustration 35. Analyse. Configuration de l'analyse

SELECTION DES ACTIONS A REALISER SUR LES OBJETS

Si à la fin de l'exécution de la tâche de recherche de virus, il se trouve qu'un objet quelconque est infecté ou potentiellement infecté, le comportement suivant de Kaspersky Endpoint Security dépendra de l'état de l'objet et de l'action sélectionnée.

A la fin de l'analyse, chaque objet peut se voir attribuer un des statuts suivants :

- état de l'un des programmes malveillants (exemple, *virus*, *cheval de Troie*) ;
- état *probablement infecté* lorsqu'il est impossible d'affirmer avec certitude si l'objet est infecté ou non. Cela signifie que le fichier contient la séquence du code d'un virus inconnu ou le code modifié d'un virus connu.

Par défaut, tous les objets malveillants sont réparés et tous les objets probablement infectés sont placés en quarantaine (cf. section "Quarantaine" à la page 94).

Pour sélectionner une action à effectuer par Kaspersky Endpoint Security lors de la détection d'un objet infecté ou potentiellement infecté, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (à la page 35), sélectionnez l'onglet **Analyse** et le nom de la tâche de recherche de virus dans la liste des tâches à gauche (cf. ill. ci-après).

2. Dans le groupe **Action**, sélectionnez l'action de Kaspersky Endpoint Security.

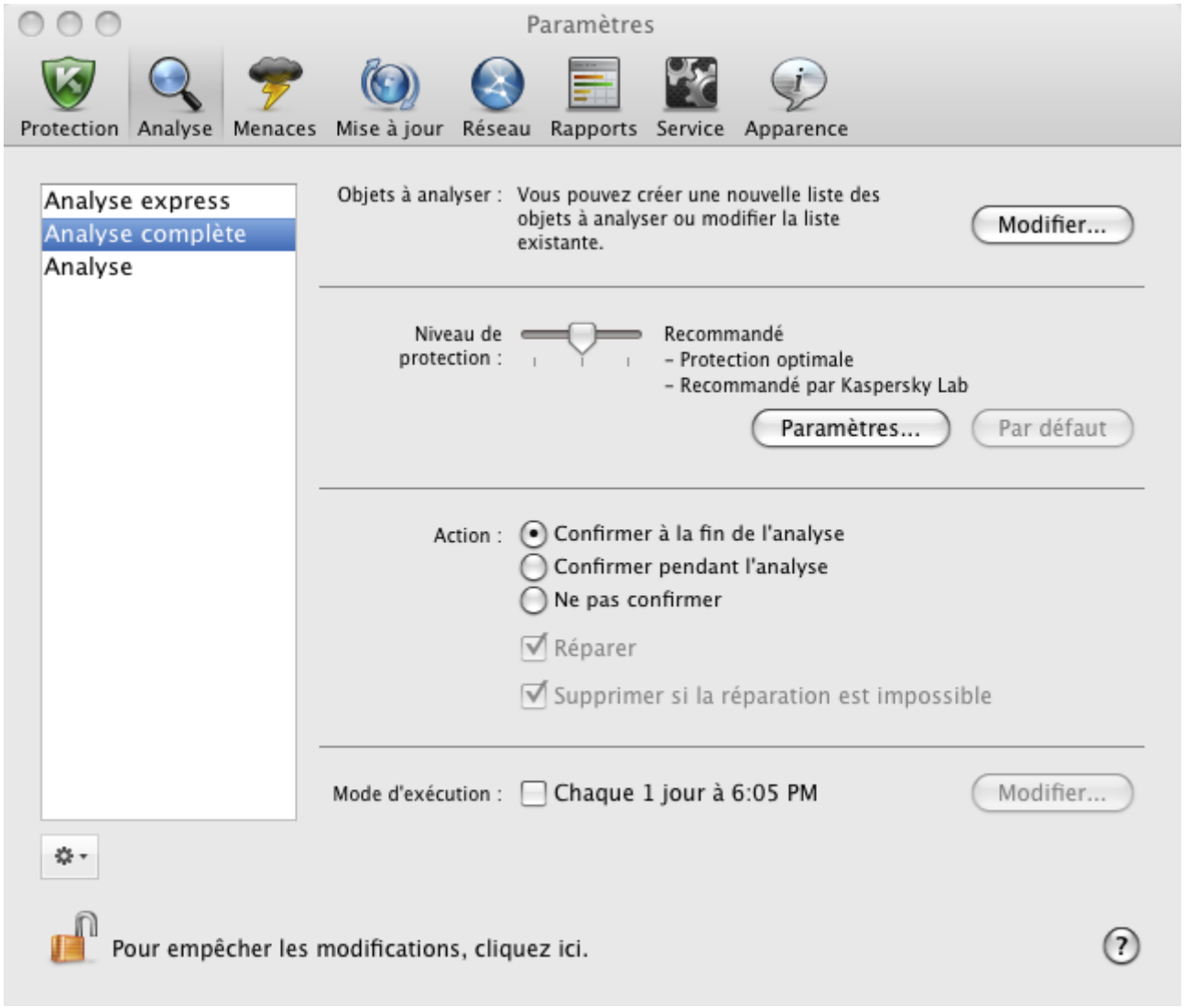


Illustration 36. Fenêtre de configuration de l'application. Tâche Analyse complète

Avant toute réparation ou suppression d'un objet, Kaspersky Endpoint Security crée une copie de sauvegarde et la place dans le dossier de sauvegarde (à la page 97) au cas où il faudrait restaurer l'objet ou s'il devenait possible de le réparer.

CONFIGURATION DE L'EXECUTION PROGRAMMEE DE L'ANALYSE

Vous pouvez lancer à la main (cf. section "Lancement/arrêt des tâches liées à la recherche de virus" à la page 68) toutes les tâches de recherche de virus sur votre ordinateur. Outre cela, les tâches **Analyse express** et **Analyse complète** et les tâches créées par l'utilisateur peuvent être lancées par Kaspersky Endpoint Security selon la programmation prédéfinie.

➧ *Pour configurer le lancement des tâches **Analyse express** et **Analyse complète**, ainsi que des tâches utilisateurs de recherche de virus selon la programmation, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application (à la page 35) et sélectionnez l'onglet **Analyse**.

2. Dans la liste de gauche, sélectionnez le nom de la tâche d'analyse, puis dans le groupe **Mode d'exécution**, activez le lancement de la tâche programmé. Cliquez sur le bouton **Modifier** pour configurer les paramètres de lancement de la tâche.

3. Dans la fenêtre ouverte (cf. ill. ci-après), indiquez la fréquence de lancement de la tâche.

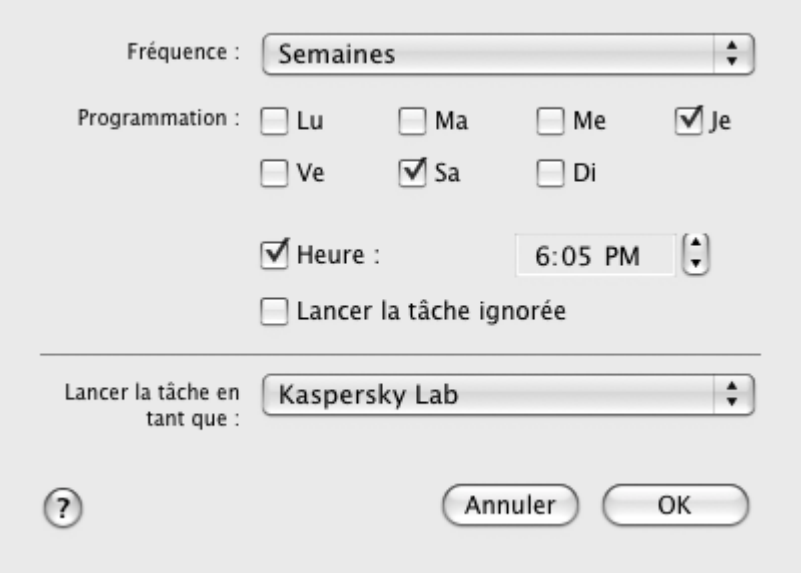


Illustration 37. Programmation du lancement des tâches de recherche de virus

LANCEMENT DES TACHES D'ANALYSE AU NOM DE L'UTILISATEUR

La possibilité de lancement des tâches de recherche de virus par l'utilisateur de la part d'un autre compte utilisateur a été réalisée dans cette application. Ceci assure l'opportunité de l'analyse de l'ordinateur peu importe les privilèges de l'utilisateur qui travaille sur l'ordinateur dans ce moment. Par exemple, les privilèges d'accès à l'objet analysé peuvent être requises lors de l'exécution d'une tâche d'analyse. En utilisant ce service, vous pouvez programmer le lancement d'une tâche de recherche de virus au nom de l'utilisateur possédant de tels privilèges.

Par défaut, ce service est désactivé et les tâches sont lancées au nom du compte utilisateur actuel sous lequel vous êtes enregistrés dans le système d'exploitation.

Vous pouvez configurer le lancement de tâches de recherche de virus du nom de l'utilisateur privilégié uniquement pour les tâches **Analyse express** et **Analyse complète**, ainsi que pour les tâches d'utilisateur de recherche créées sur leur *base.

Pour créer un compte depuis lequel les tâches de recherche de virus seront lancées, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (à la page 35) sélectionnez l'onglet **Analyse**.

2. Dans la liste de gauche, sélectionnez le nom de la tâche d'analyse, puis dans le groupe **Mode d'exécution**, activez le lancement de la tâche programmé. Cliquez sur le bouton **Modifier** afin de configurer le lancement de la tâche au nom d'un utilisateur.

3. Dans la fenêtre ouverte (cf. ill. ci-après) dans le groupe **Lancer la tâche en tant que** choisissez un compte utilisateur de la liste déroulante au nom duquel la tâche sera lancée.

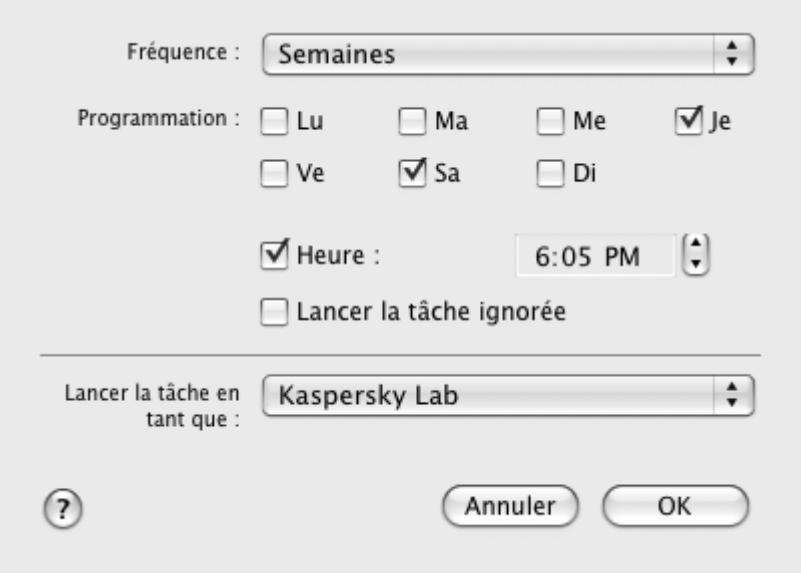


Illustration 38. Programmation du lancement des tâches de recherche de virus

DEFINITION DE PARAMETRES D'ANALYSE UNIQUES POUR TOUTES LES TACHES DE RECHERCHE DE VIRUS

Par défaut, les tâches de recherche de virus comprises dans Kaspersky Endpoint Security sont exécutées conformément aux paramètres recommandés par les experts de Kaspersky Lab. Les tâches d'utilisateur de recherche créées sur leur base héritent tous les paramètres installées. Vous pouvez non seulement modifier les paramètres (cf. section "Configuration des tâches liées à la recherche de virus" à la base 74) de chaque tâche de recherche de virus en particulier, mais aussi indiquer les paramètres uniques de l'analyse pour toutes les tâches de recherche de virus. Les valeurs des paramètres **Niveau de protection** et **Action** de la tâche **Analyse** conçue pour analyser un objet en particulier seront prises pour base.

➧ *Afin de définir les paramètres d'analyse uniques pour toutes les tâches de recherche de virus, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application (à la page 35) et sélectionnez l'onglet **Analyse**.

2. Dans la liste à gauche, sélectionnez la tâche **Analyse** (cf. ill. ci-après)**.**

3. Indiquez le niveau de protection (cf. section "Sélection du niveau de protection" à la page 74) le plus proche à vos exigences, modifiez ses paramètres (cf. section "Définition du type d'objet analysé" à la page 76) et sélectionnez l'action sur les objets infectés ou potentiellement infectés (cf. section "Sélection des actions à réaliser sur les objets" à la page 77).

4. Dans le groupe **Paramètres des autres tâches**, cliquez sur le bouton **Appliquer**. Kaspersky Endpoint Security applique les valeurs des paramètres **Niveau de protection** et **Action** aux autres tâches d'analyse, y compris celles définies par les utilisateurs.

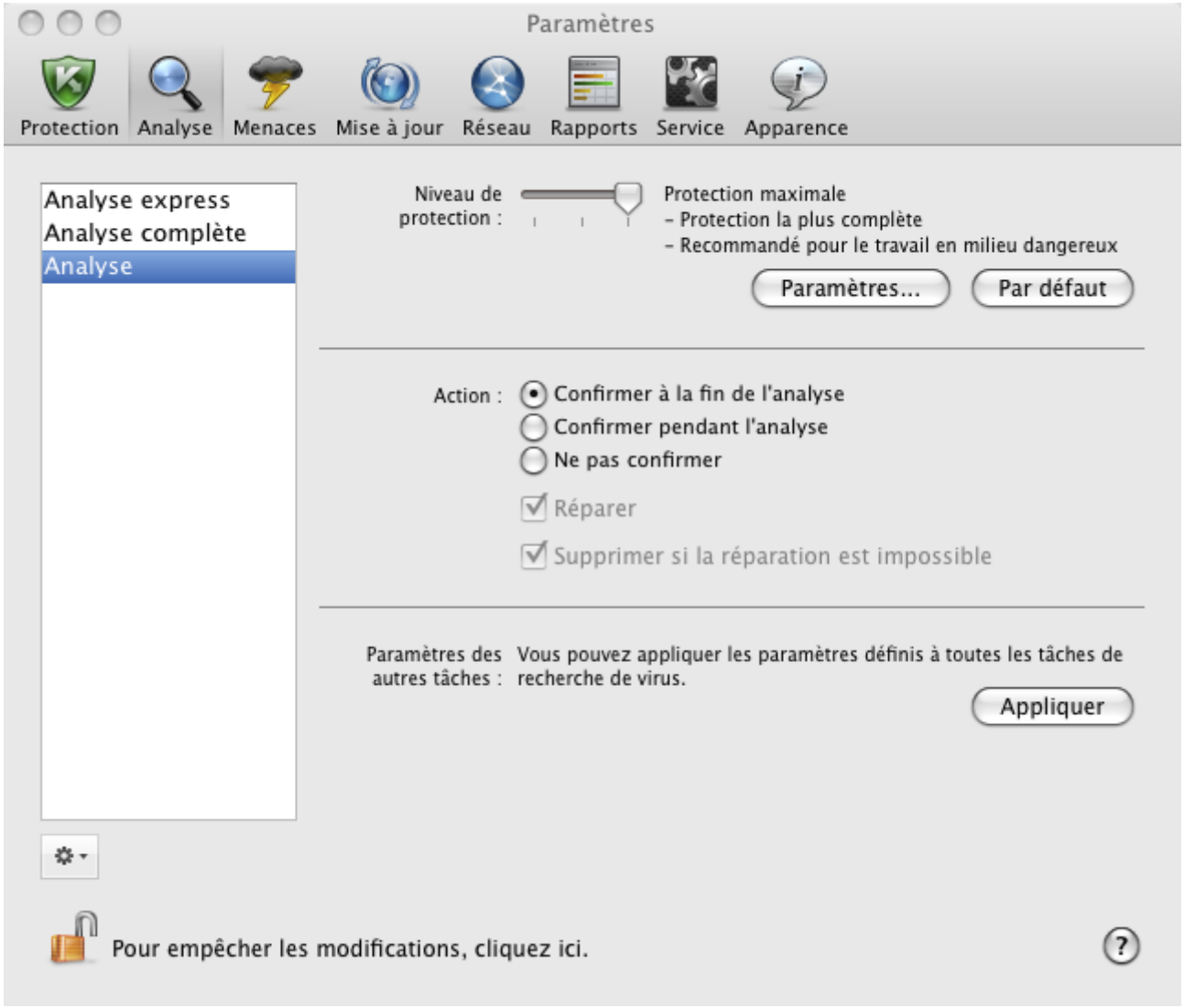


Illustration 39. Fenêtre de configuration de l'application. Tâche Analyse

RESTAURATION DES PARAMETRES D'ANALYSE PAR DEFAUT

En tout moment, vous pouvez retourner aux paramètres des tâches de recherche de virus par défaut. Il s'agit des paramètres optimums recommandés par les experts de Kaspersky Lab et regroupés au sein du niveau de protection **Recommandé**.

Pour restaurer les paramètres d'analyse des objets par défaut, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (à la page 35), sélectionnez l'onglet **Analyse**, puis le nom de la tâche requise dans la liste de gauche.

2. Dans le groupe **Niveau de protection** (cf. ill. ci-après), cliquez sur le bouton **Par défaut**. Les paramètres de la tâche vont retourner aux valeurs recommandées.

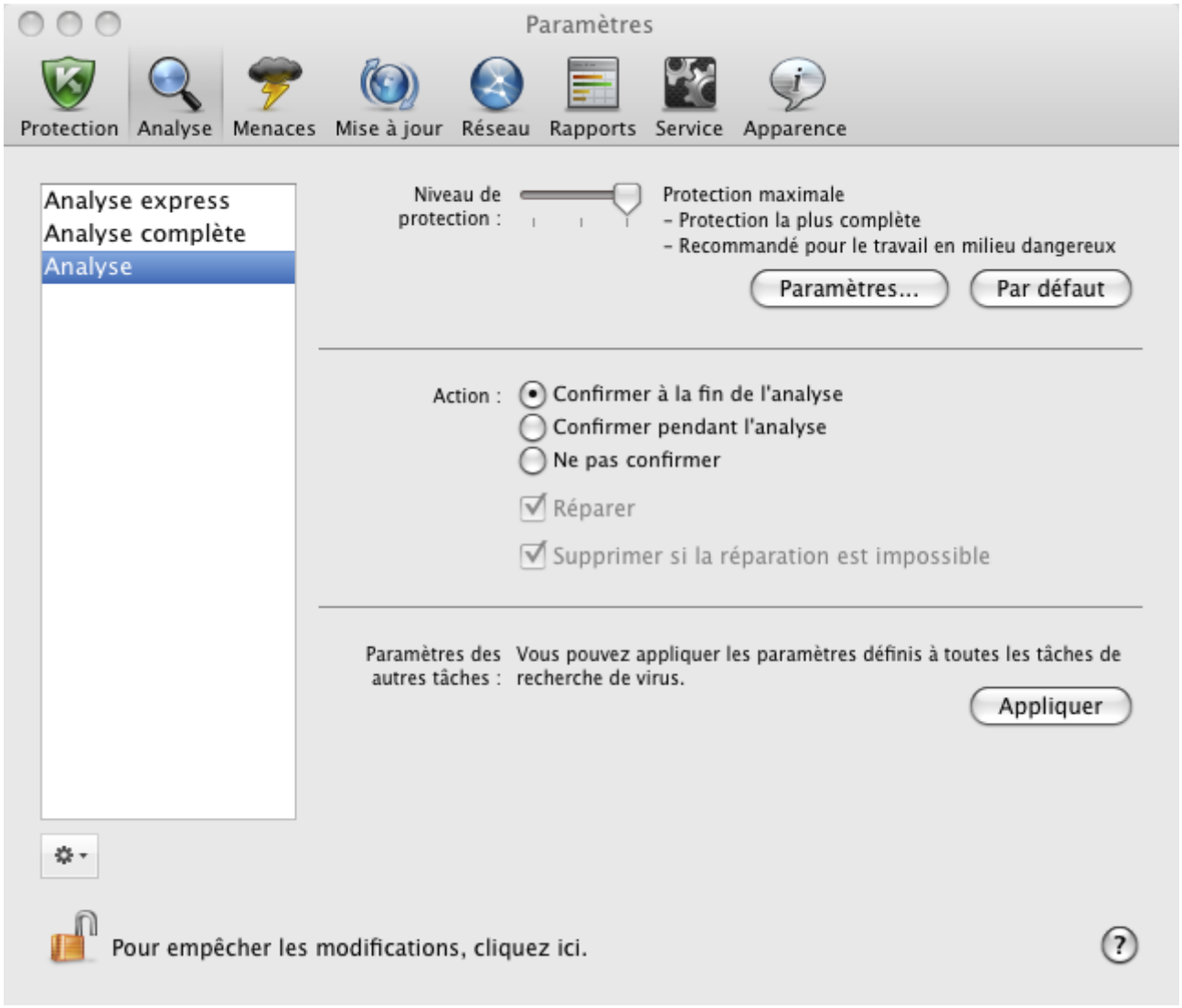


Illustration 40. Fenêtre de configuration de l'application. Tâche Analyse

STATISTIQUES DE LA RECHERCHE DE VIRUS

Les brèves informations sur l'exécution de chaque tâche actuelle de recherche de virus (exprimée en pour cent) sont présentées dans la fenêtre principale de l'application (cf. section "Fenêtre principale de l'application" à la page 33).

Kaspersky Endpoint Security propose également un rapport détaillé sur l'exécution des tâches d'analyse.

Pour consulter le rapport sur l'exécution de la tâche en cours, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (à la page 33) et cliquez sur le bouton  .

2. Dans la rubrique **Tâches exécutées** de la fenêtre des rapports qui s'ouvre, sélectionnez le nom de la tâche qui vous intéresse.

Si la tâche de recherche de virus est déjà terminée, alors les informations sur les résultats de son exécution sont présentées dans la section **Tâches terminées**.

Dans la partie inférieure de la fenêtre des rapports, les informations sur l'exécution de la tâche actuelle ou les statistiques de synthèse avec les résultats de la tâche terminée de recherche de virus sont affichées. Les statistiques présentent des données sur le nombre d'objets analysés, le nombre de menaces découvertes et le nombre d'objets devant être traités. Vous trouverez également l'heure de début de l'analyse, la fin escomptée et sa durée.

Si des erreurs se sont produites pendant l'exécution de la tâche, lancez la tâche à nouveau. Si la tentative réitérative d'exécution de l'analyse se solde sur un échec, contactez le Service d'assistance technique (cf. section "Contacter le Service d'assistance technique" à la page 157).

Les informations détaillées sur l'exécution des tâches de recherche de virus sont présentées dans la fenêtre des rapports, sous les onglets suivants :

- L'onglet **Détectés** reprend tous les objets dangereux détectés durant le processus d'exécution de la tâche. Pour chaque objet, le nom et le chemin d'accès au dossier (où l'objet a été enregistré) sont indiqués, ainsi que l'état attribué à cet objet par Kaspersky Endpoint Security. Si le programme a pu définir exactement le programme malveillant qui a infecté l'objet, il recevra l'état, par exemple : *virus*, *cheval de Troie*, etc. S'il est impossible de définir avec exactitude le type de programme malveillant, l'objet recevra le statut *suspect*. En plus de l'état, le rapport reprend également les informations relatives à l'action exécutée sur l'objet (*découvert*, *réparé*).

- L'onglet **Evénements** reprend la liste complète des événements apparaissant pendant l'exécution de la tâche de recherche de virus avec l'indication de l'heure de survenance de l'événement, son nom, état et causes d'apparition. Les événements prévus sont :

  - *événement informatif* (par exemple : l'objet n'a pas été traité : ignoré selon le type) ;

  - *avertissement* (par exemple : découverte d'un virus) ;

  - *remarque* (par exemple : archive protégée par un mot de passe).

- L'onglet **Statistiques** reprend les informations sur le nombre total d'objets analysés, et dans les colonnes séparées vous retrouverez le nombre d'objets parmi le nombre total d'objets en cours d'analyse étant les archives, les objets dangereux, réparés, placés en quarantaine, etc.

- L'onglet **Paramètres** reprend les paramètres généraux conformément auxquels la tâche de recherche de virus se réalise. Pour passer rapidement à la configuration des paramètres de recherche, cliquez sur le bouton **Modifier les paramètres**.

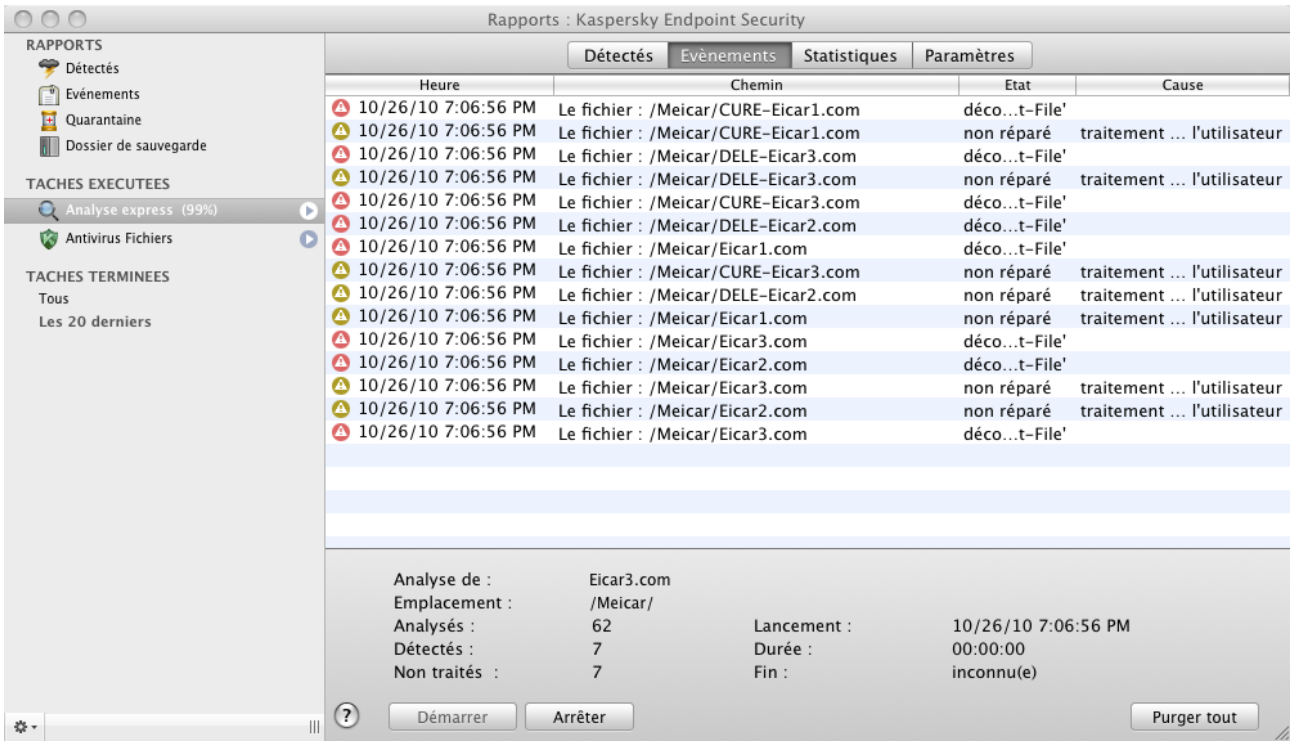


Illustration 41. Fenêtre des rapports. Analyse

MISE A JOUR DE L'APPLICATION

L'actualité des bases antivirus est le garant de la sécurité de votre ordinateur. Chaque jour, de nouveaux virus, chevaux de Troie et autres programmes malveillants apparaissent. Il est donc primordial de s'assurer que vos données sont bien protégées.

La mise à jour de Kaspersky Endpoint Security suppose le téléchargement et l'installation sur votre ordinateur des éléments suivants :

- **Les bases antivirus de l'application**

  La protection de données sur l'ordinateur s'assure à l'aide des bases antivirus. L'Antivirus Fichiers (à la page 56) et les tâches de recherche de virus (cf. section "Analyse" à la page 68) les utilisent pour la recherche et la neutralisation des objets malveillants sur votre ordinateur. Les bases antivirus sont enrichies chaque jour par les définitions des nouvelles menaces et les moyens de lutter contre celles-ci. Il est par conséquent vivement recommandé de les actualiser régulièrement.

- **Modules de l'application**

  En plus des bases, vous pouvez actualiser les modules internes de Kaspersky Endpoint Security. Des paquets de mises à jour sont diffusés régulièrement par Kaspersky Lab.

Les serveurs de mise à jour de Kaspersky Lab et le Serveur d'administration Kaspersky Administration Kit sont les sources principales pour les mises à jour de Kaspersky Endpoint Security.

Pour réussir le téléchargement des mises à jour depuis les serveurs, la connexion de l'ordinateur à Internet est requise. Si la connexion à Internet s'opère par un serveur proxy, il faudra alors configurer les paramètres du réseau (cf. section "Configuration des paramètres de connexion au serveur proxy" à la page 91).

Si vous ne pouvez accéder aux serveurs de mise à jour de Kaspersky Lab (par ex. : pas de connexion à Internet), vous pouvez contacter le Service d'assistance technique de Kaspersky Lab (cf. section "Contacter le Service d'assistance technique" à la page 157) qui pourra vous donner la mise à jour de Kaspersky Endpoint Security sur CD-ROM dans un fichier ZIP.

Le téléchargement des mises à jour s'opère selon l'un des modes suivants :

- *Automatique*. Kaspersky Endpoint Security vérifie à intervalle régulier si des mises à jour sont disponibles sur la source des mises à jour. L'intervalle de vérification peut être réduit en cas d'épidémie et agrandi en situation normale. Lorsque Kaspersky Endpoint Security découvre de nouvelles mises à jour, il les télécharge en arrière-plan et les installe sur l'ordinateur. Ce mode est utilisé par défaut.

- *Selon la programmation*. La mise à jour de Kaspersky Endpoint Security se produit automatiquement selon l'horaire défini.

- *Manuel*. Vous lancez vous-même la procédure de mise à jour de Kaspersky Endpoint Security.

Durant la mise à jour, les modules de l'application et les bases antivirus sur votre ordinateur sont comparés avec les modules et les bases accessibles à ce moment dans la source de la mise à jour. Si la dernière version des bases et des modules a été installée sur votre ordinateur, alors l'enregistrement sur le fait, que les bases antivirus sont en état actuel, apparaîtra dans la fenêtre principale de l'application (cf. section "Fenêtre principale de l'application" à la page 33). Si les bases et les modules diffèrent de ceux qui sont présents sur la source de mises à jour, seule la partie manquante de la mise à jour sera installée sur votre ordinateur. Les bases et les modules ne sont pas copiés en entier, ce qui accélère la mise à jour et réduit le volume du trafic de réseau.

Avant la mise à jour des bases et des modules, Kaspersky Endpoint Security crée leur copie de sauvegarde, au cas où il sera nécessaire de revenir à l'utilisation de la version précédente. La possibilité de revenir à l'état antérieur à la mise à jour (cf. section "Annulation de la dernière mise à jour" à la page 85) est utile, par exemple, si la nouvelle version des bases contient une signature incorrecte qui entraîne le blocage d'une application inoffensive par Kaspersky Endpoint Security.

Lors de la corruption des bases, Kaspersky Endpoint Security recommande de lancer la tâche de mise à jour, pour télécharger l'ensemble actuel des bases pour la protection actuelle.

Parallèlement à la mise à jour de Kaspersky Endpoint Security, vous pouvez copier les mises à jour obtenues dans une source locale (cf. section "Mise à jour depuis une source locale" à la page 86). Ce service permet d'actualiser localement les bases antivirus de Kaspersky Endpoint Security et les modules utilisés par l'application sur d'autres ordinateurs afin de limiter le trafic Internet.

DANS CETTE SECTION

LANCEMENT DE LA MISE A JOUR

La mise à jour en temps utiles de Kaspersky Endpoint Security permet de maintenir la protection de l'ordinateur au niveau requis. Si la mise à jour des bases antivirus et des modules de l'application ne se réalise pas, les informations sur votre ordinateur sont soumises au sérieux danger.

La partie inférieure de la fenêtre principale de l'application (cf. section "Fenêtre principale de l'application" à la page 33) reprend les informations suivantes sur la mise à jour de Kaspersky Endpoint Security : date d'édition des bases, nombre d'enregistrements dans les bases installées sur votre ordinateur, ainsi que données sur l'actualité des bases utilisées. Le nombre d'enregistrement dans les bases reflète le nombre de menaces connues en ce moment, contre lesquelles l'ordinateur est protégé.

Pendant l'utilisation de Kaspersky Endpoint Security, vous pouvez actualiser l'application à tout moment. Pour ce faire, cliquez sur le bouton  dans la fenêtre principale. Les informations détaillées sur l'exécution de cette tâche sont présentées dans la fenêtre des rapports (cf. section "Rapports" à la page 98).

Parallèlement à l'obtention des mises à jour depuis les serveurs de Kaspersky Lab ou depuis le Serveur d'administration Kaspersky Administration Kit, leur copie dans une source locale (cf. section "Mise à jour depuis une source locale" à la page 86) serait exécutée, à condition, si ce service était activé.

ANNULATION DE LA DERNIERE MISE A JOUR

Chaque fois que vous lancez la mise à jour, Kaspersky Endpoint Security crée d'abord une copie de sauvegarde de la version actuelle des bases antivirus et des modules de l'application utilisés, et procède seulement ensuite à leur actualisation. Ce système permet, le cas échéant, de revenir à l'état antérieur à la mise à jour. La possibilité de revenir à l'état antérieur de la mise à jour est utile, par exemple, si la nouvelle version des bases contient la signature incorrecte, à cause de laquelle Kaspersky Endpoint Security bloque l'application protégée.

Lors de la corruption des bases, Kaspersky Endpoint Security recommande de lancer la tâche de mise à jour, pour télécharger l'ensemble actuel des bases pour la protection actuelle.

➧ *Pour revenir à l'utilisation de la version précédente des bases antivirus, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application (à la page 35) et sélectionnez l'onglet **Mise à jour** (cf. ill. ci-après).

2. Dans le groupe **Annulation de la mise à jour**, cliquez sur le bouton **Annulation de la mise à jour**.

Les résultats de l'exécution de la remise à l'état antérieur de la mise à jour seront affichés dans la fenêtre des rapports (cf. section "Statistiques de la mise à jour" à la page 92).

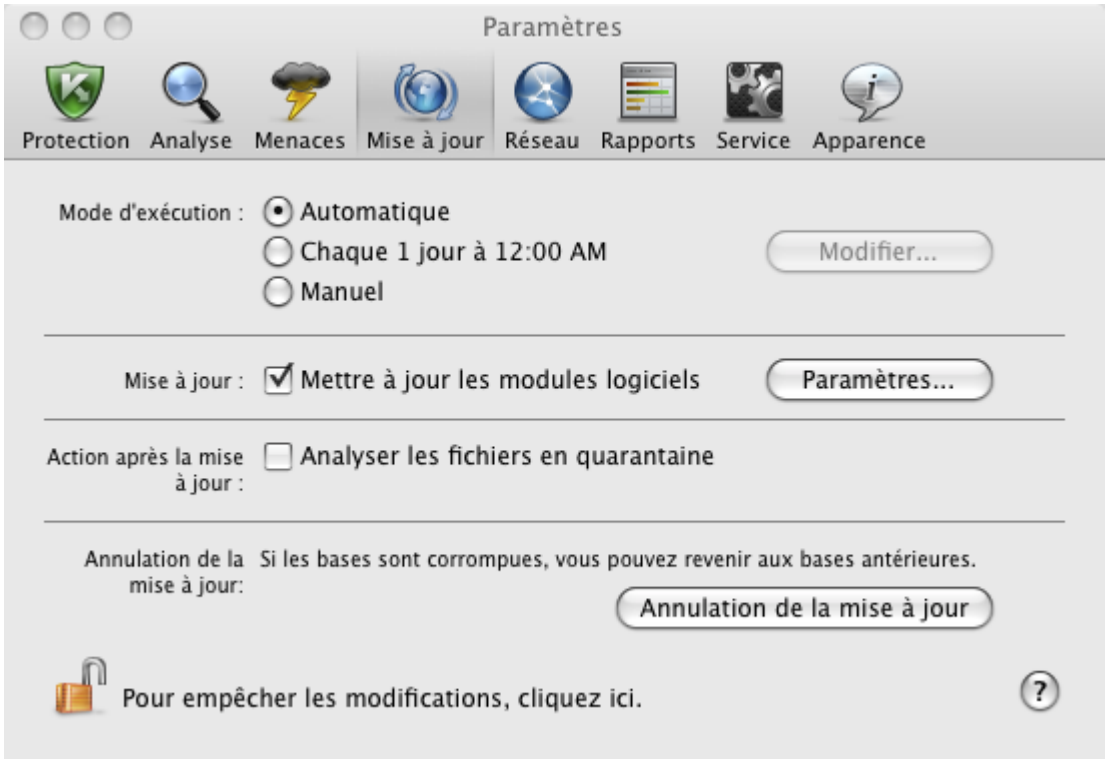


Illustration 42. Fenêtre de configuration de l'application. Mise à jour

MISE A JOUR DEPUIS UNE SOURCE LOCALE

Si plusieurs ordinateurs sont réunis dans un réseau local, il n'est pas nécessaire d'obtenir des mises à jour de Kaspersky Endpoint Security pour chaque ordinateur en particulier, puisque dans ce cas le trafic de réseau augmente considérablement. Vous pouvez utiliser le service de copie des mises à jour obtenues. Ceci permettra d'actualiser localement les bases antivirus de Kaspersky Endpoint Security et les modules utilisés par l'application sur d'autres ordinateurs afin de réduire le trafic Internet. La procédure d'obtention des mises à jour sera organisée de manière suivante :

1. Un des ordinateurs du réseau récupère les mises à jour pour Kaspersky Endpoint Security sur les serveurs de Kaspersky Lab ou sur le Serveur d'administration Kaspersky Administration Kit ou sur tout autre serveur en ligne proposant les mises à jour les plus récentes. Les mises à jour ainsi obtenues sont enregistrées dans un dossier partagé.

   Il faut créer préalablement un dossier partagé.

2. Les autres ordinateurs du réseau s'adressent au dossier partagé en tant que source des mises à jour pour obtenir des mises à jour.

Pour activer le service de copie des mises à jour dans une source locale, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (à la page 35) et sélectionnez l'onglet **Mise à jour** (cf. ill. ci-après).

2. Dans la rubrique **Mise à jour**, cliquez sur le bouton **Paramètres**.

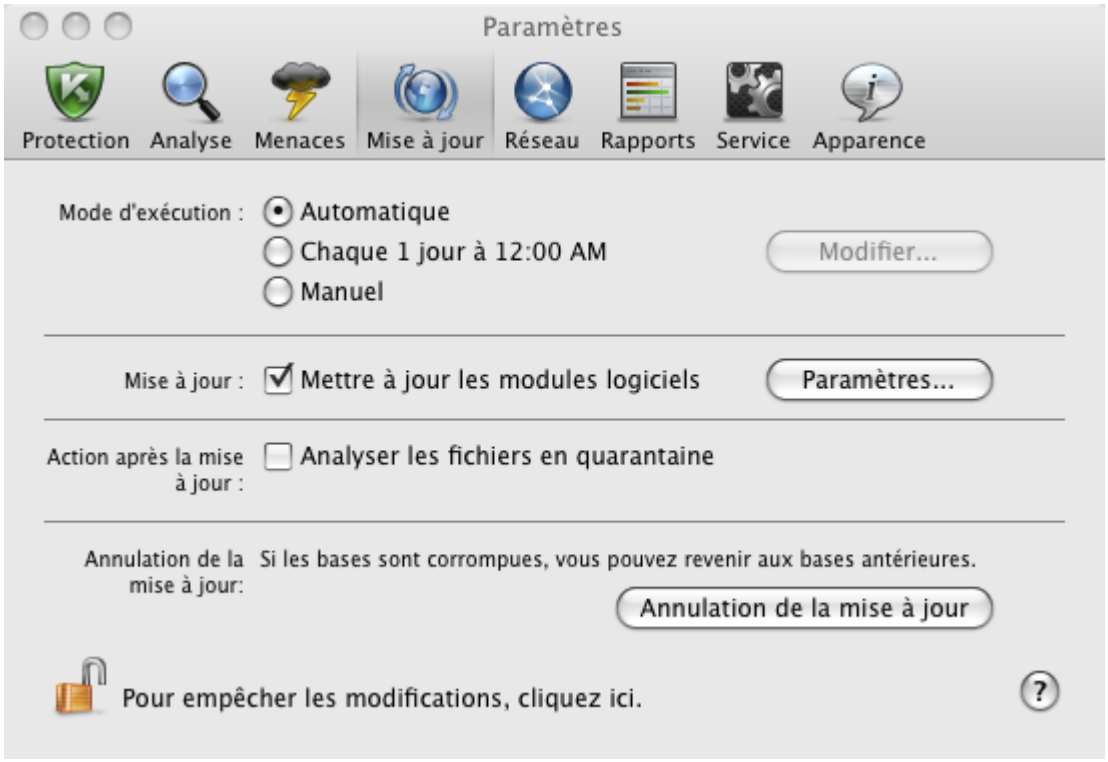


Illustration 43. Fenêtre de configuration de l'application. Mise à jour

3. Dans la fenêtre qui s'ouvre, sélectionnez l'onglet **Avancé** (cf. ill. ci-après). Cochez la case **Copier dans le répertoire**, cliquez sur le bouton **Sélectionner**.

4. Dans la fenêtre ouverte standard, sélectionnez le dossier partagé à conserver les mises à jour obtenues.

Kaspersky Endpoint Security ne reçoit sur les serveurs de mise à jour de Kaspersky Lab ou sur le Serveur d'administration Kaspersky Administration Kit que ses propres paquets de mises à jour.

Illustration 44. Configuration du service de copie des mises à jour

CONFIGURATION DE LA MISE A JOUR

La mise à jour de Kaspersky Endpoint Security est exécutée conformément aux paramètres suivants :

- **Mode d'exécution**

  Le choix du mode de lancement d'une mise à jour détermine la manière dont la mise à jour va être lancée : automatiquement (mode recommandé par les experts de Kaspersky Lab), manuellement ou selon une programmation définie. En cas de sélection de la dernière option, il faudra programmer le lancement de la tâche de mise à jour (cf. section "Programmation du lancement des tâches de mise à jour" à la page 91).

- **Objet de mise à jour**

  L'objet de mise à jour désigne l'élément qui va être actualisé : uniquement les bases antivirus ou les bases et les modules de l'application. Les bases de Kaspersky Endpoint Security sont toujours actualisées tandis que les modules sont actualisés uniquement si la case correspondante a été cochée (cf. section "Sélection du mode et des objets de la mise à jour" à la page 88).

- **Source des mises à jour**

  La source des mises à jour est la ressource contenant les fichiers d'actualité des bases antivirus et des modules de Kaspersky Endpoint Security. La source de mises à jour peut être le serveur HTTP ou FTP, voire un répertoire local ou de réseau.

- **Paramètres du réseau**

  La connexion de l'ordinateur à Internet est requise pour le téléchargement réussi des mises à jour depuis les serveurs de mises à jour de Kaspersky Lab ou d'autres sources de mises à jour, sauf les dossiers locaux ou de réseau. Si la connexion à Internet s'opère par un serveur proxy, il faudra alors configurer les paramètres du réseau (cf. section "Configuration des paramètres de connexion au serveur proxy" à la page 91).

SELECTION DU MODE ET DES OBJETS DE LA MISE A JOUR

Au moment de configurer les paramètres de la mise à jour de Kaspersky Endpoint Security, il est important de désigner l'objet et le mode d'exécution de la mise à jour.

Pour sélectionner le mode de lancement d'une mise à jour, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (à la page 35) et sélectionnez l'onglet **Mise à jour** (cf. ill. ci-après).

2. Sélectionnez, dans le groupe **Mode d'exécution**, le mode d'exécution de la tâche de mise à jour.

Pour copier et installer non seulement les bases antivirus, mais aussi les modules de l'application pendant la mise à jour de l'application, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (à la page 35), sélectionnez l'onglet **Mise à jour** (cf. ill. ci-après).

2. Dans le groupe **Mise à jour**, cochez la case **Mettre à jour les modules de l'application**.

Si durant l'exécution de la tâche de mise à jour, les mises à jour des modules de l'application seront accessibles dans la source de mises à jour, Kaspersky Endpoint Security les obtiendra et les appliquera après le redémarrage de l'ordinateur. Les mises à jour téléchargées ne seront pas installées tant que l'ordinateur ne sera pas redémarré. Si la mise à jour suivante de l'application sera disponible avant le redémarrage de l'ordinateur et l'installation des mises à jour antérieure des modules de l'application, seule la mise à jour des signatures des menaces aura lieu.

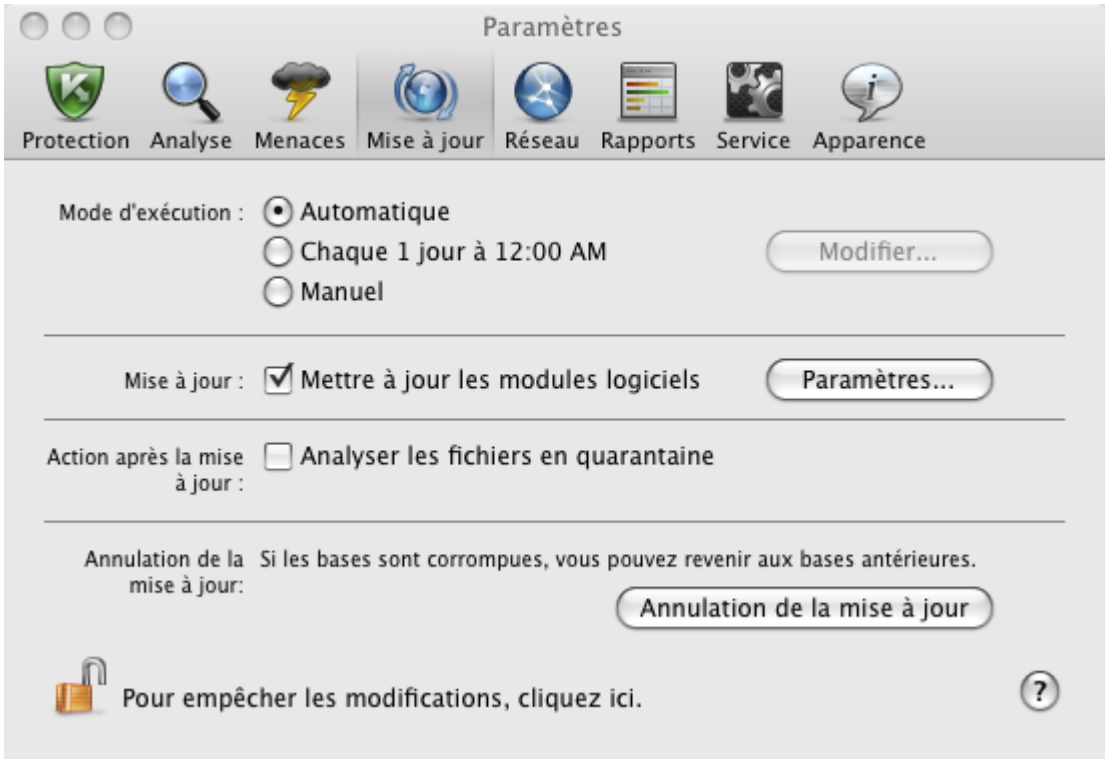


Illustration 45. Fenêtre de configuration de l'application. Mise à jour

SELECTION DE LA SOURCE DE MISES A JOUR

La source des mises à jour est la ressource contenant les fichiers des bases antivirus et des modules internes de Kaspersky Endpoint Security. Il peut s'agir d'un serveur HTTP ou FTP, voire d'un répertoire local ou de réseau.

Les serveurs de mise à jour de Kaspersky Lab constituent la source principale de mises à jour de l'application. Il s'agit de sites Internet spéciaux prévus pour la diffusion des bases antivirus et des modules internes pour tous les produits de Kaspersky Lab. Le Serveur d'administration Kaspersky Administration Kit est aussi la source de mise à jour de Kaspersky Endpoint Security.

Si vous ne pouvez accéder aux serveurs de mise à jour de Kaspersky Lab (par ex. : pas de connexion à Internet), vous pouvez contacter le Service d'assistance technique de Kaspersky Lab, qui pourra vous donner la mise à jour dans un fichier ZIP. Les mises à jour obtenues peuvent être par la suite placées sur un site FTP ou HTPP ou dans un répertoire local ou de réseau.

Lors de la commande des mises à jour sur disque amovible, précisez si vous souhaitez recevoir la mise à jour des modules internes de Kaspersky Endpoint Security.

Pour sélectionner la source de la mise à jour de Kaspersky Endpoint Security, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (à la page 35) et sélectionnez l'onglet **Mise à jour**.
2. Dans la rubrique **Mise à jour**, cliquez sur le bouton **Paramètres**.

3. Dans la fenêtre qui s'ouvre, sélectionnez l'onglet **Source de mises à jour** (cf. ill. ci-après). Modifiez la liste des sources de mises à jour, s'il est nécessaire.

Par défaut, la liste des sources de mises à jour contient uniquement les serveurs de mise à jour de Kaspersky Lab et le Serveur d'administration Kaspersky Administration Kit. En exécutant la mise à jour, Kaspersky Endpoint Security s'adresse à cette liste, sélectionne la première adresse du serveur de la liste et tente de télécharger les mises à jour depuis cette adresse. Si l'adresse sélectionnée ne répond pas, l'application choisit le serveur suivant et tente de télécharger à nouveau les bases antivirus. Ce processus se poursuit tant qu'une connexion n'a pu être établie et tant que toutes les sources disponibles n'ont pas été sondées. La prochaine fois pour obtenir les mises à jour, l'application va s'adresser, en premier lieu, au serveur depuis lequel les mises à jour ont bien été obtenues la fois précédente.

Vous pouvez exécuter les opérations suivantes :

- Ajouter une nouvelle source de mises à jour dans la liste.

  Cliquez sur le bouton [+] et sélectionnez de la liste déroulante l'option qui vous convient le mieux (**Chemin** : pour le dossier de réseau ou local ou **URL** : pour le serveur HTTP ou FTP). Dans la fenêtre ouverte, indiquez l'emplacement d'une nouvelle source de mises à jour.

- Modifier une source de mises à jour.

  Sélectionnez une source de mises à jour dans la liste et cliquez sur le bouton **Modifier**. Saisissez vos modifications dans la fenêtre ouverte.

  N'oubliez pas que les serveurs de mises à jour de Kaspersky Lab et le Serveur d'administration Kaspersky Administration Kit sont les sources qui ne peuvent être modifiées ou supprimées.

- Désactiver temporairement l'obtention des mises à jour depuis une source.

  Sélectionnez une source de mises à jour dans la liste et décochez la case à côté de cette règle. La mise à jour de Kaspersky Endpoint Security depuis cette source ne sera pas exécutée jusqu'à ce que la case ne soit pas cochée de nouveau.

- Supprimer la source de mises à jour.

  Sélectionnez une source de mises à jour dans la liste et cliquez sur le bouton [−].

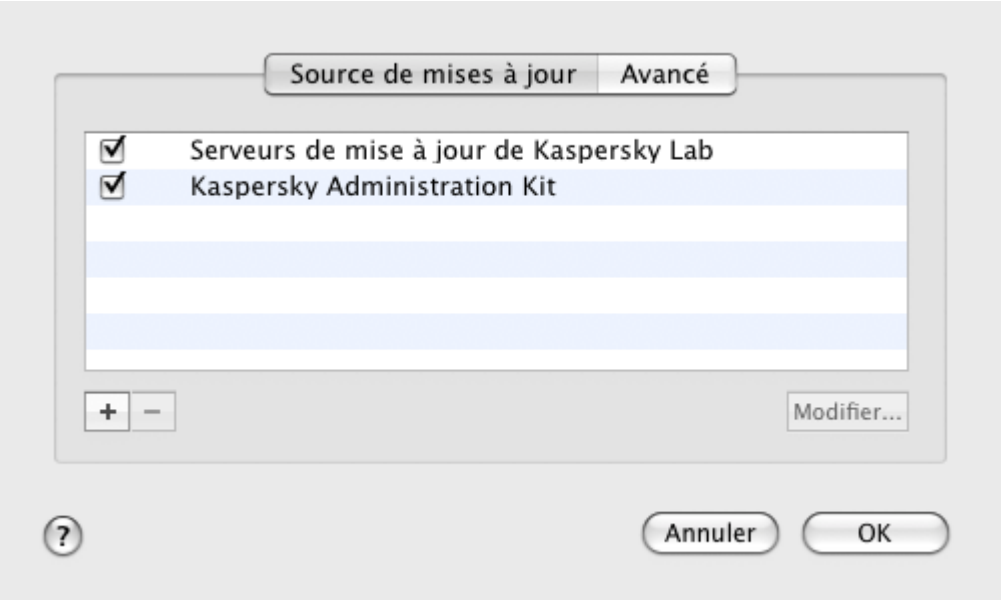


Illustration 46. Sélection de la source de mises à jour

PROGRAMMATION DU LANCEMENT DES TACHES DE MISE A JOUR

Par défaut, la mise à jour de Kaspersky Endpoint Security se réalise automatiquement. Vous pouvez sélectionner un autre mode d'exécution de la tâche de mise à jour : à la main ou selon un horaire défini.

Pour configurer le lancement de la tâche de mise à jour de Kaspersky Endpoint Security selon la programmation, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (à la page 35) et sélectionnez l'onglet **Mise à jour**.

2. Dans le groupe **Mode d'exécution**, sélectionnez l'option du lancement de la mise à jour selon la programmation et cliquez sur le bouton **Modifier**.

3. Dans la fenêtre ouverte (cf. ill. ci-après), indiquez la fréquence de lancement de la mise à jour de l'application.

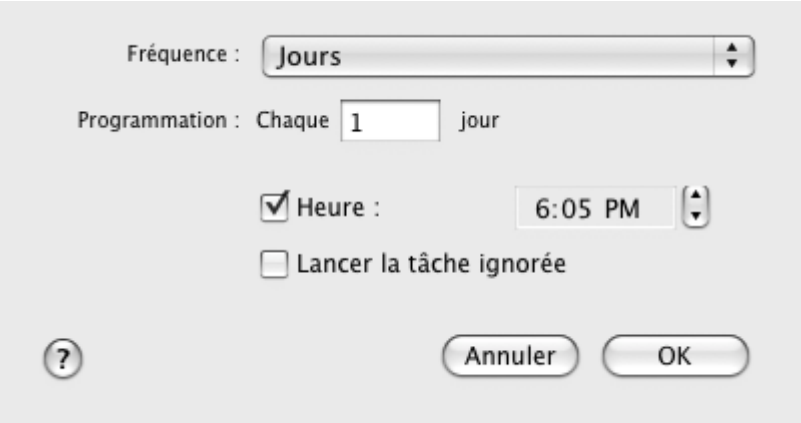


Illustration 47. Programmation du lancement des tâches de mise à jour

CONFIGURATION DES PARAMETRES DE CONNEXION AU SERVEUR PROXY

Si la connexion à Internet s'opère par un serveur proxy, il faudra alors configurer les paramètres de connexion de ce dernier. Kaspersky Endpoint Security utilise ces paramètres pour la mise à jour des bases antivirus et des modules.

Pour configurer les paramètres de connexion au serveur proxy, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (à la page 35) et sélectionnez l'onglet **Réseau** (cf. ill. ci-après).

2. Dans le groupe **Principales**, cochez la case **Utiliser le serveur proxy**.

3. Dans la fenêtre **Serveur proxy**, configurez les paramètres du serveur proxy.

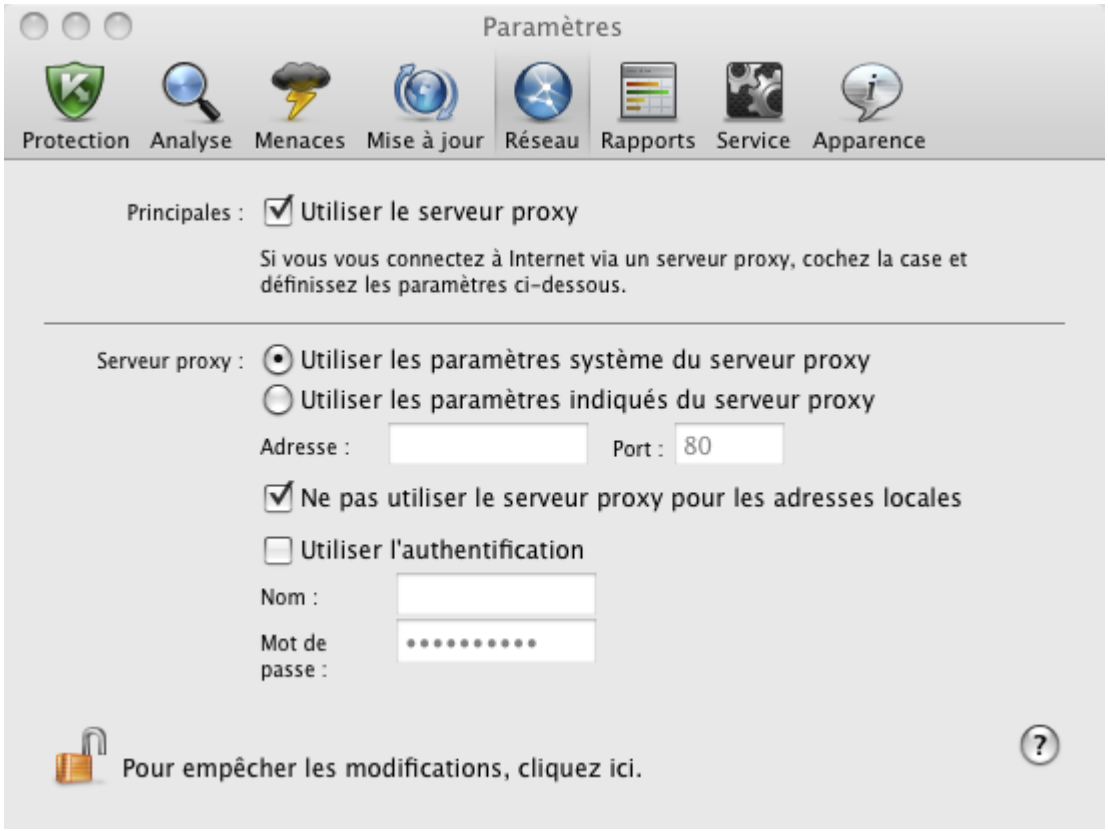


Illustration 48. Fenêtre de configuration de l'application. Réseau

En cas de mise à jour depuis un serveur FTP, la connexion est établie par défaut en mode passif. Si une erreur survient lors de cette connexion, une tentative de connexion en mode actif est lancée.

Par défaut, le temps réservé à l'établissement de la connexion avec le serveur de mise à jour est d'une minute. Si la connexion n'a pas été établie à l'issue de cet intervalle, l'application tentera d'établir la connexion avec la source suivante de mises à jour de la liste. Ce processus se poursuit tant qu'une connexion n'a pu être établie et tant que toutes les sources disponibles n'ont pas été sondées.

STATISTIQUES DE LA MISE A JOUR

Les brèves statistiques sur le fonctionnement actuel du service de mise à jour (date d'édition des bases antivirus, nombre d'enregistrements dans les bases, données sur l'actualité des bases utilisées) sont présentées dans la partie inférieure de la fenêtre principale de l'application (cf. section "Fenêtre principale de l'application" à la page 33).

Les informations relatives à la dernière mise à jour sont absentes si la mise à jour de Kaspersky Endpoint Security n'a pas encore été réalisée.

Kaspersky Endpoint Security propose également un rapport détaillé sur l'exécution de la tâche de mise à jour.

Pour consulter le rapport sur l'exécution de la tâche en cours, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (à la page 33) et cliquez sur le bouton  .

2. Dans la section **Tâches exécutées** de la fenêtre qui s'ouvre, choisissez **Mise à jour**.

Les informations relatives aux mises à jour antérieures figurent dans la section **Tâches terminées.**

Dans la partie inférieure de la fenêtre des rapports, les informations sur l'exécution de la tâche actuelle de mise à jour ou les statistiques de synthèse avec les résultats de la tâche terminée de mise à jour sont affichées. Si la mise à jour a réussi, des statistiques seront présentées, notamment la taille des mises à jour copiées et installées, la vitesse à laquelle la mise à jour a été réalisée, la durée du lancement et de la fin de la mise à jour et la durée d'exécution de la tâche.

Si l'opération n'a pas pu être réalisée, il faut vérifier les paramètres de la mise à jour, du réseau et la disponibilité de la source. Relancez la mise à jour. Si la tentative se solde sur un échec, contactez le Service d'assistance technique (cf. section "Contacter le Service d'assistance technique" à la page 157).

Les informations détaillées sur l'exécution des tâches de mise à jour sont présentées dans la fenêtre des rapports, sous les onglets suivants :

- L'onglet **Evénements** reprend successivement toutes les opérations exécutées durant la mise à jour avec l'indication des noms des objets actualisés, des chemins d'accès aux dossiers où ces objets sont conservés et de l'heure d'appel vers ces objets.

- L'onglet **Paramètres** reprend les paramètres principaux conformément auxquels la mise à jour était réalisée. Pour passer à la configuration des paramètres de la mise à jour, cliquez sur le bouton **Modifier les paramètres**.

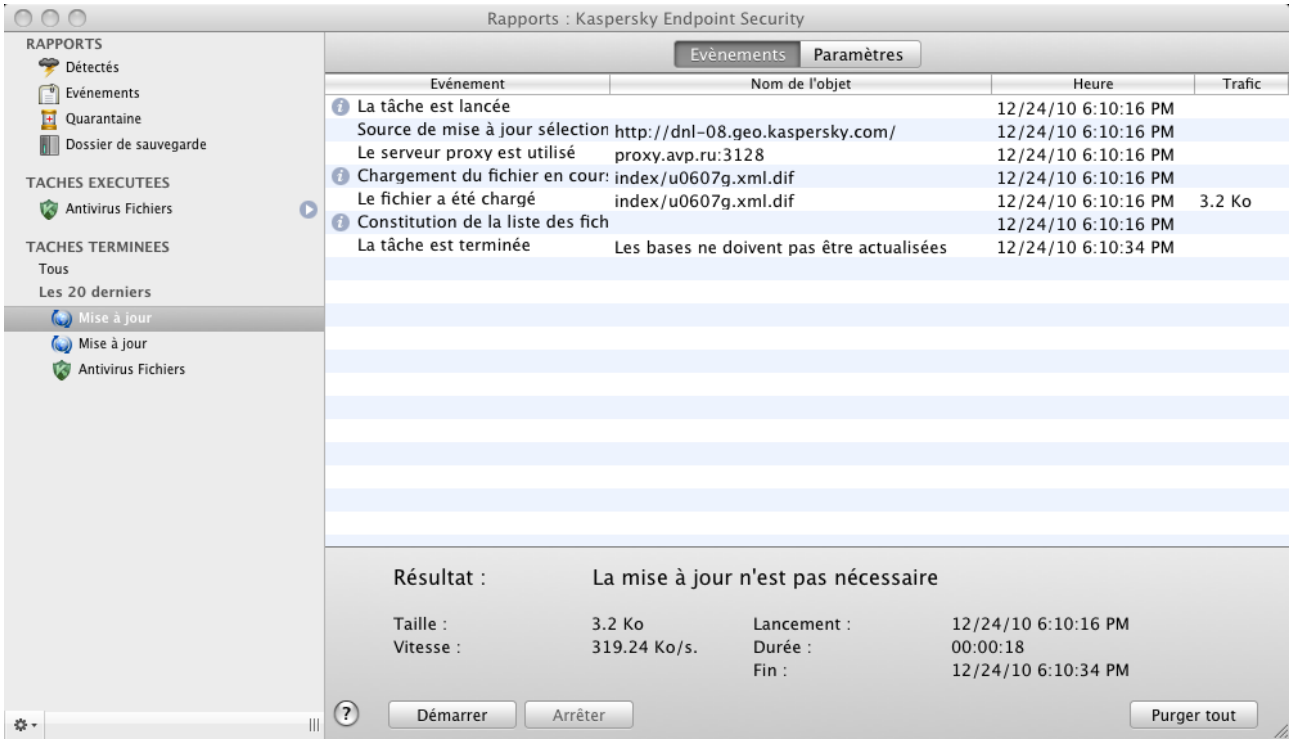


Illustration 49. Fenêtre des rapports. Mise à jour

RAPPORTS ET STOCKAGES

Kaspersky Endpoint Security permet de placer les objets potentiellement infectés dans la quarantaine, de créer une copie des objets infectés dans la sauvegarde avant de les réparer ou de les supprimer et de créer un rapport détaillé sur le fonctionnement de chaque composant de l'application.

DANS CETTE SECTION

QUARANTAINE

La *quarantaine* est un dossier spécial dans lequel on retrouve les objets qui ont peut-être été infectés par des virus.

Les objets potentiellement infectés sont des objets qui ont peut-être été infectés ou modifiés par des virus. L'état *potentiellement infecté* peut être attribué à un objet dans les cas suivants :

- Le code de l'objet analysé est semblable à celui d'une menace connue, mais a été partiellement modifié.

  Les bases antivirus de Kaspersky Endpoint Security contiennent les menaces qui ont été étudiées à ce jour par les experts de Kaspersky Lab. Si les bases ne contiennent pas encore les informations relatives à une modification d'un programme malveillant, alors Kaspersky Endpoint Security classe l'objet infecté par cette modification dans les objets potentiellement infectés et indique à quelle menace ressemble cette infection.

- Le code de l'objet infecté rappelle par sa structure celui d'un programme malveillant, mais les bases de Kaspersky Endpoint Security ne recensent rien de similaire.

  Il est tout à fait possible qu'il s'agisse d'un nouveau type de virus et pour cette raison, Kaspersky Endpoint Security le classe comme un objet potentiellement infecté.

L'objet potentiellement infecté peut être découvert et placé en quarantaine par l'Antivirus Fichiers (cf. section "Antivirus Fichiers" à la page 56), et durant la recherche de virus (cf. section "Analyse" à la page 68).

De plus, vous pouvez placer un objet en quarantaine manuellement en cliquant sur le bouton **Quarantaine** dans la notification (cf. section "Comment traiter les notifications de l'application" à la page 50) spéciale qui apparaît lors de la découverte d'un objet potentiellement infecté.

En déplaçant l'objet potentiellement infecté dans la quarantaine, Kaspersky Endpoint Security le supprime du dossier actuel et l'enregistre dans le dossier de la quarantaine. Les fichiers mis en quarantaine sont convertis dans un format spécial et ne représentent aucun danger au fonctionnement de l'ordinateur.

AFFICHAGE DU CONTENU DE LA QUARANTAINE

Vous pouvez consulter le contenu de la quarantaine dans la section **Quarantaine** de la fenêtre des rapports (cf. ill. ci-après).

Pour consulter le contenu de la quarantaine, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (à la page 33) et cliquez sur le bouton  . La fenêtre des rapports de Kaspersky Endpoint Security s'ouvre.

2. Dans la partie gauche de la fenêtre des rapports, sélectionnez **Quarantaine**. La partie droite de la fenêtre affichera le contenu de la quarantaine.

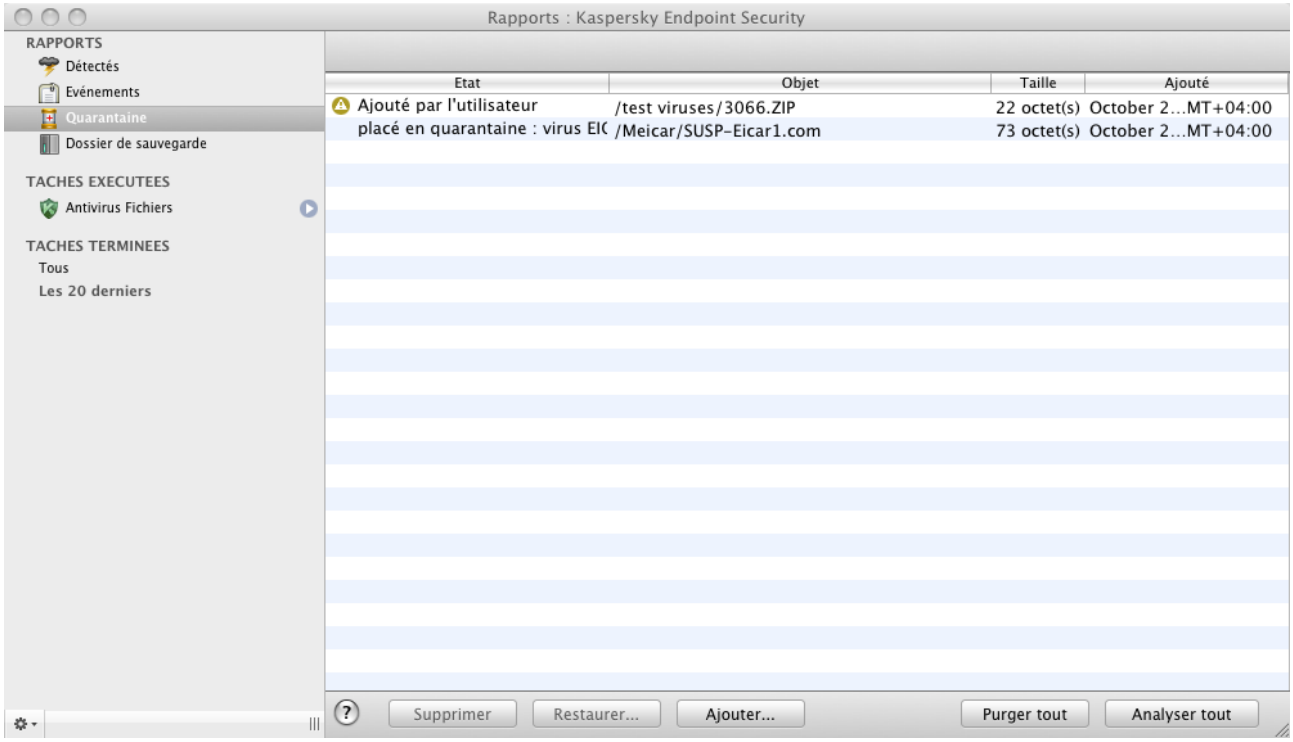


Illustration 50. Fenêtre des rapports. Dossier de quarantaine

MANIPULATION DES OBJETS EN QUARANTAINE

Kaspersky Endpoint Security permet d'exécuter les actions suivantes sur les objets potentiellement infectés :

- Déplacer manuellement dans la quarantaine les fichiers soupçonnés d'avoir des virus, mais pas détectés par Kaspersky Endpoint Security.

  Pour ce faire, dans la fenêtre de consultation de la quarantaine (cf. ill. ci-dessous), cliquez sur le bouton **Ajouter** et dans la fenêtre standard ouverte, sélectionnez le fichier nécessaire. Il sera ajouté à la liste sous le signe *ajouté par l'utilisateur*.

- Analyser et réparer à l'aide de la version actuelle des bases de Kaspersky Endpoint Security tous les objets potentiellement infectés qui se trouvent en quarantaine.

  Pour ce faire, dans la fenêtre de consultation de la quarantaine (cf. ill. ci-dessous), cliquez sur le bouton **Analyser tout**. L'état de chaque objet en quarantaine après l'analyse et la réparation peut être soit *faux positif* ou *placé en quarantaine*.

  Kaspersky Endpoint Security analyse automatiquement par défaut les objets de la quarantaine après chaque mise à jour (cf. section "Analyse des objets en quarantaine après la mise à jour de l'application" à la page 96).

- Restaurer les fichiers dans le dossier indiqué par l'utilisateur, ou le dossier duquel les fichiers ont été déplacés dans la quarantaine (par défaut).

  Pour restaurer un objet, sélectionnez-le dans la fenêtre de consultation de la quarantaine (cf. ill. ci-dessous) et cliquez sur le bouton **Restaurer**. Confirmez l'action dans la fenêtre ouverte. Pour restaurer des objets placés en quarantaine qui sont issus d'archives provenant des bases de données électroniques ou de courriers individuels, il est indispensable de désigner le dossier dans lequel ils seront restaurés.

Nous vous conseillons de restaurer uniquement les objets dont l'état correspond à *faux positif*. La restauration d'autres types d'objets pourrait entraîner l'infection de votre ordinateur.

- Supprimer tout objet de la quarantaine.

  Supprimez uniquement les objets qui ne peuvent pas être réparés. Pour supprimer un objet, sélectionnez-le dans la fenêtre de consultation de la quarantaine (cf. ill. ci-dessous) et cliquez sur le bouton **Supprimer**. Pour vider complètement la quarantaine, cliquez sur le bouton **Purger tout**. Vous pouvez aussi configurer une suppression automatiques de plus anciens objets de la quarantaine (cf. section "Configuration de la quarantaine et du dossier de sauvegarde" à la page 101).

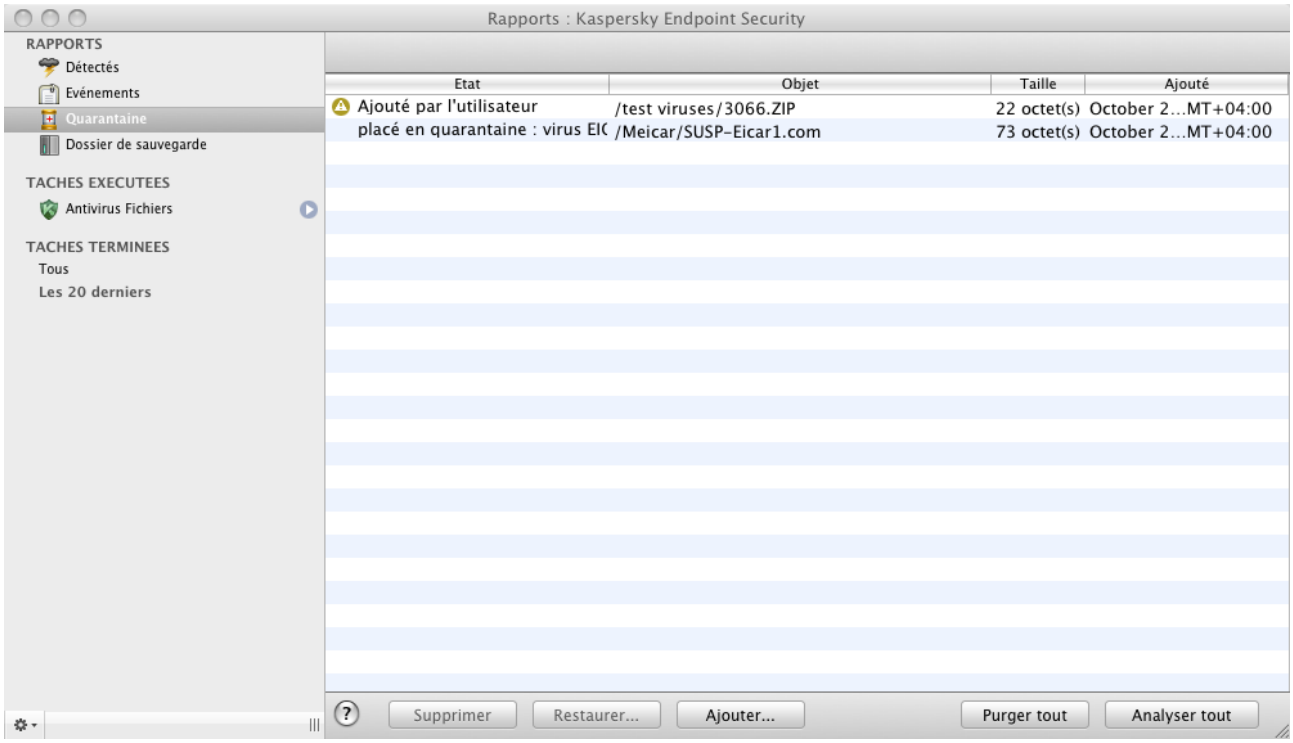


Illustration 51. Fenêtre des rapports. Dossier de quarantaine

ANALYSE DES OBJETS EN QUARANTAINE APRES LA MISE A JOUR DE L'APPLICATION

Chaque paquet de mise à jour des bases antivirus de l'application contient les nouvelles enregistrements permettant de protéger votre ordinateur contre les menaces récentes. Les experts de Kaspersky Lab vous recommandent d'analyser les objets potentiellement infectés placés en quarantaine (cf. section "Quarantaine" à la page 94) directement après la mise à jour de l'application.

La quarantaine contient des objets dont il n'a pas pu être possible de définir exactement l'origine de leur infection lors de l'analyse par l'Antivirus Fichiers ou lors de l'exécution de la tâche de recherche de virus. Il se peut que la version actualisée des bases de Kaspersky Endpoint Security puisse reconnaître et neutraliser le danger.

Kaspersky Endpoint Security analyse par défaut les objets de la quarantaine après chaque mise à jour.

Kaspersky Endpoint Security ne peut pas analyser les objets en quarantaine directement après la mise à jour des signatures des menaces si vous utilisez la quarantaine à ce moment-là.

Vous pouvez désactiver l'analyse de la quarantaine après chaque mise à jour en décochant la case requise sous l'onglet **Mise à jour** de la fenêtre de configuration de l'application.

DOSSIER DE SAUVEGARDE

Il n'est pas toujours possible de préserver l'intégrité des objets infectés lors de la réparation. Si le fichier réparé contenait des informations importantes et que celles-ci ne sont plus accessibles (complètement ou partiellement) suite à la réparation, il est possible de le restaurer à partir de sa copie de sauvegarde.

La copie de sauvegarde est une copie de l'objet dangereux original qui est créée lors de la première réparation ou suppression de l'objet en question et qui est conservée dans le dossier de sauvegarde.

Le dossier de sauvegarde est un dossier spécial qui contient les copies des objets dangereux traités ou supprimés. La fonction principale du dossier de sauvegarde est de permettre à n'importe quel moment la restauration de l'objet original. Les fichiers placés dans le dossier de sauvegarde sont convertis dans un format spécial et ne représentent aucun danger à l'ordinateur.

AFFICHAGE DU CONTENU DE LA SAUVEGARDE

Vous pouvez consulter le contenu de la sauvegarde dans la section **Dossier de sauvegarde** de la fenêtre des rapports (cf. ill. ci-après).

➧ *Pour consulter le contenu de la sauvegarde, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application (à la page 33) et cliquez sur le bouton  . La fenêtre des rapports de Kaspersky Endpoint Security s'ouvre.

2. Dans la partie gauche de la fenêtre des rapports, sélectionnez **Dossier de sauvegarde**. La partie droite de la fenêtre affichera le contenu de la quarantaine.

   Les informations suivantes sont fournies pour chaque copie de sauvegarde : nom complet de l'objet avec chemin d'accès à son emplacement d'origine, l'heure du placement dans le stockage, l'état de l'objet attribué suite à l'analyse et sa taille.

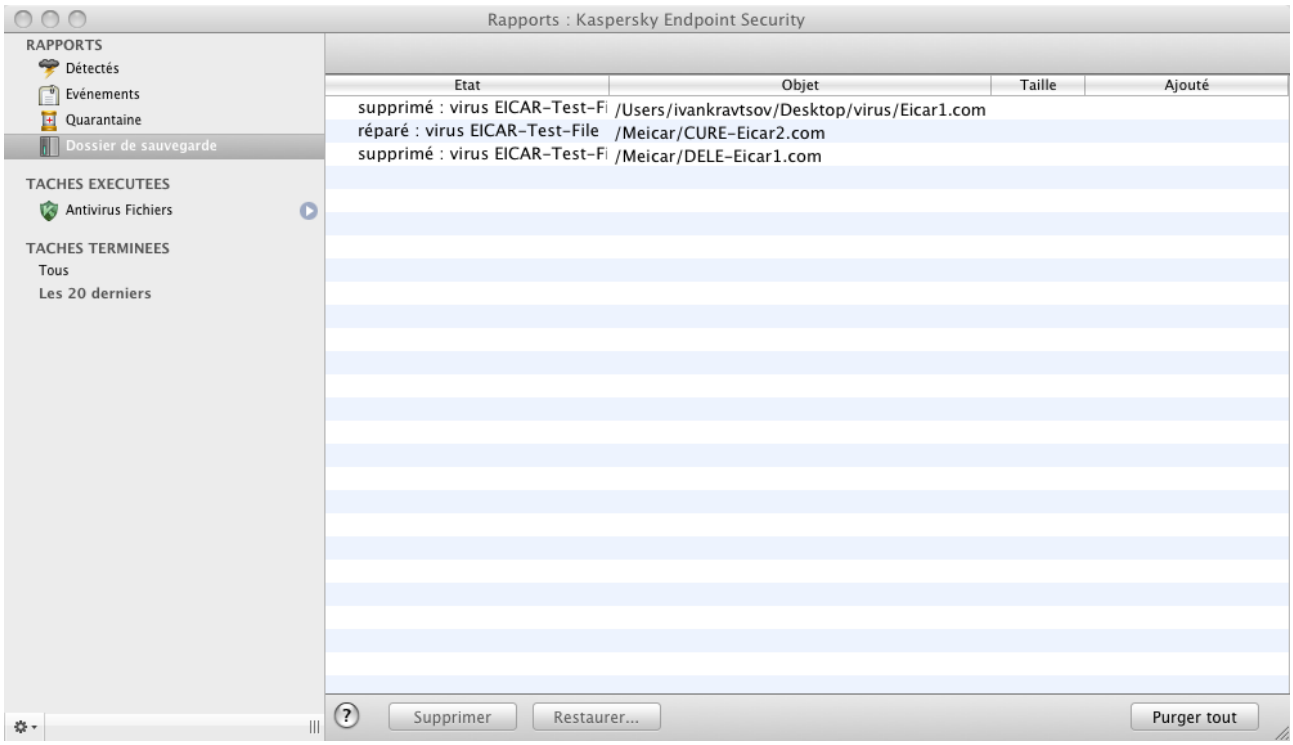


Illustration 52. Fenêtre des rapports. Dossier de sauvegarde

MANIPULATION DES COPIES DE SAUVEGARDE

Kaspersky Endpoint Security permet de réaliser les actions suivante sur les copies de sauvegarde des objets :

- Restaurer les copies de sauvegarde sélectionnées depuis le dossier de sauvegarde.

  Pour ce faire, dans la fenêtre de consultation du dossier de sauvegarde (cf. ill. ci-dessous), sélectionnez la copie de sauvegarde de l'objet nécessaire dans la liste et cliquez sur le bouton **Restaurer**. Confirmez l'action dans la fenêtre ouverte. L'objet sera restauré dans l'emplacement d'origine avec le même nom qu'avant la réparation. Si l'emplacement d'origine contient un objet portant le même nom (cette situation est possible en cas de restauration d'un objet dont la copie avait déjà été créée avant la réparation), un avertissement apparaîtra à l'écran. Vous pouvez modifier l'emplacement de l'objet restauré ainsi que son nom.

  Nous recommandons d'analyser les objets tout de suite après la restauration. Il sera possible de le réparer avec les bases antivirus les plus récentes tout en préservant son intégrité.

  Il n'est pas recommandé, sans urgence, de restaurer les copies de sauvegarde des objets. Cela pourrait en effet entraîner l'infection de votre ordinateur.

- Supprimer les copie de sauvegarde d'objets depuis la sauvegarde.

  Nous vous recommandons de consulter régulièrement la sauvegarde et la purger. Pour supprimer des objets, sélectionnez les dans la fenêtre de consultation du dossier de sauvegarde (cf. ill. ci-dessous) et cliquez sur le bouton **Supprimer**. Pour vider complètement la sauvegarde, cliquez sur le bouton **Tout supprimer**. Vous pouvez aussi configurer une suppression automatiques de plus anciennes copies de sauvegarde de la sauvegarde (cf. section "Configuration de la quarantaine et du dossier de sauvegarde" à la page 101).

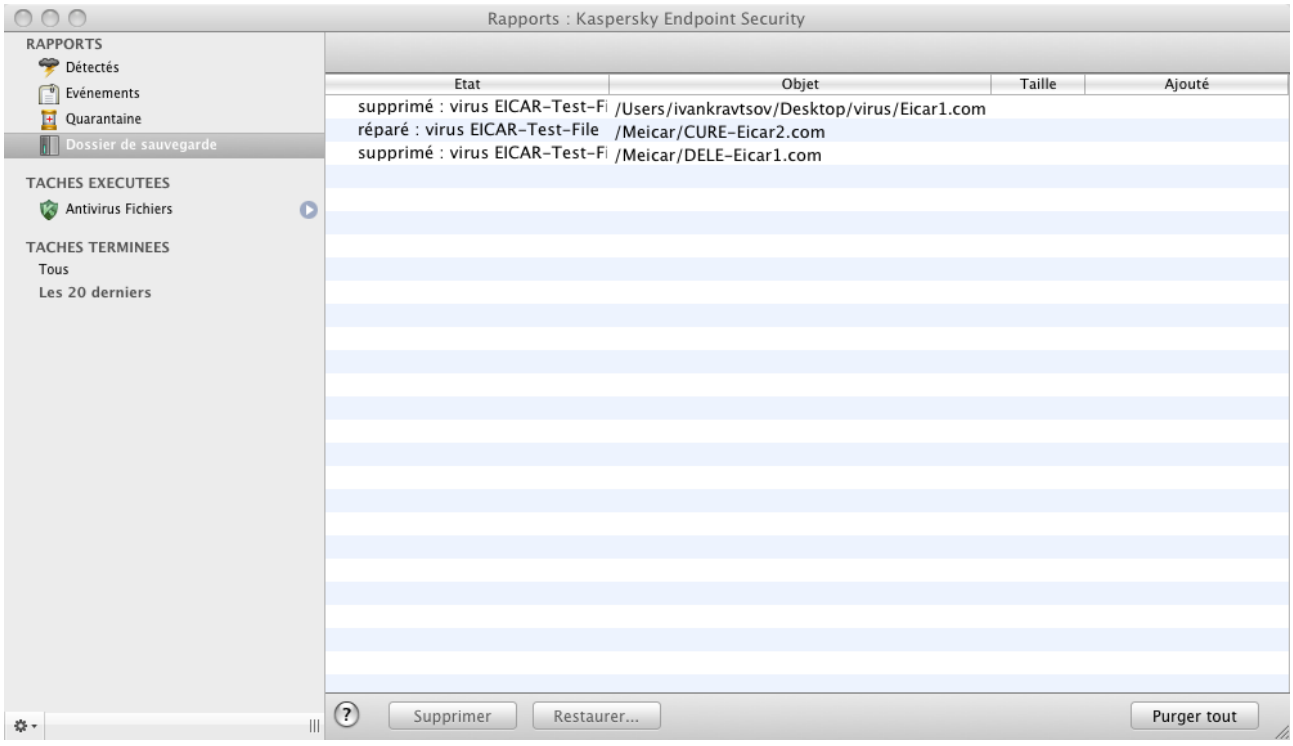


Illustration 53. Fenêtre des rapports. Dossier de sauvegarde

RAPPORTS

Kaspersky Endpoint Security offre la possibilité d'obtenir les rapports sur les résultats de son fonctionnement avec tous les événements survenus lors du fonctionnement de l'application. Un rapport détaillé est également généré pour chaque composant de l'application : l'Antivirus Fichiers (cf. section "Statistiques de la protection des fichiers" à la page 66), les tâches de recherche de virus (cf. section "Statistiques de la recherche de virus" à la page 82) et les mises à jour (cf. section "Statistiques de la mise à jour" à la page 92).

Pour ouvrir la fenêtre des rapports,

ouvrez la fenêtre principale de l'application (à la page 33) et cliquez sur le bouton  .

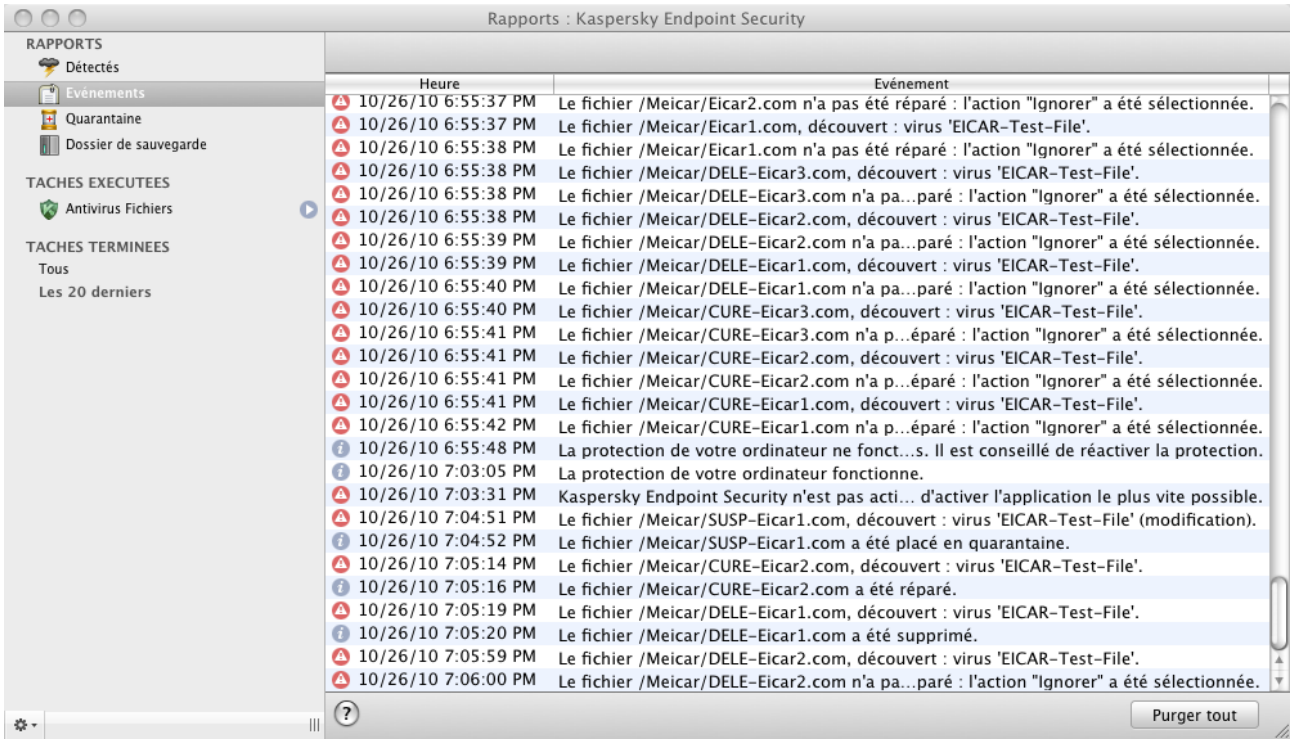


Illustration 54. Fenêtre des rapports de Kaspersky Endpoint Security

La fenêtre des rapports contient les rubriques suivantes :

- **Rapports**. Les statistiques sur les objets dangereux découverts, les objets placés en quarantaine et dans le dossier de sauvegarde et la liste des événements fixés dans le fonctionnement de l'application. Toutes les statistiques sont réparties dans les sous-sections :
  - **Détectés**. Liste de l'ensemble des objets dangereux et suspects découverts par l'Antivirus Fichiers et la recherche de virus. Pour neutraliser immédiatement les objets dangereux, appuyez sur le bouton **Réparer tous**. Pour supprimer les enregistrements relatifs aux objets, cliquez sur **Purger**. N'oubliez pas que dans ce cas, tous les objets dangereux identifiés restent sur votre ordinateur.
  - **Evénements**. Liste de tous les événements enregistrés pendant le fonctionnement de Kaspersky Endpoint Security. Pour supprimer les informations de la liste, cliquez sur le bouton **Purger tout**.
  - **Quarantaine**. Liste des objets placés en quarantaine (cf. section "Quarantaine" à la page 94).
  - **Dossier de sauvegarde**. Liste des objets placés dans le dossier de sauvegarde (à la page 97).
- **Tâches exécutées**. Liste des tâches en cours d'exécution. Si aucune tâche n'a été lancée et que l'Antivirus Fichiers est désactivé, la liste sera vide.

- **Tâches terminées**. Liste des tâches terminées. Vous pouvez consulter toutes les tâches terminées ou les vingt dernières. Pour purger la liste, cliquez sur le bouton  dans le coin inférieur gauche des rapports et sélectionnez **Supprimer toutes les tâches terminées**.

La fenêtre des rapports vous permet de gérer le fonctionnement de l'Antivirus Fichiers, des tâches d'analyse et de mise à jour, mais vous permet aussi de les lancer et de les arrêter. Pour ce faire, utilisez les boutons du même nom dans la fenêtre des rapports d'un composant ou d'une tâche.

Kaspersky Endpoint Security peut enregistrer le rapport sur son fonctionnement dans un fichier texte. Cela est par exemple utile dans le cas où une erreur est survenue dans le fonctionnement de l'Antivirus Fichiers ou lors de l'exécution de la tâche, et qu'il est impossible de l'éliminer indépendamment et que l'aide du Service d'assistance technique de Kaspersky Lab" (cf. section "Contacter le Service d'assistance technique" à la page 157) est requise. Dans ce cas, il faut envoyer le rapport au format texte au Service d'assistance technique, pour que nos spécialistes puissent étudier le problème en détail et de le résoudre le plus vite possible.

Pour exporter le rapport sur le fonctionnement de Kaspersky Endpoint Security dans un fichier texte, procédez comme suit :

1. Dans la fenêtre des rapports, sélectionnez le rapport nécessaire ou la tâche.

2. Dans le coin inférieur gauche de la fenêtre des rapports, cliquez sur le bouton  , sélectionnez la commande **Exporter** et dans la fenêtre ouverte, indiquez le nom du fichier et le dossier à placer ce fichier.

CONFIGURATION DES RAPPORTS ET DES BANQUES

Sous l'onglet **Rapports** de la fenêtre de configuration de l'application (cf. section "Fenêtre de configuration de l'application" à la page 35), vous pouvez configurer les paramètres de composition et de conservation des rapports ainsi que la durée maximale de conservation des objets dans la quarantaine ou le dossier de sauvegarde.

CONFIGURATION DES PARAMETRES DES RAPPORTS

Afin de configurer les paramètres de constitution et de conservation des rapports, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (à la page 35) et sélectionnez l'onglet **Rapports** (cf. ill. ci-après).

2. Configurez les paramètres suivants dans le groupe **Rapports** :

   - Consigner les événements à caractère informatif.

     En règle générale, ces événements ne jouent pas un rôle crucial dans la protection. Pour fixer de tels événements dans le rapport, cochez la case **Consigner les événements non critiques**.

   - Enregistrer dans le rapport uniquement les événements importants survenus lors du dernier lancement de la tâche.

     Cela permet de gagner de l'espace sur le disque en diminuant la taille du rapport. Si la case **Conserver uniquement les événements courants** est cochée, l'information présentée dans le rapport sera actualisée lors de chaque redémarrage de la tâche : par ailleurs, l'information importante (par ex. : les enregistrements relatifs aux objets malveillants découverts) sera sauvegardée, et l'information à caractère non critique sera supprimée.

   - Définir le délai de conservation des rapports.

Par défaut, la durée de conservation des rapports est de 30 jours. Les objets sont supprimés à l'issue de cette période. Vous pouvez modifier la durée de conservation des rapports ou ne pas imposer de limite.

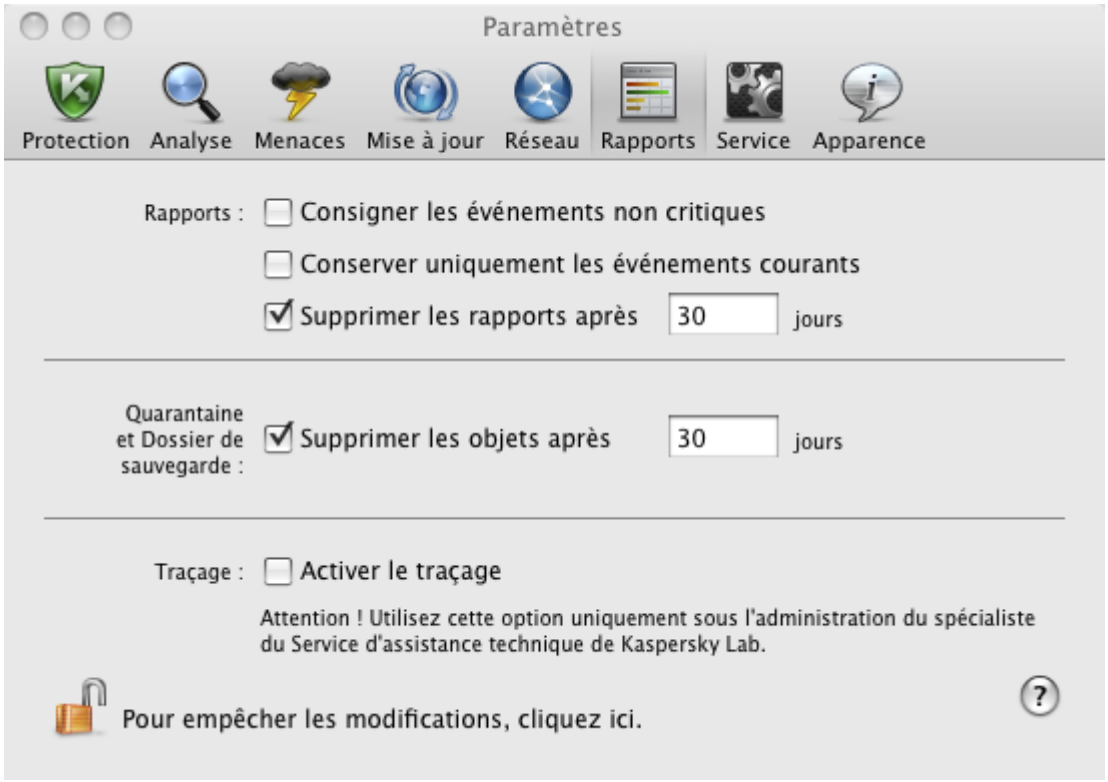


Illustration 55. Fenêtre de configuration de l'application. Rapports

CONFIGURATION DE LA QUARANTAINE ET DU DOSSIER DE SAUVEGARDE

Par défaut, la durée de conservation des objets dans la quarantaine et dans le dossier de sauvegarde est de 30 jours ; au terme desquels les objets sont supprimés. Vous pouvez modifier la durée de conservation des objets ou ne pas imposer de limite.

- *Pour configurer les paramètres du dossier de sauvegarde des objets dans le dossier de sauvegarde, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application (à la page 35) et sélectionnez l'onglet **Rapports** (cf. ill. ci-après).

2. Dans le groupe **Quarantaine et Dossier de sauvegarde**, cochez la case **Supprimer les objets après** et définissez le délai de conservation au terme duquel les objets seront automatiquement supprimés.

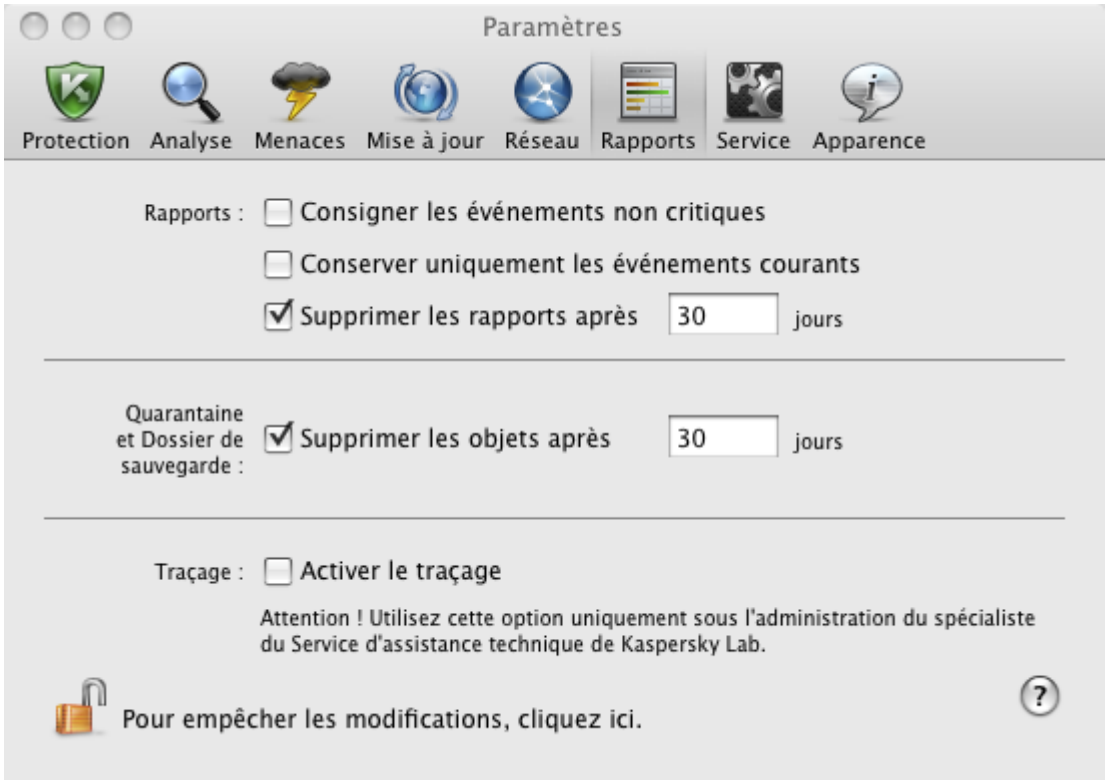


Illustration 56. Fenêtre de configuration de l'application. Rapports

UTILISATION DE L'APPLICATION AU DEPART DE LA LIGNE DE COMMANDE

Vous pouvez utiliser Kaspersky Endpoint Security à l'aide de la ligne de commande.

La syntaxe de la ligne de commande est la suivante :

```
kav <instruction> [paramètres]
```

En tant que <commande> vous pouvez utiliser :

- **help :** aide sur la syntaxe de la commande ou la liste des commandes ;
- **scan :** analyse des objets sur la présence de virus ;
- **update :** lance la mise à jour de l'application ;
- **rollback :** retour à l'état antérieur à la dernière mise à jour de Kaspersky Endpoint Security (l'exécution de cette instruction requiert les privilèges d'administrateur) ;
- **srart :** lancement du composant ou de la tâche ;
- **stop :** arrêt du composant ou de la tâche (l'exécution de cette instruction requiert les privilèges d'administrateur) ;
- **status :** affichage de l'état actuel du composant ou de la tâche ;
- **statistics :** affichage des statistiques du composant ou de la tâche ;
- **export :** exportation des paramètres de fonctionnement du composant ou de la tâche ;
- **import :** importation des paramètres de fonctionnement du composant ou de la tâche (l'exécution de cette instruction requiert les privilèges d'administrateur) ;
- **addkey :** activation de l'application à l'aide du fichier clé (l'exécution de cette instruction requiert les privilèges d'administrateur) ;
- **exit :** quitte l'application (l'exécution de cette instruction requiert les privilèges d'administrateur).

Chaque commande possède sa propre sélection de paramètres.

DANS CETTE SECTION

CONSULTATION DE L'AIDE

Pour consulter l'aide au départ de la ligne de commande, utilisez la syntaxe suivante :

```
kav [ -? | help ]
```

Pour obtenir de l'aide sur la syntaxe d'une commande particulière, vous pouvez utiliser une des commandes suivantes :

```
kav <instruction> -?
kav help <instruction>
```

RECHERCHE DE VIRUS

La ligne de commande pour le lancement de l'analyse antivirus d'un secteur quelconque ressemble à ceci :

```
kav scan [<objet à analyser>] [<action>] [<types de fichiers>] [<exclusions>]
[<paramètres du rapport>] [< paramètres complémentaires >]
```

Pour analyser les objets, vous pouvez également utiliser les tâches créées dans l'application en lançant la tâche requise via la ligne de commande (cf. section "Lancement/arrêt du fonctionnement du composant ou de la tâche" à la page 107). Dans ce cas, la tâche sera réalisée selon les paramètres définis dans l'interface de Kaspersky Endpoint Security.

Description des paramètres

<objet à analyser> : ce paramètre définit la liste des objets qui seront soumis à la recherche de code malveillant. Il peut contenir plusieurs des valeurs de la liste ci-après, séparées par un espace :

<files> : liste des chemins d'accès aux fichiers et / ou aux répertoires à analyser. La saisie d'un chemin relatif ou absolu est autorisée. Les éléments de la liste doivent être séparés par un espace. Remarques :

- si le nom de l'objet ou le chemin d'accès contient un espace ou un caractère spécial ($, &, @, etc.), il doit être repris entre guillemets ou le caractère doit être précédé d'une barre oblique inverse ;
- lorsqu'un répertoire particulier a été défini, l'analyse porte sur tous les fichiers qu'il contient.

-all : analyse complète de l'ordinateur ;

-remdrives : tous les disques amovibles ;

-fixdrives : tous les disques locaux ;

-netdrives : tous les disques de réseau ;

-quarantine : objets placés en quarantaine ;

/@:<filelist.lst> : chemin d'accès au fichier de la liste des objets et dossiers inclus dans l'analyse. Le fichier doit être au format texte et chaque nouvel objet doit être mis à la ligne. Les chemins absolus au fichier sont admis uniquement.

Si la liste des objets à analyser n'est pas indiquée, alors Kaspersky Endpoint Security lancera la tâche **Analyse** avec les paramètres installés dans l'interface de l'application.

<action> : ce paramètre définit les actions exécutées sur les objets malveillants découverts lors de l'analyse. Si le paramètre n'est pas défini, l'action exécutée par défaut sera l'action définie par la valeur **-i8**. Les valeurs suivantes sont possibles :

-i0 : aucune action n'est exécutée, seules les informations sont consignées dans le rapport ;

-i1 : réparer les objets infectés, si la réparation est impossible, les ignorer ;

-i2 : réparer les objets infectés, si la réparation est impossible, les supprimer ; ne pas supprimer les conteneurs à l'exception des conteneurs avec un en-tête exécutable (archives sfx) ;

-i3 : réparer les objets infectés, si la réparation est impossible, supprimer complètement les conteneurs s'il n'est pas possible de supprimer les fichiers infectés qu'ils contiennent ;

-i4 : supprimer les objets infectés ; supprimer complètement les conteneurs s'il n'est pas possible de supprimer les fichiers infectés qu'ils contiennent ;

-i8 : confirmer l'action auprès de l'utilisateur en cas de découverte d'un objet infecté. Cette action est utilisée par défaut ;

-i9 : confirmer l'action auprès de l'utilisateur à la fin de l'analyse.

Le paramètre **<types de fichiers>** définit les types de fichiers qui seront soumis à l'analyse antivirus. Si le paramètre n'est pas défini, seuls seront analysés par défaut les objets pouvant être infectés en fonction du contenu. Les valeurs suivantes sont possibles :

-fe : analyser uniquement les fichiers qui peuvent être infectés selon l'extension ;

-fi : analyser uniquement les fichiers qui peuvent être infectés selon le contenu ;

-fa : analyser tous les fichiers.

Le paramètre **<exclusions>** définit les objets exclus de l'analyse. Il est possible de citer plusieurs paramètres de la liste suivante, à condition de les séparer par un espace :

-e:a : ne pas analyser les archives ;

-e:b : ne pas analyser les bases de messagerie ;

-e:m : ne pas analyser les messages électroniques au format texte ;

-e:<mask> : ne pas analyser les objets en fonction du masque (cf. section "Masques autorisés pour les exclusions de fichiers" à la page 161) ;

-e:<seconds> : ignorer les objets dont l'analyse dure plus que la valeur attribuée au paramètre <seconds> ;

-es:<size> : ignorer les objets dont la taille dépasse la valeur définie en mégaoctets.

<paramètres du rapport> : le paramètre définit le format du rapport sur les résultats de l'analyse. Les chemins relatifs et absolus au fichier pour l'enregistrement du rapport sont admis. Si le paramètre n'est pas indiqué, les résultats de l'analyse sont affichés à l'écran et portent sur tous les événements.

-r:<report_file> : consigner uniquement les événements importants dans le fichier indiqué ;

-ra:<report_file> : consigner tous les événements dans le rapport.

<paramètres complémentaires> : paramètres qui définissent l'utilisation de technologies de recherche de virus et l'utilisation du fichier de configuration des paramètres :

-iSwift=<on|off> : activer / désactiver l'utilisation de la technologie iSwift ;

-c:<nom_du_fichier_de_configuration> : le paramètre définit le chemin d'accès au fichier de configuration qui contient les paramètres utilisés par l'application pour l'analyse. La saisie d'un chemin relatif ou absolu est autorisée. Si le paramètre n'est pas défini, les valeurs définies dans l'interface utilisateur de l'application sont utilisées en plus des valeurs déjà indiquées dans la ligne de commande.

Exemple :

Lancer l'analyse des dossiers ~/Documents, /Applications et du fichier my test.exe:

```
kav scan ~/Documents /Applications 'my test.exe'
```

Analyser les objets dont la liste est reprise dans le fichier object2scan.txt. Utiliser le fichier de configuration scan_settings.txt. A la fin de l'analyse, rédiger un rapport qui reprendra tous les événements :

```
Y /@:objects2scan.txt /C:scan_settings.txt /RA:scan.log
```

Exemple de fichier de configuration:

```
-netdrives -@:objects2scan.txt -ra:scan.log
```

MISE A JOUR DE L'APPLICATION

La commande de mise à jour des modules et des bases antivirus de l'application possède la syntaxe suivante :

```
kav update [<source_de_la_mise_à_jour>] [-app=<on|off>] [<paramètres_de_rapport>]
[<paramètres_complémentaires>]
```

Description des paramètres

<source_des_mises_à_jour> : serveur HTTP ou FTP ou répertoire réseau ou local pour le téléchargement des mises à jour. Si le chemin d'accès n'est pas indiqué, la source de la mise à jour sera définie par les paramètres du service de mise à jour de l'application.

-app=<on|off> – active/désactive la mise à jour des modules de l'application.

<paramètres du rapport> : le paramètre définit le format du rapport sur les résultats de l'analyse. Les chemins relatifs et absolus au fichier sont admis. Si le paramètre n'est pas indiqué, les résultats de l'analyse sont affichés à l'écran et portent sur tous les événements. Les valeurs suivantes sont possibles :

-r:<report_file> : consigner uniquement les événements importants dans le fichier indiqué ;

-ra:<report_file> : consigner tous les événements dans le rapport.

<paramètres complémentaires> : paramètre qui définit l'utilisation du fichier de configuration des paramètres.

-c:<nom_du_fichier_de_configuration> : le paramètre définit le chemin d'accès au fichier de configuration qui contient les paramètres utilisés par le programme pour l'analyse. La saisie d'un chemin relatif ou absolu est autorisée. Si ce paramètre n'est pas défini, ce sont les valeurs définies dans l'interface de l'application qui seront utilisées.

Exemple :

Actualiser les bases de l'application depuis la source par défaut et consigner tous les événements dans le rapport :

```
UPDATE -RA:avbases_upd.txt
```

Mettre à jour les modules de Kaspersky Endpoint Security en utilisant les paramètres du fichier de configuration updateapp.ini :

```
kav update -app=on -c:updateapp.ini
```

ANNULATION DE LA DERNIERE MISE A JOUR

Syntaxe de la commande :

```
kav rollback [<paramètres_du_rapport>]
```

L'exécution de cette instruction requiert les privilèges d'administrateur.

Description des paramètres

<paramètres du rapport> – le paramètre définit le format du rapport sur les résultats de l'analyse. Les chemins relatifs et absolus au fichier sont admis. Si le paramètre n'est pas indiqué, les résultats de l'analyse sont affichés à l'écran et portent sur tous les événements.

-r:<report_file> : consigner uniquement les événements importants dans le fichier indiqué ;

-ra:<report_file> : consigner tous les événements dans le rapport. Les chemins relatifs et absolus au fichier sont admis. Si le paramètre n'est pas indiqué, les résultats de l'analyse sont affichés à l'écran et portent sur tous les événements.

Exemple :

```
kav rollback -ra:rollback.txt
```

LANCEMENT / ARRET DU FONCTIONNEMENT D'UN COMPOSANT OU D'UNE TACHE

Syntaxe de la commande start :

```
kav start <profil|nom_de_la_tâche> [<paramètres_du_rapport>]
```

Syntaxe de la commande stop :

```
kav stop <profil|nom_de_la_tâche>
```

L'exécution de l'instruction stop requiert les privilèges d'administrateur.

Description des paramètres

<paramètres du rapport> : le paramètre définit le format du rapport sur les résultats de l'analyse. Les chemins relatifs et absolus au fichier sont admis. Si le paramètre n'est pas indiqué, les résultats de l'analyse sont affichés à l'écran et portent sur tous les événements. Les valeurs suivantes sont possibles :

-r:<report_file> : consigner uniquement les événements importants dans le fichier indiqué ;

-ra:<report_file> : consigner tous les événements dans le rapport. Les chemins relatifs et absolus au fichier sont admis. Si le paramètre n'est pas indiqué, les résultats de l'analyse sont affichés à l'écran et portent sur tous les événements.

<profil|nom_de_la_tâche> : attribuez une des valeurs suivantes :

file_monitoring (fm) : Antivirus Fichiers ;

scan_my_computer (full) : la tâche d'analyse complète de l'ordinateur ;

scan_objects : analyse des objets ;

scan_quarantine : analyse de la quarantaine ;

scan_critical_areas (quick) : tâche d'analyse express de l'ordinateur ;

updater : tâche de mise à jour ;

rollback : tâche d'annulation d'une mise à jour.

Il est aussi possible d'indiquer le nom de la tâche de recherche de virus créée par l'utilisateur en tant que la valeur de ce paramètre.

Les composants et les tâches lancés via la ligne de commande sont exécutés selon les paramètres définis dans l'interface du logiciel.

Exemple :

Pour activer l'Antivirus Fichiers, saisissez dans la ligne de commande :

```
kav start fm
```

Pour arrêter la tâche d'analyse complète, saisissez dans la ligne de commande :

```
kav stop scan_my_computer
```

STATISTIQUES DU FONCTIONNEMENT DU COMPOSANT OU DE LA TACHE

Syntaxe de la commande status :

```
kav status [<profil|nom_de_la_tâche>]
```

Syntaxe de la commande statistics :

```
kav statistics <profil|nom_de_la_tâche>
```

Description des paramètres

<profil|nom_de_la_tâche> : une des valeurs citées dans la commande start/stop s'indique. (cf. la section "Lancement/arrêt du composant ou de la tâche" à la page 107)

Si l'instruction status est exécutée sans définir le paramètre **<profil|nom_de_la_tâche>**, alors l'état actuel de toutes les tâches et de tous les composants de l'application sera affiché. Pour l'instruction statistics, la valeur du paramètre **<profil|nom_de_la_tâche>** doit être définie.

EXPORTATION DES PARAMETRES DE PROTECTION

Syntaxe de la commande :

```
kav export <profil|nom_de_la_tâche> <nom_du_fichier>
```

Description des paramètres

<profil|nom_de_la_tâche> désigne une des valeurs reprises pour l'instruction start / stop (cf. section "Lancement/arrêt d'un composant ou d'une tâche" à la page 107).

<nom_du_fichier> – chemin d'accès au fichier vers lequel sont exportés les paramètres de l'application. Vous pouvez indiquer un chemin relatif ou absolu.

Exemple :

```
kav export fm fm_settings.txt - format texte
```

IMPORTATION DES PARAMETRES DE PROTECTION

Syntaxe de la commande :

```
kav import <nom_du_fichier>
```

L'exécution de cette instruction requiert les privilèges d'administrateur.

Description des paramètres

<nom_du_fichier> – chemin d'accès au fichier duquel sont importés les paramètres de l'application. Vous pouvez indiquer un chemin relatif ou absolu.

Exemple :

```
kav import settings.dat
```

ACTIVATION DE L'APPLICATION

Kaspersky Endpoint Security peut être activé à l'aide d'un fichier clé.

Syntaxe de la commande :

```
kav addkey <nom_du_fichier>
```

L'exécution de cette instruction requiert les privilèges d'administrateur.

Description des paramètres

<nom_du_fichier> : fichier clé pour l'application, portant l'extension .key.

Exemple :

```
kav addkey 1AA111A1.key
```

ARRET DE L'APPLICATION

Syntaxe de la commande :

```
kav exit
```

L'exécution de cette instruction requiert les privilèges d'administrateur.

CODES DE RETOUR DE LA LIGNE DE COMMANDE

Les codes généraux peuvent être renvoyés par n'importe quelle commande. Les codes de retour des tâches concernent les codes généraux et les codes spécifiques à un type de tâche en particulier.

Codes de retour généraux :

- 0 – opération réussie ;
- 1 – valeur de paramètre invalide ;
- 2 – erreur inconnue ;
- 3 – erreur d'exécution de la tâche ;
- 4 – annulation de l'exécution de la tâche.

Codes de retour des tâches d'analyse antivirus :

- 101 – tous les objets dangereux ont été traités ;
- 102 – des objets dangereux ont été découverts.

ADMINISTRATION DU LOGICIEL VIA KASPERSKY ADMINISTRATION KIT

Kaspersky Administration Kit- est un système qui permet d'exécuter, de manière centralisée, les principales tâches d'administration de la sécurité des ordinateurs du réseau d'une entreprise. Il repose sur les applications faisant partie de la suite Kaspersky Open Space Security. Kaspersky Administration Kit prend en charge toutes les configurations réseau utilisant le protocole TCP/IP.

Kaspersky Administration Kit est un outil pour administrateurs de réseaux d'entreprise et pour responsables de sécurité antivirale.

Kaspersky Endpoint Security fait partie des produits de Kaspersky Lab qui peuvent être administrés via leur propre interface (cf. page 31), via la ligne de commande (cf. section "Utilisation du programme au départ de la ligne de commande" à la page 103) ou à l'aide de l'application Kaspersky Administration Kit.

L'administration de l'application via Kaspersky Administration Kit s'opère grâce à la Console d'administration (cf. ill. ci-après). Cette console 'se présente sous la forme d'une interface standard intégrée au MMC. Grâce à elle, l'administrateur peut exécuter les tâches suivantes :

- Installer Kaspersky Endpoint Security à distance sur les ordinateurs du réseau ;
- Configurer Kaspersky Endpoint Security à distance sur les ordinateurs du réseau ;
- Actualiser les bases antivirus et les modules de l'application et revenir à l'état antérieur à la mise à jour ;
- Lancer la recherche de la présence éventuelle de virus sur les ordinateurs du réseau ;
- Activer l'application à distance à l'aide d'un fichier clé ;
- Consulter les statistiques et composer un rapport sur le fonctionnement de Kaspersky Endpoint Security sur les ordinateurs du réseau.

Illustration 57. Ouvrez la console d'administration de Kaspersky Administration Kit

L'apparence de la fenêtre principale de Kaspersky Administration Kit dépend du système d'exploitation de l'ordinateur de l'administrateur.

Concepts et définitions

En cas d'utilisation de Kaspersky Administration Kit, l'administration de Kaspersky Endpoint Security s'opère selon les paramètres des stratégies, les paramètres des tâches et les paramètres de l'application définis par l'administrateur.

Une action portant un nom et exécutée par l'application s'appelle une *tâche*. Les types de tâche suivants sont identifiés selon les fonctions exécutées :

- recherche de virus ;
- mise à jour de l'application ;
- annulation de la dernière mise à jour ;
- installation du fichier clé.

Un groupe de paramètres de fonctionnement de l'application correspond à chaque tâche. Les paramètres communs à tous les types de tâche sont appelés les *paramètres de l'application*. Les paramètres spécifiques à chaque type de tâche s'intitulent les *paramètres de tâche*. Aucun conflit n'est possible entre les paramètres de l'application et les paramètres de tâche.

Parmi les particularités de l'administration centralisée, citons la répartition des ordinateurs distants en groupe et l'administration des paramètres via la création et la définition de stratégies de groupe.

La stratégie – est un ensemble de paramètres de fonctionnement de l'application dans le groupe ainsi qu'un ensemble de restrictions sur la redéfinition des paramètres lors de la configuration de l'application et des tâches sur un ordinateur client distant. La stratégie inclut les paramètres permettant de configurer toutes les fonctionnalités de l'application, à l'exception de paramètres spécifiques à certains modèles de tâche. Il peut notamment s'agir des paramètres de programmation.

La stratégie comprend par exemple les paramètres :

- communs à tous les types de tâche, à savoir les paramètres de l'application ;
- communs à tous les modèles de tâche d'un type donné, à savoir la majeure partie des paramètres de tâche.

En d'autres termes, la stratégie de Kaspersky Endpoint Security, dont font partie les tâches de protection et de recherche de virus, comprend tous les paramètres utilisés par l'ensemble des tâches exécutées mais n'inclut pas la programmation des tâches de recherche de virus et les paramètres définissant la zone d'analyse.

DANS CETTE SECTION

SCHEMA TYPIQUE DE DEPLOIEMENT

Afin d'administrer Kaspersky Endpoint Security via Kaspersky Administration Kit, procédez comme suit :

1. Déployez le Serveur d'administration dans le réseau ;
2. Installez la Console d'administration[2] et le plug-in d'administration Kaspersky Endpoint Security (cf. section "Installation du plug-in d'administration de Kaspersky Endpoint Security" à la page 114) sur le poste de travail de l'administrateur de Kaspersky Administration Kit.
3. Installez l'Agent d'administration et Kaspersky Endpoint Security sur les ordinateurs Mac.
   - L'installation de l'Agent d'administration peut être réalisée localement (cf. section "Installation locale de l'Agent d'administration" à la page 115) ou à distance à l'aide du protocole SSH (cf. section "Installation de l'Agent d'administration à l'aide du protocole SSH" à la page 116).
   - L'installation de Kaspersky Endpoint Security peut également être réalisée localement (cf. section "Installation de l'application" à la page 20), à distance via le protocole SSH (cf. section "Installation de l'application à l'aide du protocole SSH" à la page 119) ou à distance via Kaspersky Administration Kit et un paquet d'installation (cf. section "Installation de l'application via Kaspersky Administration Kit" à la page 120) créé au préalable.

Si une version de Kaspersky Anti-Virus for Mac est déjà installée sur l'ordinateur de l'utilisateur, alors il faudra la supprimer avant d'installer Kaspersky Endpoint Security.

[2] Pour les détails, consultez le Guide de déploiement de Kaspersky Administration Kit.

INSTALLATION DE L'APPLICATION INDISPENSABLE A L'ADMINISTRATION A DISTANCE DE KASPERSKY ENDPOINT SECURITY

Pour réaliser l'administration à distance de Kaspersky Endpoint Security via Kaspersky Administration Kit, il faut installer les applications suivantes :

- Plug-in d'administration de Kaspersky Endpoint Security sur le poste de travail de l'administrateur de Kaspersky Administration Kit où la console d'administration est déjà installée.
- Agent d'administration – sur les ordinateurs Mac du réseau de l'entreprise.

DANS CETTE SECTION

INSTALLATION DU PLUG-IN D'ADMINISTRATION DE KASPERSKY ENDPOINT SECURITY

Avant d'installer le plug-in d'administration de Kaspersky Endpoint Security, il faut quitter la console d'administration sur le poste de travail de l'administrateur de Kaspersky Administration Kit.

Pour installer le plug-in d'administration de Kaspersky Endpoint Security sur le poste de travail de l'administrateur, procédez comme suit :

1. Ouvrez le contenu du fichier d'installation de Kaspersky Endpoint Security. Pour ce faire, introduisez le disque d'installation dans le lecteur. Dans la fenêtre contenant la distribution, ouvrez le dossier **AdminKit Deployment.**

   Si vous avez acheté Kaspersky Endpoint Security dans un magasin en ligne, alors le fichier d'installation de l'application au format ZIP peut être téléchargé du site de Kaspersky Lab. Décompressez le fichier et ouvrez le fichier .dmg afin de voir le contenu du paquet d'installation.

2. Ouvrez le dossier **AdminKit Console Plugin**, puis le sous-dossier contenant la version de l'application dans la langue souhaitée.

3. Lancer le fichier exécutable klcfginst.exe. Patientez pendant l'exécution de l'installation.

À l'issue de l'installation, le plug-in d'administration de Kaspersky Endpoint Security sera ajouté à la liste des plug-ins installés pour l'administration des applications[3].

[3] Lisez attentivement l'aide de Kaspersky Administration Kit.

INSTALLATION LOCALE DE L'AGENT D'ADMINISTRATION

Pour exécuter l'installation locale de l'Agent d'administration sur l'ordinateur de l'utilisateur, procédez comme suit :

1. Ouvrez le contenu de la distribution de l'Agent d'administration. Pour ce faire, introduisez le disque d'installation dans le lecteur.

   Si vous avez acheté Kaspersky Endpoint Security dans un magasin en ligne, alors le fichier d'installation de l'application au format ZIP peut être téléchargé du site de Kaspersky Lab. Décompressez le fichier et ouvrez le fichier .dmg afin de voir le contenu du paquet d'installation.

2. Lancez le programme d'installation de l'Agent d'administration. Pour ce faire, ouvrez le paquet d'installation **Kaspersky Network Agent** dans la fenêtre du contenu du paquet d'installation.

   Confirmez le lancement de l'installation de l'application dans la fenêtre qui s'ouvre. Ensuite, installez l'application en suivant les instructions du programme d'installation.

3. Dans la fenêtre **Introduction**, cliquez sur le bouton **Continuer**.

4. Dans la fenêtre **Lisez-moi**, lisez les informations sur l'application à installer.

   Assurez-vous que l'ordinateur de l'utilisateur correspond aux exigences de système indiquées. Pour imprimer ces informations, cliquez sur le bouton **Imprimer**. Pour sauvegarder les informations dans un fichier texte, cliquez sur le bouton **Enregistrer**. Pour poursuivre l'installation, cliquez sur **Continuer**.

5. Dans la fenêtre **Licence**, lisez le texte du contrat de licence sur l'utilisation de l'Agent d'administration, qui a été conclu entre vous et Kaspersky Lab. Le texte du contrat est disponible en plusieurs langues. Pour imprimer le texte du contrat, cliquez sur le bouton **Imprimer**. Pour sauvegarder le contrat dans un fichier texte, cliquez sur le bouton **Enregistrer**.

   Si vous acceptez toutes les conditions du contrat, cliquez sur le bouton **Continuer**. La fenêtre de confirmation de l'acceptation des termes du contrat de licence s'ouvrira. Vous pouvez exécuter les opérations suivantes :

   - Poursuivre l'installation de l'Agent d'administration en cliquant sur le bouton **Accepter** ;
   - Revenir au texte du contrat en cliquant sur le bouton **Lire la licence** ;
   - Interrompre l'installation de l'application en cliquant sur le bouton **Refuser**.

6. Dans la fenêtre **Paramètres**, saisissez dans le champ **Serveur** l'adresse IP ou le nom DNS du serveur sur lequel Kaspersky Administration Kit est installé et dans le champ **Port**, le numéro du port pour la connexion non sécurisée avec le serveur et dans le champ **Port SSL**, le numéro du port pour la connexion avec le serveur avec l'utilisation de SSL.

   Si vous ne souhaitez pas utiliser le SSL pour la connexion au serveur, décochez la case **Utiliser SSL**. Pour poursuivre l'installation, cliquez sur **Continuer**.

7. Dans la fenêtre **Type d'installation**, regardez les informations relatives au disque sur lequel l'application va être installée.

   Pour installer l'application en utilisant les paramètres d'installation standards proposés, cliquez sur le bouton **Installer** et saisissez le mot de passe de l'administrateur pour confirmer.

   Pour sélectionner un autre disque pour installer l'application, cliquez sur le bouton **Modifier l'emplacement de l'installation** et sélectionnez un autre disque, puis cliquez sur le bouton **Continuer**.

   Le disque d'amorçage est requis pour l'installation de l'application. Le système d'exploitation de la version non pas inférieure à celle indiquée dans les exigences de système (cf. section "Configuration matérielle et logicielle requises" à la page 18) doit être installé sur le disque.

Attendez la fin de l'installation des composants par le programme d'installation de l'Agent d'administration.

8. Dans la fenêtre **Résumé**, lisez les informations sur la fin du processus d'installation et cliquez sur le bouton **Fermer** pour quitter le programme d'installation.

INSTALLATION DE L'AGENT D'ADMINISTRATION A L'AIDE DU PROTOCOLE SSH

Avant d'installer l'Agent d'administration sur l'ordinateur distant à l'aide du protocole SSH, assurez-vous que les conditions suivantes sont remplies :

- Le serveur d'administration Kaspersky Administration Kit est déployé sur le réseau de l'entreprise[4].
- La console d'administration est installée sur le poste de travail de l'administrateur de Kaspersky Administration Kit.
- Le paquet d'installation de l'Agent d'administration a été créé et se trouve dans le dossier partagé du Serveur d'administration[5].

Pour procéder à l'installation de l'Agent d'administration sur un ordinateur distant via le protocole SSH, procédez comme suit :

1. Activez le service **Session à distance** sur l'ordinateur Mac.
2. Sur le poste de travail de l'administrateur, lancez le client SSH et connectez-vous à l'ordinateur Mac distant.
3. Connectez le dossier partagé du Serveur d'administration en tant que disque réseau sur l'ordinateur distant. Pour ce faire, saisissez les instructions suivantes dans le terminal du client SSH :

   ```
   mkdir /Volumes/KLSHARE
   ```

   ```
   mount_smbfs //<admin_login>:<password>@<AK_server_address>/KLSHARE
   /Volumes/KLSHARE
   ```

   Description des paramètres:

   - **<admin_login>** : identifiant de l'administrateur du Serveur d'administration ;
   - **<password>** : mot de passe de l'administrateur du Serveur d'administration ;
   - **<AK_server_address>** : adresse IP du serveur sur lequel Kaspersky Administration Kit est installé.

4. Lancez le script d'installation. Pour ce faire, saisissez les instructions suivantes dans le terminal du client SSH :

   ```
   cd /Volumes/KLSHARE/Packages/<klnagent_package_folder>
   ```

   ou <**klnagent_package_folder>** désigne le dossier qui contient le paquet d'installation de l'Agent d'administration.

   ```
   sudo ./install.sh -r <serveur> [-s <action>] [-p <numéro du port>] [-l <numéro du
   port SSL>]
   ```

   Description des paramètres:

   - **<action>** : paramètre définissant si le cryptage sera utilisé ou non lors de la connexion de l'Agent d'administration avec le Serveur d'administration. Si la valeur est 0, alors la connexion non sécurisée sera utilisée. Si la valeur est 1, la connexion sera réalisée selon le protocole SSL (valeur par défaut) ;
   - **<serveur>** : adresse IP ou nom DNS du serveur sur lequel Kaspersky Administration Kit est installé ;

[4] Pour les détails, consultez le Guide de déploiement de Kaspersky Administration Kit.
[5] Lisez attentivement l'aide de Kaspersky Administration Kit.

- **<numéro du port>** : numéro de port à utiliser pour une connexion non sécurisée au Serveur d'administration. Par défaut le port 14000 est utilisé.

- **-ps <numéro du port SSL>** : numéro de port SSL à utiliser pour une connexion sécurisée au Serveur d'administration sous protocole SSL. Par défaut, il s'agit du port 13000.

L'exécution de cette instruction requiert les privilèges d'administrateur.

5. Déconnectez le disque réseau de l'ordinateur distant. Pour ce faire, saisissez l'instruction suivante dans le terminal du client SSH :

   ```
   umount /Volumes/KLSHARE
   ```

6. Vérifiez le fonctionnement de l'Agent d'administration sur l'ordinateur distant. Pour ce faire, saisissez les instructions suivantes dans le terminal du client SSH :

   ```
   cd /Library/Application\ Support/Kaspersky\ Lab/klnagent/Binaries/
   sudo ./klnagchk
   ```

   Si la vérification réussit, alors l'Agent d'administration fonctionne normalement.

ACTUALISATION DE L'AGENT D'ADMINISTRATION VIA KASPERSKY ADMINISTRATION KIT

Avant le lancement de la mise à jour de l'Agent d'administration installé sur l'ordinateur distant, assurez-vous que les conditions suivantes sont remplies :

- Le serveur d'administration Kaspersky Administration Kit est déployé sur le réseau de l'entreprise[6].

- La console d'administration est installée sur le poste de travail de l'administrateur de Kaspersky Administration Kit.

- L'Agent d'administration est installé sur l'ordinateur Mac.

- Le paquet d'installation pour la mise à jour de l'Agent d'administration a été créé et se trouve dans le dossier partagé du Serveur d'administration[7].

  Dans la fenêtre des propriétés du paquet d'installation, sous l'onglet **Connexion**, dans le champ **Adresse du serveur**, il faut indiquer l'adresse IP ou le nom DNS du Serveur d'administration, dans le champ **Numéro de port** - le numéro de port pour une connexion non sécurisée avec le serveur et dans le champ **Numéro du port SSL** - le numéro du port pour la connexion avec le serveur avec l'utilisation de SSL. Si vous ne souhaitez pas utiliser le SSL pour la connexion au serveur, décochez la case **Utiliser la connexion SSL**.

- L'ordinateur Mac est ajouté au groupe **Ordinateurs administrés** du Serveur d'administration (à la demande)[8].

La mise à jour de l'Agent d'administration installé sur l'ordinateur distant (via Kaspersky Administration Kit) est effectuée à l'aide de la création et du lancement ultérieur de la tâche d'installation à distance de l'application.

Pour créer une tâche d'installation à distance de l'application sur un ordinateur distant via Kaspersky Administration Kit, procédez comme suit :

1. Lancez la Console d'administration de Kaspersky Administration Kit.

2. Déployez le nœud **Serveur d'administration** et sélectionnez le dossier **Tâches pour les sélections d'ordinateurs**.

[6] Pour les détails, consultez le Guide de déploiement de Kaspersky Administration Kit.
[7] Lisez attentivement l'aide de Kaspersky Administration Kit.
[8] Lisez attentivement le Guide de l'administrateur de Kaspersky Administration Kit.

3. Lancez l'Assistant de création de tâche en cliquant sur le lien **Créer une tâche** dans le volet des tâches. Suivez les étapes de l'Assistant pour créer la tâche d'installation à distance.

4. Dans le champ **Nom** de la fenêtre **Nom de la tâche** saisissez le nom de la tâche, puis cliquez sur le bouton **Suivant**.

5. Dans la fenêtre **Type de tâche**, sélectionnez la tâche **Installation à distance de l'application** dans la liste pour l'application Kaspersky Administration Kit, puis cliquez sur **Suivant**.

6. Dans la liste de la fenêtre **Paquet d'installation**, sélectionnez le paquet d'installation pour l'Agent d'administration, puis cliquez sur **Suivant**.

7. Dans la fenêtre **Méthode d'installation**, choisissez l'option **Installation forcée** en guise de méthode d'installation à distance, puis cliquez sur **Suivant**.

8. Dans la fenêtre **Paramètres** cliquez sur **Suivant**.

9. Dans la fenêtre **Redémarrage**, choisissez l'option **Ne pas redémarrer l'ordinateur**, puis cliquez sur le bouton **Suivant**.

   Le redémarrage de l'ordinateur après la mise à jour de l'Agent d'administration n'est pas requis.

10. Dans la fenêtre **Déplacement des ordinateurs**, sélectionnez le groupe à déplacer l'ordinateur d'utilisateur par Kaspersky Administration Kit après la mise à jour de l'Agent d'administration. Si le déplacement de l'ordinateur dans un autre groupe n'est pas requis, sélectionnez l'option **Ne pas déplacer les ordinateurs**. Cliquez sur **Suivant**.

11. Sélectionnez, dans la fenêtre **Mode de sélection des postes clients**, l'option de sélection des ordinateurs pour l'installation de l'application qui vous convient le mieux. Vous pouvez installer l'application :

    - sur la base des données obtenues lors du sondage du réseau Windows ;
    - sur la base des adresses d'ordinateurs saisies manuellement.

    Cliquez sur **Suivant**.

12. Dans la fenêtre **Postes clients**, désignez les ordinateurs pour lesquels la tâche d'installation à distance sera créée, conformément à l'option choisie à l'étape antérieure. Cliquez sur **Suivant**.

13. Dans la fenêtre **Compte**, cliquez sur le bouton **Suivant**.

14. Dans la fenêtre **Planification de l'exécution de la tâche**, sélectionnez le mode de lancement de la tâche : manuel ou selon un horaire défini. Pour ce faire, sélectionnez dans la liste déroulante la fréquence de lancement de la tâche et indiquez l'heure de lancement de la tâche. Cliquez sur **Suivant**.

15. La dernière fenêtre de l'Assistant vous informe de la réussite de la création de la tâche. Cliquez sur le bouton **Terminer** pour quitter l'Assistant.

La tâche créée apparaît dans l'arborescence de la console dans le dossier **Tâches pour les sélections d'ordinateurs**.

SUPPRESSION DE L'AGENT D'ADMINISTRATION

Pour supprimer l'Agent d'administration de l'ordinateur, procédez comme suit :

1. Ouvrez le contenu de la distribution de l'Agent d'administration. Pour ce faire, introduisez le disque d'installation dans le lecteur.

   Si vous avez acheté Kaspersky Endpoint Security dans un magasin en ligne, alors le fichier d'installation de l'application au format ZIP peut être téléchargé du site de Kaspersky Lab. Décompressez le fichier et ouvrez le fichier .dmg afin de voir le contenu du paquet d'installation.

2. Lancez le programme de suppression de l'Agent d'administration. Pour ce faire, ouvrez le paquet d'installation **Suppression de Kaspersky Network Agent** dans la fenêtre du contenu du paquet d'installation.

   Suivez les étapes du programme de suppression.

3. Dans la fenêtre **Introduction**, cliquez sur le bouton **Poursuivre**.

4. Dans la fenêtre **Informations**, lisez les informations importantes. Pour lancer la procédure de suppression, cliquez sur le bouton **Supprimer** et saisissez le mot de passe de l'administrateur pour confirmer. Attendez pendant la suppression de l'application.

5. Dans la fenêtre **Fin**, lisez les informations sur la fin du processus de suppression et cliquez sur le bouton **Terminer** pour quitter le programme de suppression.

INSTALLATION A DISTANCE DE KASPERSKY ENDPOINT SECURITY

Kaspersky Endpoint Security peut être installé sur l'ordinateur de l'utilisateur d'une des méthodes suivantes :

- localement (cf. section "Installation de l'application" à la page 20) ;
- à distance à l'aide du protocole SSH (cf. section "Installation de l'application à l'aide du protocole SSH" à la page 119) ;
- à distance via Kaspersky Administration Kit (cf. section "Installation de l'application via Kaspersky Administration Kit" à la page 120).

Cette section décrit comment supprimer l'application sur l'ordinateur de l'utilisateur via Kaspersky Administration Kit (cf. section "Suppression de l'application via Kaspersky Administration Kit" à la page 122).

DANS CETTE SECTION

INSTALLATION DE L'APPLICATION A L'AIDE DU PROTOCOLE SSH

Avant d'installer Kaspersky Endpoint Security sur un ordinateur distant, assurez-vous que les conditions suivantes sont remplies :

- Le serveur d'administration Kaspersky Administration Kit est déployé sur le réseau de l'entreprise[9].
- La console d'administration est installée sur le poste de travail de l'administrateur de Kaspersky Administration Kit.
- Le paquet d'installation pour l'application Kaspersky Endpoint Security a été créé et se trouve dans le dossier partagé du Serveur d'administration[10].
- Le fichier clé pour Kaspersky Endpoint Security est conservé dans le dossier partagé du Serveur d'administration (à la demande).

[9] Pour les détails, consultez le Guide de déploiement de Kaspersky Administration Kit.
[10] Lisez attentivement l'aide de Kaspersky Administration Kit.

Pour procéder à l'installation de Kaspersky Endpoint Security sur un ordinateur distant via le protocole SSH, procédez comme suit :

1. Activer le service **Session à distance** sur l'ordinateur Mac.
2. Sur le poste de travail de l'administrateur, lancez le client SSH et connectez-vous à l'ordinateur Mac distant.
3. Connectez le dossier partagé du Serveur d'administration en tant que disque réseau sur l'ordinateur distant. Pour ce faire, saisissez les instructions suivantes dans le terminal du client SSH :

   ```
   mkdir /Volumes/KLSHARE
   mount_smbfs //<admin_login>:<password>@<AK_server_address>/KLSHARE
   /Volumes/KLSHARE
   ```

   Description des paramètres:

   - **<admin_login>** : identifiant de l'administrateur du Serveur d'administration ;
   - **<password>** : mot de passe de l'administrateur du Serveur d'administration ;
   - **<AK_server_address>** : adresse IP du serveur sur lequel Kaspersky Administration Kit est installé.

4. Lancez le script d'installation. Pour ce faire, saisissez les instructions suivantes dans le terminal du client SSH :

   ```
   cd /Volumes/KLSHARE/Packages/<kes_package_folder>
   sudo ./install.sh
   ```

   où **<kes_package_folder>** désigne le dossier où se trouve le paquet d'installation pour Kaspersky Endpoint Security.

   L'exécution de cette instruction requiert les privilèges d'administrateur.

5. Déconnectez le disque réseau de l'ordinateur distant. Pour ce faire, saisissez l'instruction suivante dans le terminal du client SSH :

   ```
   umount /Volumes/KLSHARE
   ```

INSTALLATION DE L'APPLICATION VIA KASPERSKY ADMINISTRATION KIT

Avant d'installer Kaspersky Endpoint Security sur un ordinateur distant, assurez-vous que les conditions suivantes sont remplies :

- Le serveur d'administration Kaspersky Administration Kit est déployé sur le réseau de l'entreprise[11].
- La console d'administration est installée sur le poste de travail de l'administrateur de Kaspersky Administration Kit.
- L'Agent d'administration est installé sur l'ordinateur Mac.
- Le paquet d'installation pour l'application Kaspersky Endpoint Security a été créé et se trouve dans le dossier partagé du Serveur d'administration[12].
- Le fichier clé pour Kaspersky Endpoint Security est conservé dans le dossier partagé du Serveur d'administration (à la demande).
- L'ordinateur Mac est ajouté au groupe **Ordinateurs administrés** du Serveur d'administration (à la demande)[13].

[11] Pour les détails, consultez le Guide de déploiement de Kaspersky Administration Kit.
[12] Lisez attentivement l'aide de Kaspersky Administration Kit.

L'installation de Kaspersky Endpoint Security sur un ordinateur distant via Kaspersky Administration Kit s'opère via la création et l'exécution d'une tâche d'installation à distance de l'application.

Pour créer une tâche d'installation à distance de Kaspersky Endpoint Security sur un ordinateur distant via Kaspersky Administration Kit, procédez comme suit :

1. Lancez la Console d'administration de Kaspersky Administration Kit.
2. Déployez le nœud **Serveur d'administration** et sélectionnez le dossier **Tâches pour les sélections d'ordinateurs**.
3. Lancez l'Assistant de création de tâche en cliquant sur le lien **Créer une tâche** dans le volet des tâches. Suivez les étapes de l'Assistant pour créer la tâche d'installation à distance de Kaspersky Endpoint Security.
4. Dans le champ **Nom** de la fenêtre **Nom de la tâche** saisissez le nom de la tâche, puis cliquez sur le bouton **Suivant**.
5. Dans la fenêtre **Type de tâche**, sélectionnez la tâche **Installation à distance de l'application** dans la liste pour l'application Kaspersky Administration Kit, puis cliquez sur **Suivant**.
6. Dans la liste de la fenêtre **Paquet d'installation**, sélectionnez le paquet d'installation pour l'application Kaspersky Endpoint Security, puis cliquez sur **Suivant**.
7. Dans la fenêtre **Méthode d'installation**, choisissez l'option **Installation forcée** en guise de méthode d'installation à distance, puis cliquez sur **Suivant**.
8. Dans la fenêtre **Paramètres**, configurez les paramètres de l'installation à distance de l'application, puis cliquez sur **Suivant**.
9. Dans la fenêtre **Avancé**, désignez le paquet d'installation complémentaire pour l'installation conjointe des applications, si nécessaire. Cliquez sur **Suivant**.
10. Dans la fenêtre **Redémarrage**, choisissez l'option **Ne pas redémarrer l'ordinateur**, puis cliquez sur le bouton **Suivant**.

    Il n'est pas nécessaire de redémarrer l'ordinateur après l'installation de l'application.

11. Sélectionnez, dans la fenêtre **Mode de sélection des postes clients**, l'option de sélection des ordinateurs pour l'installation de l'application qui vous convient le mieux. Vous pouvez installer l'application :

    - sur la base des données obtenues lors du sondage du réseau Windows ;
    - sur la base des adresses d'ordinateurs saisies manuellement.

    Cliquez sur **Suivant**.
12. Dans la fenêtre **Postes clients**, désignez les ordinateurs pour lesquels la tâche d'installation à distance sera créée, conformément à l'option choisie à l'étape antérieure. Cliquez sur **Suivant**.
13. Dans la fenêtre **Compte**, cliquez sur le bouton **Suivant**.
14. Dans la fenêtre **Planification de l'exécution de la tâche**, sélectionnez le mode de lancement de la tâche : manuel ou selon un horaire défini. Pour ce faire, sélectionnez dans la liste déroulante la fréquence de lancement de la tâche et indiquez l'heure de lancement de la tâche. Cliquez sur **Suivant**.
15. La dernière fenêtre de l'Assistant vous informe de la réussite de la création de la tâche. Cliquez sur le bouton **Terminer** pour quitter l'Assistant.

La tâche créée apparaît dans l'arborescence de la console dans le dossier **Tâches pour les sélections d'ordinateurs**.

[13] Lisez attentivement le Guide de l'administrateur de Kaspersky Administration Kit.

SUPPRESSION DE L'APPLICATION VIA KASPERSKY ADMINISTRATION KIT

En supprimant Kaspersky Endpoint Security d'un ordinateur distant, vous exposez ce dernier à un grave risque d'infection.

Avant de supprimer Kaspersky Endpoint Security d'un ordinateur distant, assurez-vous que les conditions suivantes sont remplies :

- Le serveur d'administration Kaspersky Administration Kit est déployé sur le réseau de l'entreprise[14].
- La console d'administration est installée sur le poste de travail de l'administrateur de Kaspersky Administration Kit.
- L'Agent d'administration et Kaspersky Endpoint Security sont installés sur l'ordinateur Mac.

La suppression de Kaspersky Endpoint Security depuis un poste client via Kaspersky Administration Kit s'opère via la création et l'exécution d'une tâche de suppression de l'application à distance.

Pour créer une tâche de suppression à distance de Kaspersky Endpoint Security sur un ordinateur distant via Kaspersky Administration Kit, procédez comme suit :

1. Lancez la Console d'administration de Kaspersky Administration Kit.
2. Déployez le nœud **Serveur d'administration** et sélectionnez le dossier **Tâches pour les sélections d'ordinateurs**.
3. Lancez l'Assistant de création de tâche en cliquant sur le lien **Créer une tâche** dans le volet des tâches. Suivez les étapes de l'Assistant pour créer la tâche d'installation à distance de Kaspersky Endpoint Security.
4. Dans le champ **Nom** de la fenêtre **Nom de la tâche** saisissez le nom de la tâche, puis cliquez sur le bouton **Suivant**.
5. Dans la liste de la fenêtre **Type de tâche**, sélectionnez l'application Kaspersky Administration Kit et la tâche **Tâche de désinstallation à distance de l'application** dans le dossier **Avancé**. Cliquez sur **Suivant**.
6. Dans la liste déroulante de la fenêtre **Paramètres**, sélectionnez l'application **Kaspersky Endpoint Security 8 for Mac**, puis cliquez sur le bouton **Suivant**.
7. Dans la fenêtre **Méthode de désinstallation à distance**, choisissez l'option **Désinstallation forcée** en guise de méthode de désinstallation, puis cliquez sur **Suivant**.
8. Dans la fenêtre **Paramètres**, configurez les paramètres de désinstallation à distance de l'application, puis cliquez sur **Suivant**.
9. Dans la fenêtre **Redémarrage**, choisissez l'option **Ne pas redémarrer l'ordinateur**, puis cliquez sur le bouton **Suivant**.

   Il n'est pas nécessaire de redémarrer l'ordinateur après la suppression de Kaspersky Endpoint Security.

10. Dans la fenêtre **Postes clients**, désignez les ordinateurs pour lesquels la tâche de désinstallation à distance de l'application sera créée. Cliquez sur **Suivant**.
11. Dans la fenêtre **Compte**, cliquez sur le bouton **Suivant**.

[14] Pour les détails, consultez le Guide de déploiement de Kaspersky Administration Kit.

12. Dans la fenêtre **Planification de l'exécution de la tâche**, sélectionnez le mode de lancement de la tâche : manuel ou selon un horaire défini. Pour ce faire, sélectionnez dans la liste déroulante la fréquence de lancement de la tâche et indiquez l'heure de lancement de la tâche. Cliquez sur **Suivant**.

13. La dernière fenêtre de l'Assistant vous informe de la réussite de la création de la tâche. Cliquez sur le bouton **Terminer** pour quitter l'Assistant.

La tâche créée apparaît dans l'arborescence de la console dans le dossier **Tâches pour les sélections d'ordinateurs**.

ADMINISTRATION DE L'AGENT D'ADMINISTRATION

L'administration de l'Agent d'administration est réalisée à l'aide de la ligne de commande sur l'ordinateur de l'utilisateur.

Kaspersky Administration Kit présente la possibilité de la connexion manuelle du poste client au Serveur d'administration en utilisant l'utilitaire klmover et de l'analyse de la connexion du poste client avec le Serveur d'administration à l'aide de l'utilitaire klnagchk.exe.

Vous pouvez aussi arrêter le fonctionnement de l'Agent d'administration et de le relancer.

DANS CETTE SECTION

CONNEXION MANUELLE DU POSTE CLIENT AU SERVEUR D'ADMINISTRATION. UTILITAIRE KLMOVER

Pour connecter le poste client au Serveur d'administration,

depuis la ligne de commande du poste client, lancez l'outil klmover compris dans le paquet d'installation de l'Agent d'administration.

Après l'installation de l'Agent d'administration, cet utilitaire se trouve dans le dossier /Library/Application Support/Kaspersky Lab/klnagent/Binaries et lors du lancement depuis la ligne de commande, exécute les actions suivantes selon les paramètres utilisés :

- connecte l'Agent d'administration au Serveur d'administration, en utilisant les paramètres indiqués ;
- enregistre les résultats de l'opération dans le fichier indiqué, ou les affiche à l'écran.

Avant le lancement de l'utilitaire, passez au dossier /Library/Application Support/Kaspersky Lab/klnagent/Binaries.

Syntaxe de l'utilitaire :

```
sudo ./klmover [-logfile <nomFichier>] 1 [-address <adresse serveur>] [-pn <numéro du port>] [-ps < numéro du port SSL>] [-nossl] [-cert <chemin du fichier certificat>] [-silent][-dupfix]
```

Le lancement de l'utilitaire requiert les privilèges d'administrateur.

Description des paramètres:

-logfile <nomFichier> : enregistre les résultats de l'exécution dans le fichier indiqué ; si le paramètre n'est pas indiqué, les résultats et les messages d'erreur sont affichés à l'écran.

-address <adresse serveur> : adresse du Serveur d'administration pour la connexion ; l'adresse peut être une adresse IP ou un nom DNS du serveur.

-pn <numéro du port> : numéro de port à utiliser pour une connexion non sécurisée au Serveur d'administration, par défaut le port 14000 est utilisé.

-ps <numéro du port SSL> : numéro de port SSL à utiliser pour une connexion sécurisée au Serveur d'administration sous protocole SSL. Par défaut le port 13000 est utilisé.

-nossl : utilise une connexion non sécurisée au Serveur d'administration ; si aucune clé n'est indiquée, la connexion de l'Agent d'administration au serveur sera réalisée à l'aide du protocole sécurisé SSL.

-cert <chemin du fichier certificat> : utilise le fichier de certificat spécifié pour l'authentification sur le nouveau Serveur d'administration. Si aucun paramètre n'est indiqué, l'Agent d'administration recevra le certificat lors de la première connexion au Serveur d'administration.

-silent : exécute l'utilitaire en mode non interactif.

-dupfix : paramètre utilisé en cas d'installation de l'Agent d'administration par une méthode différente de la normale (avec le kit de distribution), par exemple, par restauration depuis une image disque.

Il est recommandé de lancer l'utilitaire en indiquant les valeurs de tous les paramètres.

Exemple :

```
sudo ./klmover -logfile klmover.log -address 192.0.2.12 -ps 13001
```

VERIFICATION MANUELLE DE LA CONNEXION DU POSTE CLIENT AU SERVEUR D'ADMINISTRATION. UTILITAIRE KLNAGCHK

Pour vérifier la connexion du poste client avec le Serveur d'administration,

depuis la ligne de commande du poste client, lancez l'outil klnagchk compris dans le paquet d'installation de l'Agent d'administration.

Après l'installation de l'Agent d'administration, cet utilitaire se trouve dans le dossier /Library/Application Support/Kaspersky Lab/klnagent/Binaries et lors du lancement depuis la ligne de commande, exécute les actions suivantes selon les paramètres utilisés :

- renvoie à l'écran ou enregistre dans un fichier les valeurs des paramètres de connexion de l'Agent d'administration installé sur le poste client, utilisés afin de se connecter au Serveur d'administration ;
- enregistre dans le fichier indiqué les statistiques du fonctionnement de l'Agent d'administration (à partir du dernier démarrage du composant) et les résultats de son activité, ou les affiche à l'écran ;
- il tente de connecter l'Agent d'administration au Serveur d'administration ;
- si la connexion n'a pas pu être établie, il envoie un paquet ICMP au poste sur lequel est installé le Serveur d'administration afin de vérifier l'état du poste.

Avant le lancement de l'utilitaire, passez au dossier /Library/Application Support/Kaspersky Lab/klnagent/Binaries.

Syntaxe de l'utilitaire :

```
sudo ./klnagchk [-logfile <nomFichier>] 1 [-sp] [-savecert <chemin du fichier certificat>] [-restart]
```

Le lancement de l'utilitaire requiert les privilèges d'administrateur.

Description des paramètres

-logfile <nomFichier> : enregistrer les valeurs des paramètres de connexion utilisées par l'Agent d'administration pour se connecter au Serveur, ainsi que les résultats de l'exécution ; si le paramètre n'est pas indiqué, les paramètres de connexion au Serveur, les résultats et les messages d'erreur sont affichés à l'écran.

-sp : afficher sur l'écran le mot de passe (ou l'enregistrer dans le fichier pour les journaux) utilisé pour authentifier l'utilisateur sur le serveur proxy ; ce paramètre est utilisé si la connexion au Serveur d'administration est effectuée via un serveur proxy. Par défaut il n'est pas utilisé.

-savecert <nom du fichier> : enregistrer le certificat utilisé pour l'authentification sur le Serveur d'administration dans le fichier spécifié.

-restart : redémarre l'Agent d'administration après la fin du fonctionnement de l'utilitaire.

Exemple :

```
sudo ./klnagchk -logfile klnagchk.log -sp
```

LANCEMENT/ARRET DE L'AGENT D'ADMINISTRATION SUR LE POSTE CLIENT

Vous pouvez arrêter le fonctionnement de l'Agent d'administration et le relancer sur l'ordinateur d'utilisateur à l'aide de la ligne de commande.

- *Pour arrêter le fonctionnement de l'Agent d'administration,*

  sur le poste client depuis la ligne de commande, lancez l'utilitaire launchctl avec la commande unload.

Syntaxe de la commande

```
launchctl unload /Library/LaunchDaemons/com.kaspersky.klnagent.plist
```

- *Pour lancer l'Agent d'administration,*

  sur le poste client depuis la ligne de commande, lancez l'utilitaire launchctl avec la commande load.

Syntaxe de la commande

```
launchctl load /Library/LaunchDaemons/com.kaspersky.klnagent.plist
```

L'arrêt et le lancement de l'Agent d'administration requièrent les privilèges d'administrateur.

ADMINISTRATION DU LOGICIEL

Kaspersky Administration Kit permet d'administrer à distance le lancement et l'arrêt de Kaspersky Endpoint Security sur un poste client distinct et de configurer les paramètres généraux de fonctionnement de l'application : activation et désactivation de la protection du système de fichiers de l'ordinateur, configuration de l'affichage de l'icône de Kaspersky Endpoint Security et configuration des paramètres des rapports et des banques.

Pour passer à la configuration des paramètres du fonctionnement de l'application, procédez comme suit :

1. Lancez la Console d'administration de Kaspersky Administration Kit.

2. Déployez le nœud **Serveur d'administration**.

3. Dans le dossier **Ordinateurs administrés**, sélectionnez le dossier portant le nom du groupe auquel appartient le poste client, puis choisissez le sous-dossier **Postes clients**.

4. Dans le volet des résultats à droite, sélectionnez l'ordinateur sur lequel l'application Kaspersky Endpoint Security est installée.

5. Choisissez l'option **Propriétés** dans le menu contextuel qui s'ouvre d'un clic droit de la souris. Ouvrez la fenêtre des propriétés du poste client.

6. Dans la liste de toutes les applications de Kaspersky Lab installées sur ce serveur sous l'onglet **Applications** (cf. ill. ci-après), choisissez l'option **Kaspersky Endpoint Security 8 for Mac**.

   Les boutons d'administration se trouvent sous la liste des applications :

   - **Evénements**. Cliquez sur ce bouton pour ouvrir la fenêtre **Evénements** qui reprend la liste des événements survenus pendant l'utilisation de l'application su le poste client et consignés sur le Serveur d'administration ;

   - **Statistiques**. Cliquez sur ce bouton pour ouvrir la fenêtre **Statistiques** qui permet de consulter les statistiques actuelles du fonctionnement de l'application ;

   - **Propriétés**. Cliquez sur ce bouton pour ouvrir la fenêtre de configuration des paramètres de l'application (cf. section "Configuration des paramètres de l'application" à la page 128).

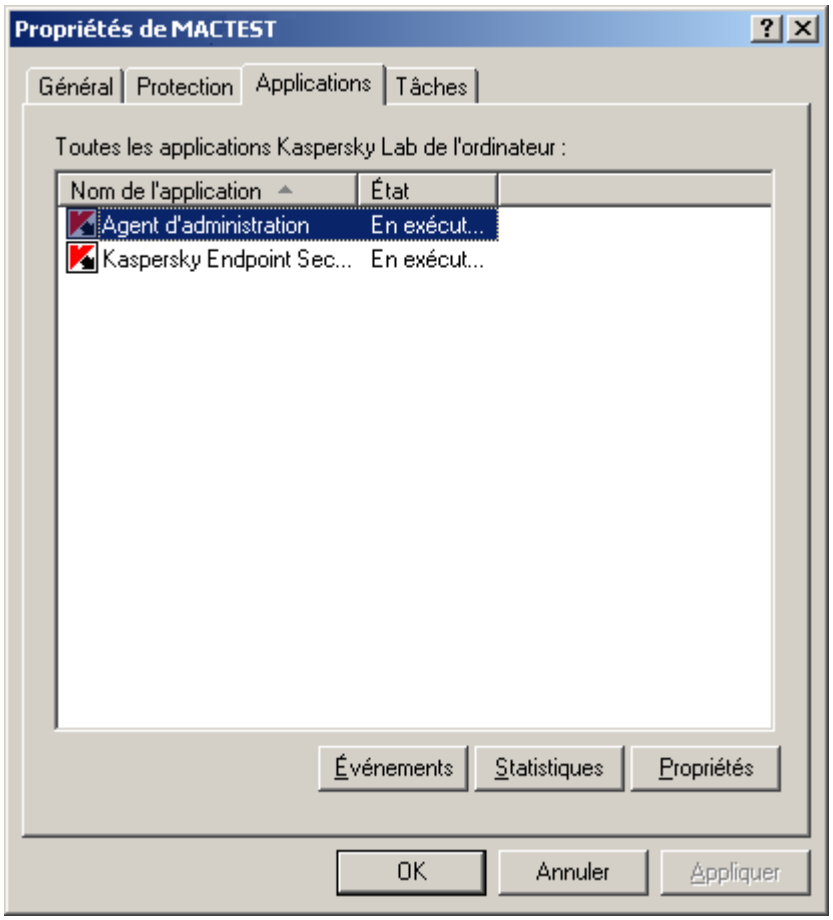


Illustration 58. Fenêtre des propriétés de l'ordinateur client. Onglet Applications

DANS CETTE SECTION

LANCEMENT ET ARRET DE L'APPLICATION

L'onglet **Général** de la fenêtre de configuration des paramètres de l'application permet d'administrer le lancement et l'arrêt de Kaspersky Endpoint Security sur le poste client distant.

La partie supérieure de la fenêtre reprend le nom de l'application, sa version, la date d'installation et la date de dernière mise à jour, son état actuel (en exécution ou arrêtée sur l'ordinateur local) ainsi que des informations sur l'état des bases de l'application.

Pour arrêter ou démarrer Kaspersky Endpoint Security sur un ordinateur distant, procédez comme suit :

1. Ouvrez la fenêtre des propriétés du poste client (cf. section "Administration de l'application" à la page 125) sous l'onglet **Applications**.

2. Dans la liste de toutes les applications de Kaspersky Lab installées sur ce serveur sous l'onglet, choisissez l'option **Kaspersky Endpoint Security 8 for Mac**, puis cliquez sur le bouton **Propriétés**.

3. Dans la fenêtre de configuration de l'application qui s'ouvre (cf. ill. ci-après), sélectionnez l'onglet **Général**, puis cliquez sur le bouton **Arrêter** pour arrêter l'application ou sur **Démarrer** pour la lancer. Patientez pendant que Kaspersky Administration Kit exécute l'action sur le poste client distant.

Quand Kaspersky Endpoint Security est arrêté sur l'ordinateur distant, l'ordinateur continue à fonctionner sans protection et il risque d'être infecté.

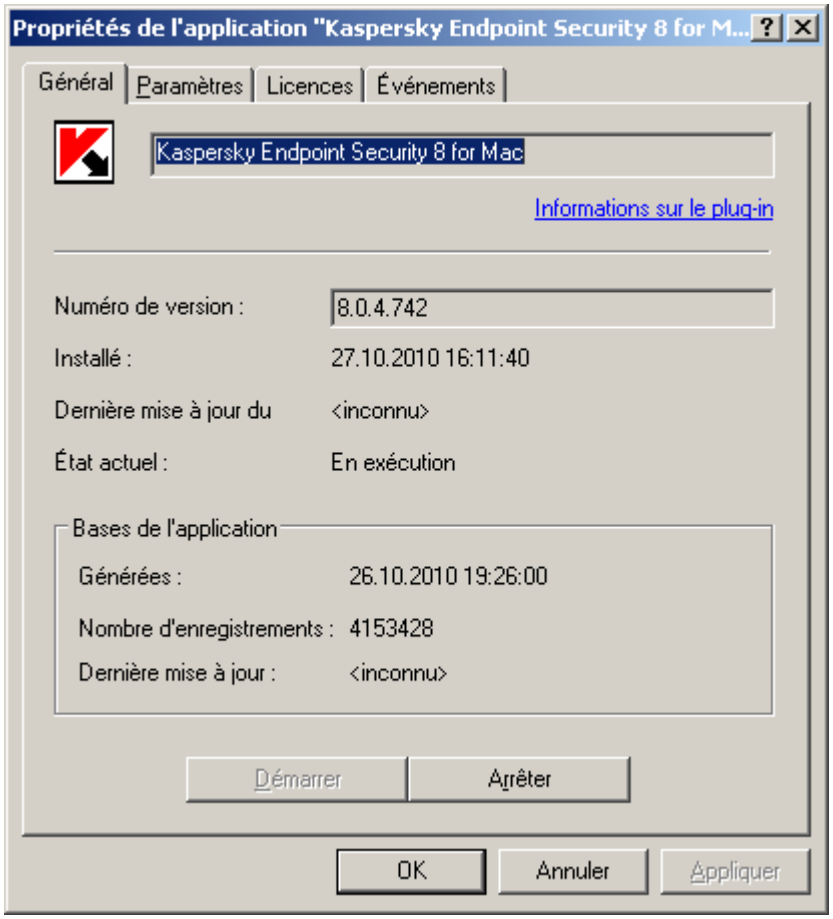


Illustration 59. Fenêtre de configuration des paramètres de l'application. Onglet Général

CONFIGURATION DES PARAMETRES DE L'APPLICATION

Vous pouvez consulter et modifier les paramètres de l'application sur le poste client distant sous l'onglet **Paramètres** de la fenêtre de configuration de l'application (cf. ill. ci-après).

Les onglets **Licence** et **Événements** sont standard pour l'application Kaspersky Administration Kit[15].

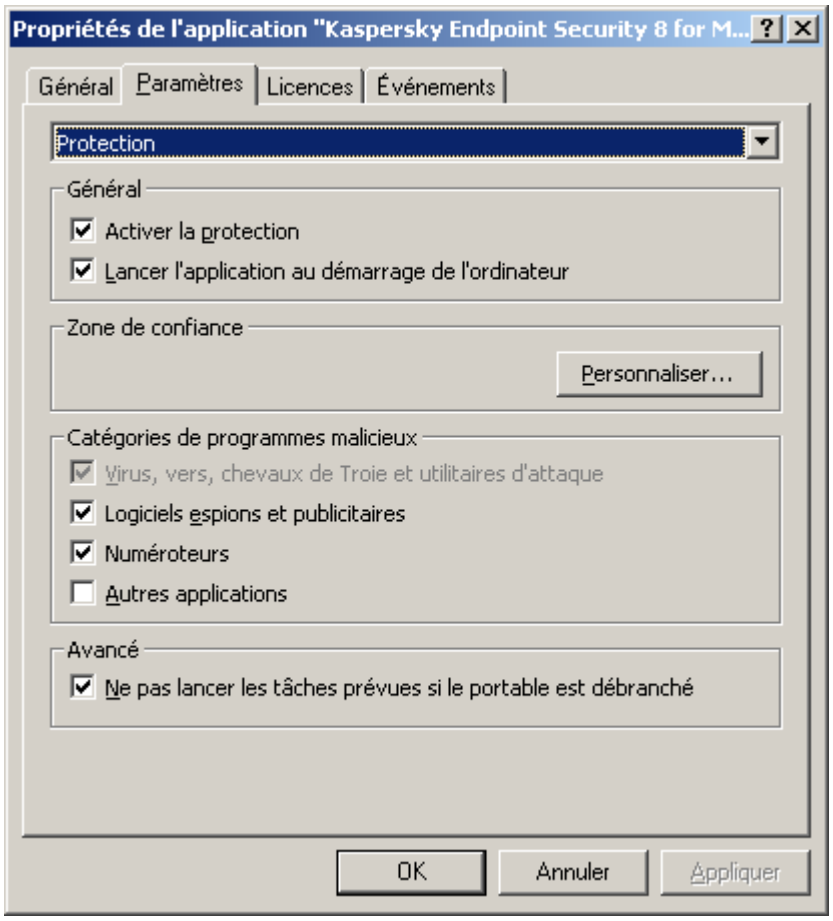


Illustration 60. Fenêtre de configuration des paramètres de l'application. Onglet Paramètres. Protection

Si une stratégie, interdisant la modification de certains paramètres a été créée pour l'application, la modification de la configuration de l'application sera impossible.

ACTIVATION ET DESACTIVATION DE LA PROTECTION DES FICHIERS

Les experts de Kaspersky Lab vous recommandent vivement de ne pas désactiver la protection offerte par l'Antivirus Fichiers en temps réel sur l'ordinateur distant, car cela pourrait entraîner l'infection de votre ordinateur et la perte de données.

Pour désactiver l'Antivirus Fichiers sur l'ordinateur distant, procédez comme suit :

1. Ouvrez la fenêtre des propriétés du poste client (cf. section "Administration de l'application" à la page 125) sous l'onglet **Applications**.
2. Dans la liste de toutes les applications de Kaspersky Lab installées sur ce serveur sous l'onglet, choisissez l'option **Kaspersky Endpoint Security 8 for Mac**, puis cliquez sur le bouton **Propriétés**.
3. Dans la fenêtre de configuration des paramètres qui s'ouvre, sélectionnez l'onglet **Paramètres**.
4. Dans la liste déroulante, située dans la partie supérieure de la fenêtre, choisissez **Protection**.

[15] Lisez attentivement l'aide de Kaspersky Administration Kit.

5. Dans le groupe **Général** (cf. ill. ci-après), décochez la case **Activer la protection**, puis cliquez sur le bouton **Appliquer**.

Pour activer l'Antivirus Fichiers sur l'ordinateur distant, procédez comme suit :

1. Ouvrez la fenêtre des propriétés du poste client (cf. section "Administration de l'application" à la page 125) sous l'onglet **Applications**.

2. Dans la liste de toutes les applications de Kaspersky Lab installées sur ce serveur sous l'onglet, choisissez l'option **Kaspersky Endpoint Security 8 for Mac**, puis cliquez sur le bouton **Propriétés**.

3. Dans la fenêtre de configuration des paramètres qui s'ouvre, sélectionnez l'onglet **Paramètres**.

4. Dans la liste déroulante, située dans la partie supérieure de la fenêtre, choisissez l'élément **Protection**.

5. Dans le groupe **Général** (cf. ill. ci-après), cochez la case **Activer la protection**, puis cliquez sur le bouton **Appliquer**.

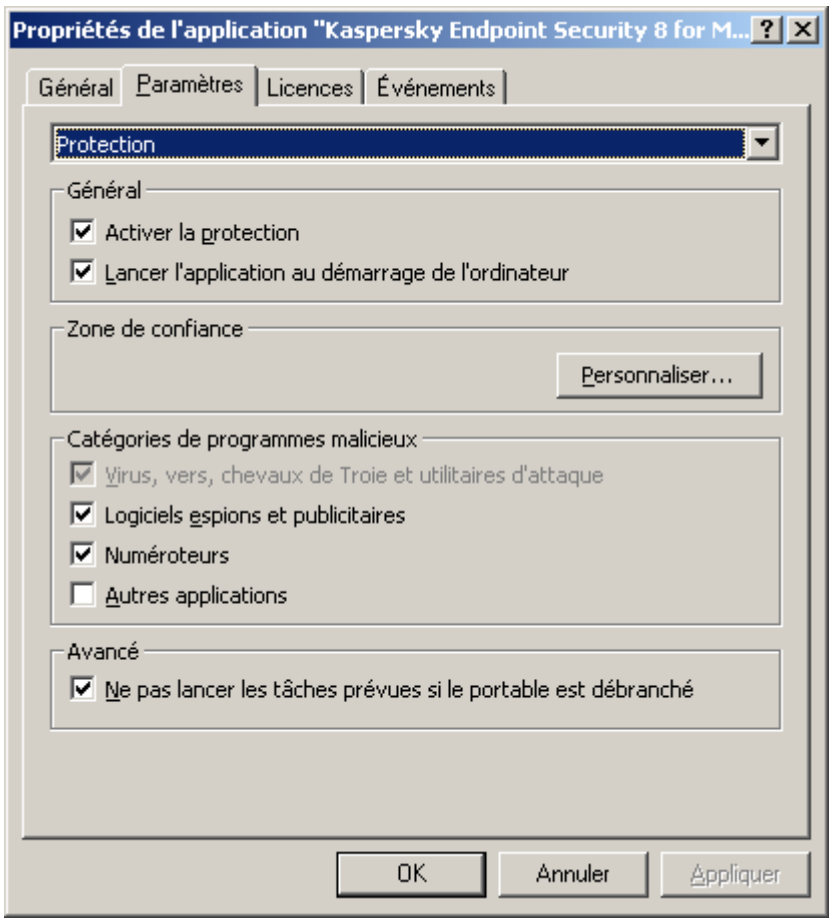


Illustration 61. Fenêtre de configuration des paramètres de l'application. Onglet Paramètres. Protection

VOIR EGALEMENT

Antivirus Fichiers 56

CONFIGURATION DU LANCEMENT AUTOMATIQUE DE KASPERSKY ENDPOINT SECURITY

Par défaut, Kaspersky Endpoint Security est lancé automatiquement au démarrage de l'ordinateur distant ou après le redémarrage du système d'exploitation.

- *Pour désactiver le mode de lancement automatique de Kaspersky Endpoint Security sur un ordinateur distant, procédez comme suit :*

1. Ouvrez la fenêtre des propriétés du poste client (cf. section "Administration de l'application" à la page 125) sous l'onglet **Applications**.
2. Dans la liste de toutes les applications de Kaspersky Lab installées sur ce serveur sous l'onglet, choisissez l'option **Kaspersky Endpoint Security 8 for Mac**, puis cliquez sur le bouton **Propriétés**.
3. Dans la fenêtre de configuration des paramètres qui s'ouvre, sélectionnez l'onglet **Paramètres**.
4. Dans la liste déroulante, située dans la partie supérieure de la fenêtre, choisissez l'élément **Protection**.
5. Dans le groupe **Général** (cf. ill. ci-dessus), décochez la case **Lancer l'application au démarrage de l'ordinateur**, puis cliquez sur **Appliquer**.

Si vous désactivez le mode de lancement automatique de Kaspersky Endpoint Security, alors après le prochain démarrage de l'ordinateur distant ou redémarrage du système d'exploitation, votre ordinateur ne sera plus protégé et il risque d'être infecté.

CONSTITUTION DE LA ZONE DE CONFIANCE

- *Pour créer une règle d'exclusion ou pour consulter et modifier des règles d'exclusion existantes pour Kaspersky Endpoint Security, installé sur l'ordinateur distant, procédez comme suit :*

1. Ouvrez la fenêtre des propriétés du poste client (cf. section "Administration de l'application" à la page 125) sous l'onglet **Applications**.
2. Dans la liste de toutes les applications de Kaspersky Lab installées sur ce serveur sous l'onglet, choisissez l'option **Kaspersky Endpoint Security 8 for Mac**, puis cliquez sur le bouton **Propriétés**.
3. Dans la fenêtre de configuration des paramètres qui s'ouvre, sélectionnez l'onglet **Paramètres**.
4. Dans la liste déroulante, située dans la partie supérieure de la fenêtre, choisissez l'élément **Protection**.
5. Dans le groupe **Zone de confiance** (cf. ill. ci-dessus), cliquez sur le bouton **Configurer**. La fenêtre **Zone de confiance** (cf. ill. ci-après) contenant la liste des objets qui ne seront pas analysés par Kaspersky Endpoint Security s'ouvre.

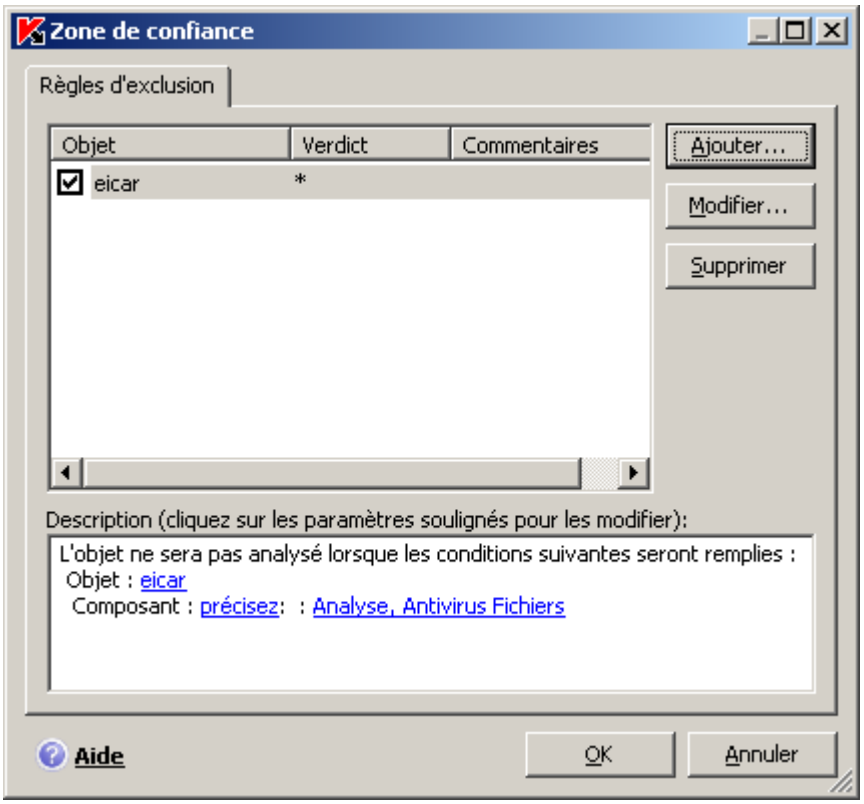


Illustration 62. Fenêtre Zone de confiance

Vous pouvez exécuter les opérations suivantes :

- Créer une nouvelle règle d'exclusion.

  Cliquez sur le bouton **Ajouter**, et dans la fenêtre ouverte **Règle d'exclusion** (cf. ill. ci-après), définissez ses conditions.

- Modifier une règle d'exclusion déjà créée.

  Sélectionnez une règle d'exclusion dans la liste et cliquez sur le bouton **Modifier**. Dans la fenêtre ouverte **Règle d'exclusion**, apportez les modifications dans ses conditions.

- Refuser temporairement l'utilisation d'une règle d'exclusion.

  Sélectionnez la règle d'exclusion dans la liste et décochez la case à côté de cette règle. La règle d'exclusion ne va pas être appliquée jusqu'à ce que la case ne soit pas cochée.

- Supprimer une règle d'exclusion.

  Sélectionnez une règle d'exclusion dans la liste et cliquez sur le bouton **Supprimer**.

Création d'une règle d'exclusion

Dans la fenêtre **Règle d'exclusion** qui s'ouvre, définissez les conditions de la règle d'exclusion à l'aide des paramètres suivants :

- **Objet**. Cochez la case **Objet** dans le champ **Paramètres** si l'objet à exclure est un fichier, un dossier ou un masque de fichier. Pour indiquer le nom/le masque de nom de l'objet, cliquez sur le lien **Objet :** dans le champ **Description** pour ouvrir la fenêtre **Nom de l'objet** et saisissez le nom du fichier, du dossier ou le masque du fichier.

- **Verdict**. Cochez la case **Verdict** dans le champ **Paramètres** pour exclure de l'analyse les objets sur la base du type de menace attribué selon le classement de l'Encyclopédie des virus. Pour indiquer le nom/le masque de la menace, cliquez sur le lien **Verdict** pour ouvrir la fenêtre **Verdict** et saisissez le nom ou le masque de la menace selon la classification de l'Encyclopédie des virus.

- **Composant**. Pour désigner le composant de Kaspersky Endpoint Security qui doit utiliser la règle créée, cliquez sur le lien **Composant :** dans le champ **Description** pour ouvrir la fenêtre **Composants/tâches à exclure** et cochez la case en regard des noms des composants : **Antivirus Fichiers** ou **Analyse**.

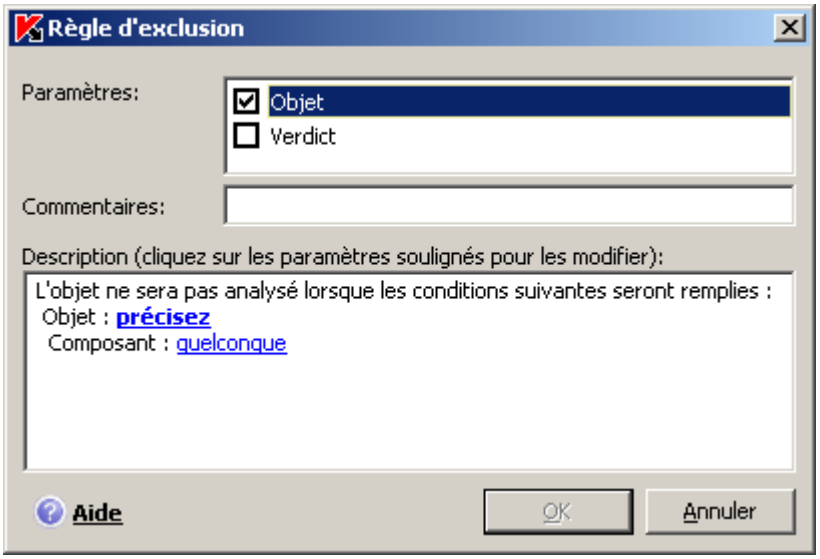


Illustration 63. Fenêtre Règles d'exclusion

VOIR EGALEMENT

Constitution de la zone de confiance 53

SELECTION DES PROGRAMMES MALVEILLANTS CONTROLES

Pour sélectionner du groupe le programme malveillant, contre lequel Kaspersky Endpoint Security va protéger l'ordinateur distant, procédez comme suit :

1. Ouvrez la fenêtre des propriétés du poste client (cf. section "Administration de l'application" à la page 125) sous l'onglet **Applications**.

2. Dans la liste de toutes les applications de Kaspersky Lab installées sur ce serveur sous l'onglet, choisissez l'option **Kaspersky Endpoint Security 8 for Mac**, puis cliquez sur le bouton **Propriétés**.

3. Dans la fenêtre de configuration des paramètres qui s'ouvre, sélectionnez l'onglet **Paramètres**.

4. Dans la liste déroulante, située dans la partie supérieure de la fenêtre, choisissez l'élément **Protection**.

5. Cochez, dans le groupe **Catégories de programmes malicieux** (cf. ill. ci-après), la case en regard des groupes de programmes malveillants contre lesquels Kaspersky Endpoint Security doit protéger l'ordinateur.

Kaspersky Endpoint Security assure la protection de votre ordinateur contre les virus, les vers, les chevaux de Troie et les utilitaires d'attaque. Pour cette raison, il est impossible de décocher la case à côté de ce groupe. Les experts de Kaspersky Lab vous recommandent de ne pas désactiver le contrôle des logiciels espions, adwares et numéroteurs automatiques. Lorsque Kaspersky Endpoint Security considère un programme qui d'après vous n'est pas dangereux comme un programme de cette catégorie, il est conseillé de configurer une règle d'exclusion (cf. section "Constitution de la zone de confiance" à la page 131).

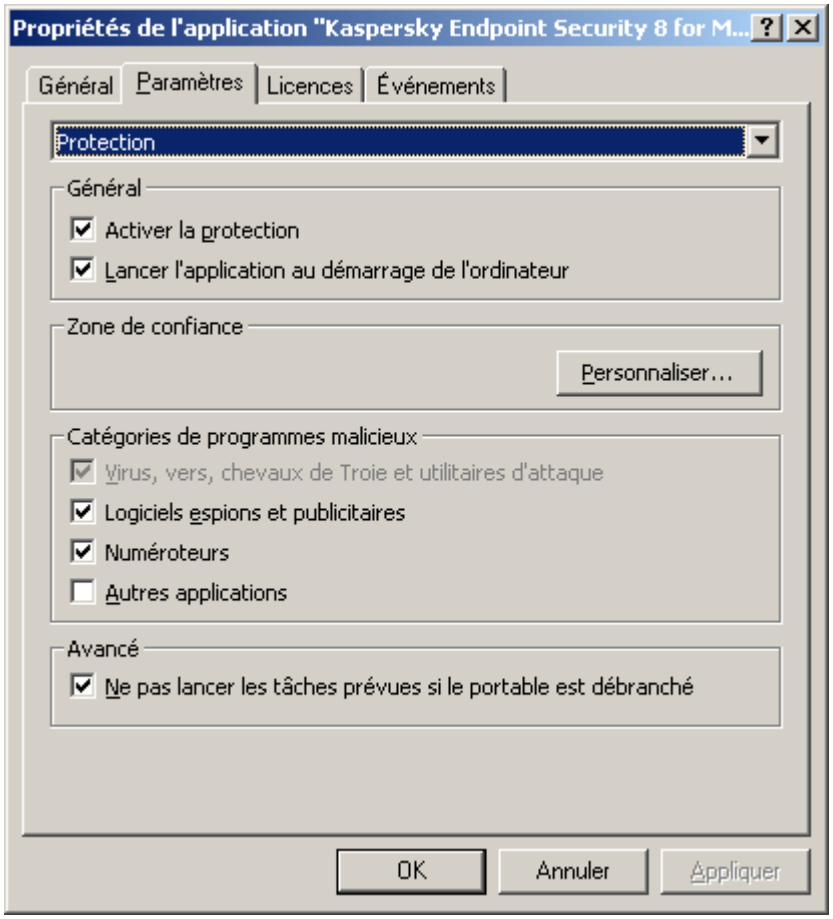


Illustration 64. Fenêtre de configuration des paramètres de l'application. Onglet Paramètres. Protection

VOIR EGALEMENT

Sélection des programmes malveillants contrôlés 51

CONFIGURATION DU MODE D'ECONOMIE DE LA CONSOMMATION ELECTRIQUE

Par défaut, Kaspersky Endpoint Security fonction en mode d'économie de la consommation électrique. Dans ce mode, les tâches d'analyse dont le lancement est programmé ne seront pas exécutées si l'ordinateur sur lequel est installée l'application est alimenté par la batterie.

Pour désactiver le mode d'économie de la consommation électrique sur l'ordinateur distant, procédez comme suit :

1. Ouvrez la fenêtre des propriétés du poste client (cf. section "Administration de l'application" à la page 125) sous l'onglet **Applications**.

2. Dans la liste de toutes les applications de Kaspersky Lab installées sur ce serveur sous l'onglet, choisissez l'option **Kaspersky Endpoint Security 8 for Mac**, puis cliquez sur le bouton **Propriétés**.

3. Dans la fenêtre de configuration des paramètres qui s'ouvre, sélectionnez l'onglet **Paramètres**.

4. Dans la liste déroulante, située dans la partie supérieure de la fenêtre, choisissez l'élément **Protection**.

5. Dans le groupe **Avancé** (cf. ill. ci-après) décochez la case **Ne pas lancer les tâches prévues si le portable est débranché**.

CONFIGURATION DE RECEPTION DES NOTIFICATIONS

Pour configurer la réception des notifications sur les événements survenus sur l'ordinateur distant, procédez comme suit :

1. Ouvrez la fenêtre des propriétés du poste client (cf. section "Administration de l'application" à la page 125) sous l'onglet **Applications**.

2. Dans la liste de toutes les applications de Kaspersky Lab installées sur ce serveur sous l'onglet, choisissez l'option **Kaspersky Endpoint Security 8 for Mac**, puis cliquez sur le bouton **Propriétés**.

3. Dans la fenêtre de configuration des paramètres qui s'ouvre, sélectionnez l'onglet **Paramètres**.

4. Dans la liste déroulante, située dans la partie supérieure de la fenêtre, choisissez l'élément **Interaction avec l'utilisateur**.

5. Dans le groupe **Notifications sur les événements** (cf. ill. ci-après), cochez la case **Activer les notifications** et passez à la configuration détaillée. Pour ce faire, cliquez sur **Avancé**.

La fenêtre qui s'ouvre vous permet de configurer les modes suivants d'envoi des notifications sur les événements mentionnés :

- *Fenêtre contextuelle*, contenant des informations sur l'événement survenu.

  Pour utiliser ce type de notification, cochez la case dans la colonne **Ecran** en regard des événements au sujet desquels vous souhaitez être alerté.

- *Notification sonore*.

  Si vous voulez accompagner cette infobulle d'un effet sonore, cochez la case **Son** en regard de l'événement.

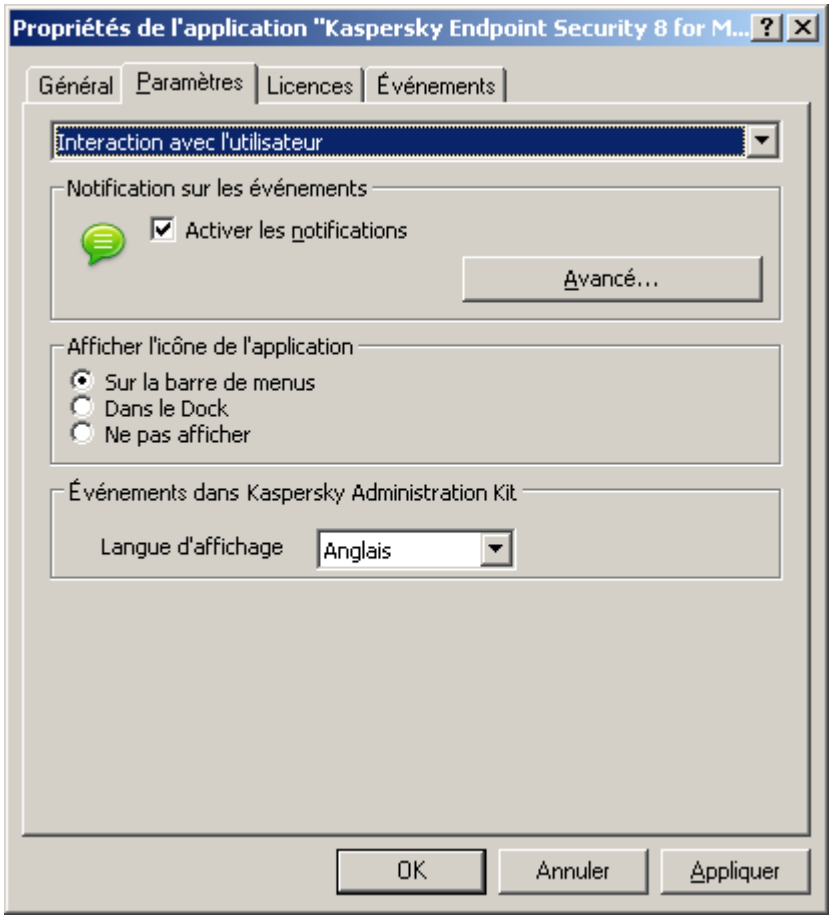


Illustration 65. Fenêtre de configuration des paramètres de l'application. Onglet Paramètres. Interaction avec l'utilisateur

VOIR EGALEMENT

Fenêtres de notification et fenêtres contextuelles 36

CONFIGURATION DE L'AFFICHAGE DE L'ICONE DE KASPERSKY ENDPOINT SECURITY

Par défaut, l'icône de Kaspersky Endpoint Security se trouve sur la barre de menus. Vous pouvez configurer l'application de telle sorte que son icône apparaisse dans le Dock de l'ordinateur distant ou n'apparaisse pas du tout.

Pour sélectionner l'affichage de l'icône de l'application sur l'ordinateur distant sur la barre de lancement rapide Dock, procédez comme suit :

1. Ouvrez la fenêtre des propriétés du poste client (cf. section "Administration de l'application" à la page 125) sous l'onglet **Applications**.
2. Dans la liste de toutes les applications de Kaspersky Lab installées sur ce serveur sous l'onglet, choisissez l'option **Kaspersky Endpoint Security 8 for Mac**, puis cliquez sur le bouton **Propriétés**.
3. Dans la fenêtre de configuration des paramètres qui s'ouvre, sélectionnez l'onglet **Paramètres**.
4. Dans la liste déroulante, située dans la partie supérieure de la fenêtre, choisissez l'élément **Interaction avec l'utilisateur**.

5. Dans le groupe **Afficher l'icône de l'application** (cf. ill. ci-dessus), sélectionnez l'option **Dans le Dock**.

Pour désactiver l'affichage de l'icône de l'application sur l'ordinateur distant, procédez comme suit :

1. Ouvrez la fenêtre des propriétés du poste client (cf. section "Administration de l'application" à la page 125) sous l'onglet **Applications**.

2. Dans la liste de toutes les applications de Kaspersky Lab installées sur ce serveur sous l'onglet, choisissez l'option **Kaspersky Endpoint Security 8 for Mac**, puis cliquez sur le bouton **Propriétés**.

3. Dans la fenêtre de configuration des paramètres qui s'ouvre, sélectionnez l'onglet **Paramètres**.

4. Dans la liste déroulante, située dans la partie supérieure de la fenêtre, choisissez l'élément **Interaction avec l'utilisateur**.

5. Dans le groupe **Afficher l'icône de l'application** (cf. ill. ci-dessus), sélectionnez l'option **Ne pas afficher**.

N'oubliez pas que la modification du paramètre n'entrera en vigueur qu'après le redémarrage de Kaspersky Endpoint Security.

VOIR EGALEMENT

Icône Kaspersky Endpoint Security..... 31

CONFIGURATION DES PARAMETRES DES RAPPORTS

Pour configurer la composition et la conservation des rapports sur le fonctionnement de Kaspersky Endpoint Security sur un poste distant, procédez comme suit :

1. Ouvrez la fenêtre des propriétés du poste client (cf. section "Administration de l'application" à la page 125) sous l'onglet **Applications**.

2. Dans la liste de toutes les applications de Kaspersky Lab installées sur ce serveur sous l'onglet, choisissez l'option **Kaspersky Endpoint Security 8 for Mac**, puis cliquez sur le bouton **Propriétés**.

3. Dans la fenêtre de configuration des paramètres qui s'ouvre, sélectionnez l'onglet **Paramètres**.

4. Dans la liste déroulante, située dans la partie supérieure de la fenêtre, choisissez l'élément **Rapports et Stockages**.

5. Dans le groupe **Rapports** (cf. ill. ci-après), configurez les paramètres suivants :

   - Consigner les événements à caractère informatif.

     En règle générale, ces événements ne jouent pas un rôle crucial dans la protection. Pour fixer de tels événements dans le rapport, cochez la case **Consigner les événements non critiques**.

   - Enregistrer dans le rapport uniquement les événements importants survenus lors du dernier lancement de la tâche.

     Cela permet de gagner de l'espace sur le disque en diminuant la taille du rapport. Si la case **Conserver uniquement les événements courants** est cochée, l'information présentée dans le rapport sera actualisée lors de chaque redémarrage de la tâche : par ailleurs, les informations importantes (par ex. : les enregistrements relatifs aux objets malveillants découverts) seront sauvegardées, et les informations à caractère non critique seront supprimées.

   - Définir le délai de conservation des rapports.

Par défaut, la durée de conservation des rapports est de 30 jours. Les objets sont supprimés à l'issue de cette période. Vous pouvez modifier la durée de conservation des rapports ou ne pas imposer de limite.

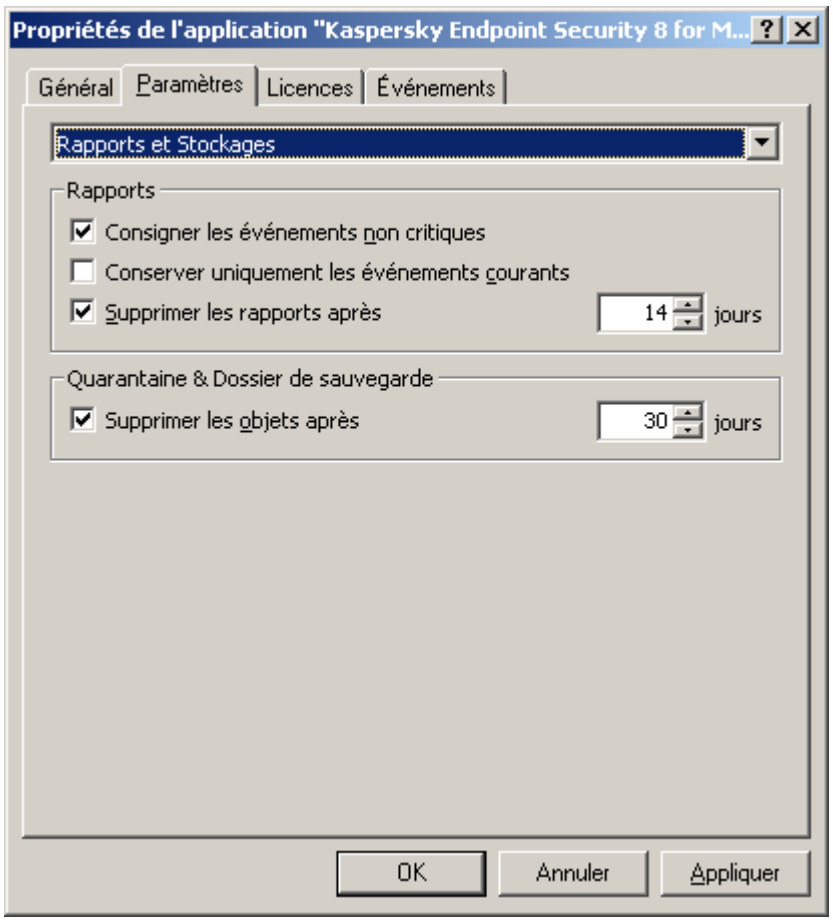


Illustration 66. Fenêtre de configuration des paramètres de l'application. Onglet Paramètres. Rapports et Stockages

CONFIGURATION DE LA QUARANTAINE ET DU DOSSIER DE SAUVEGARDE

Vous pouvez définir la durée maximale de conservation des objets dans la quarantaine et dans le dossier de sauvegarde sur l'ordinateur distant. Par défaut, la durée de conservation des objets est fixée à 30 jours, au terme desquels les objets sont supprimés. Vous pouvez modifier la durée maximum de conservation des objets ou ne pas imposer de limite.

Pour configurer les paramètres du dossier de sauvegarde des objets dans le dossier de sauvegarde, procédez comme suit :

1. Ouvrez la fenêtre des propriétés du poste client (cf. section "Administration de l'application" à la page 125) sous l'onglet **Applications**.

2. Dans la liste de toutes les applications de Kaspersky Lab installées sur ce serveur sous l'onglet, choisissez l'option **Kaspersky Endpoint Security 8 for Mac**, puis cliquez sur le bouton **Propriétés**.

3. Dans la fenêtre de configuration des paramètres qui s'ouvre, sélectionnez l'onglet **Paramètres**.

4. Dans la liste déroulante, située dans la partie supérieure de la fenêtre, choisissez l'élément **Rapports et Stockages**.

5. Dans le groupe **Quarantaine et Dossier de sauvegarde** (cf. ill. ci-dessus), cochez la case **Supprimer les objets après** et définissez le délai de conservation au terme duquel les objets seront automatiquement supprimés.

CONFIGURATION DES PARAMETRES DE CONNEXION AU SERVEUR PROXY

Si la connexion à Internet depuis le poste client distant s'opère via un serveur proxy, il faudra alors configurer les paramètres de connexion à ce dernier. Kaspersky Endpoint Security utilise ces paramètres pour la mise à jour des bases antivirus et des modules.

Pour configurer les paramètres de connexion de l'ordinateur distant au serveur proxy, procédez comme suit :

1. Ouvrez la fenêtre des propriétés du poste client (cf. section "Administration de l'application" à la page 125) sous l'onglet **Applications**.

2. Dans la liste de toutes les applications de Kaspersky Lab installées sur ce serveur sous l'onglet, choisissez l'option **Kaspersky Endpoint Security 8 for Mac**, puis cliquez sur le bouton **Propriétés**.

3. Dans la fenêtre de configuration des paramètres qui s'ouvre, sélectionnez l'onglet **Paramètres**.

4. Dans la liste déroulante, située dans la partie supérieure de la fenêtre, choisissez l'élément **Configuration du réseau**.

5. Cochez la case **Utiliser le serveur proxy** (cf. ill. ci-après) et configurez les paramètres suivants de connexion au serveur proxy :

   - utilisation par Kaspersky Endpoint Security des paramètres du serveur proxy, définis dans les paramètres système de Mac OS X ou les adresses et les ports de serveur proxy définis par l'utilisateur ;

   - possibilité d'utiliser le serveur proxy lors de la mise à jour depuis un dossier local ou réseau ;

   - paramètres d'authentification pour la connexion au serveur proxy.

En cas de mise à jour depuis un serveur FTP, la connexion est établie par défaut en mode passif. Si une erreur survient lors de cette connexion, une tentative de connexion en mode actif est lancée.

Par défaut, le temps réservé à l'établissement de la connexion avec le serveur de mise à jour est d'une minute. Si la connexion n'a pas été établie à l'issue de cet intervalle, l'application tentera d'établir la connexion avec la source suivante de mises à jour de la liste. Ce processus se poursuit tant qu'une connexion n'a pu être établie et tant que toutes les sources disponibles n'ont pas été sondées.

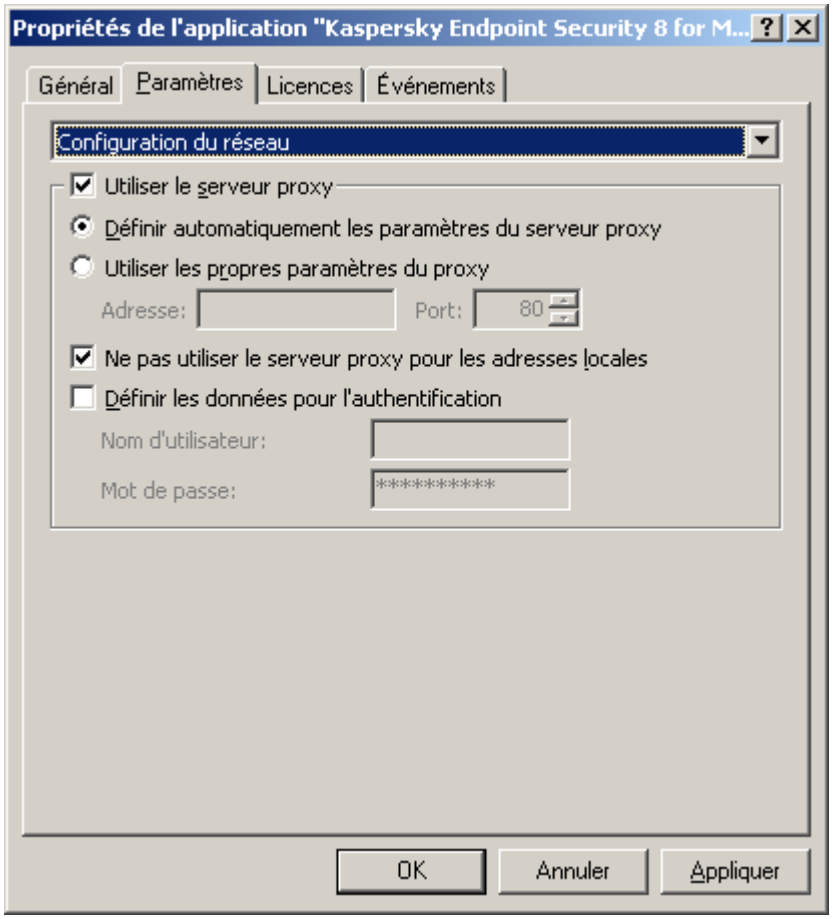


Illustration 67. Fenêtre de configuration des paramètres de l'application. Onglet Paramètres. Configuration du réseau

ADMINISTRATION DES TACHES

Cette section est consacrée à l'administration de tâches pour Kaspersky Endpoint Security[16].

Un ensemble de tâches système est créé pour chaque ordinateur du réseau lors de l'installation. Cette liste contient les tâches de la protection (Antivirus Fichiers), différentes tâches d'analyse (Analyse complète, analyse express) et des tâches de mise à jour (mise à jour des bases et des modules de l'application, remise à l'état antérieur à la mise à jour).

Vous pouvez administrer le lancement des tâches système et en configurer les paramètres. Il est toutefois impossible de les supprimer.

Il est possible de créer des tâches définies par l'utilisateur, par exemple des tâches d'analyse, de mise à jour de l'application ou de retour à l'état antérieur à la mise à jour, ou une tâche d'installation du fichier clé.

Les actions suivantes[17] peuvent être appliquées aux tâches définies par l'utilisateur :

- Configurer les paramètres de la tâche ;

[16] Lisez attentivement le Guide de l'administrateur de Kaspersky Administration Kit.
[17] Lisez attentivement l'aide de Kaspersky Administration Kit.

- Suivre l'exécution de la tâche ;
- Copier et transférer les tâches d'un groupe à un autre et supprimer les tâches à l'aide du menu contextuel ;
- Importer et exporter les tâches.

Pour ouvrir la liste des tâches créées pour le poste client, procédez comme suit :

1. Lancez la Console d'administration de Kaspersky Administration Kit.
2. Déployez le nœud **Serveur d'administration**.
3. Dans le dossier **Ordinateurs administrés**, sélectionnez le dossier portant le nom du groupe auquel appartient le poste client, puis choisissez le sous-dossier Postes clients.
4. Dans le volet des résultats à droite, sélectionnez l'ordinateur sur lequel l'application Kaspersky Endpoint Security est installée.
5. Choisissez l'option **Propriétés** dans le menu contextuel qui s'ouvre d'un clic droit de la souris. Ouvrez la fenêtre des propriétés du poste client.
6. Sélectionnez l'onglet **Tâches** (cf. ill. ci-après), pour consulter la liste complète des tâches créées pour ce poste client.

   Les boutons d'administration se trouvent sous la liste des tâches :

   - **Ajouter**. Cliquez sur ce bouton pour ouvrir l'Assistant de création d'une tâche (cf. page 144). Vous pouvez créer une tâche pour les applications de Kaspersky Lab installées sur cet ordinateur.
   - **Supprimer** en regard du message. Cliquez sur ce bouton pour ouvrir la demande de confirmation de l'action, après quoi la tâche sélectionnée dans la liste est supprimée.
   - **Résultats**. Cliquez sur ce bouton pour ouvrir la fenêtre **Résultats de l'exécution de la tâche**.
   - **Propriétés**. Cliquez sur ce bouton pour ouvrir la fenêtre des propriétés de la tâche. Vous pouvez consulter les paramètres de la tâche et introduire des modifications le cas échéant.

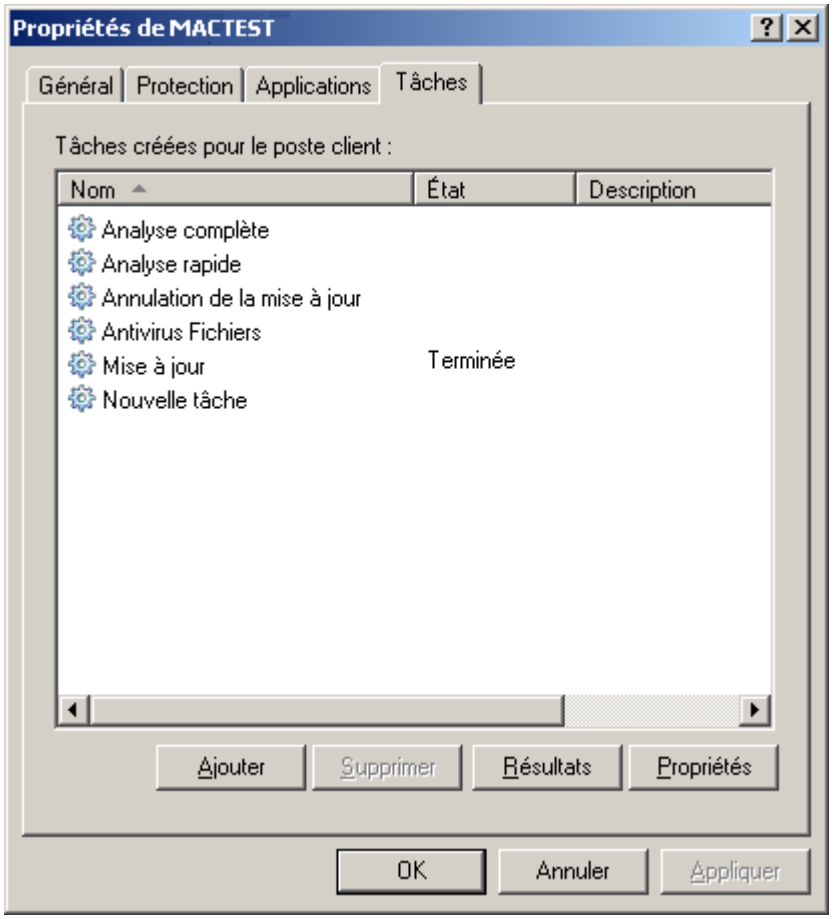


Illustration 68. Fenêtre des propriétés de l'ordinateur client. Onglet Tâches

DANS CETTE SECTION

LANCEMENT ET ARRET DES TACHES

Les tâches ne sont lancées sur un poste client que dans le cas où l'Agent d'administration est en lancé. En cas d'arrêt de l'Agent d'administration, l'exécution des tâches en cours sera interrompue.

Le lancement et l'arrêt des tâches s'opèrent soit automatiquement (selon l'horaire défini), soit manuellement (à l'aide de la commande du menu contextuel) ou depuis la fenêtre d'examen des paramètres de la tâche.

Pour lancer ou arrêter manuellement une tâche, procédez comme suit :

1. Ouvrez la fenêtre des propriétés du poste client (cf. section "Administration de l'application" à la page 125) sous l'onglet **Tâches** (cf. ill. ci-dessus).

2. Sélectionnez la tâche requise dans la liste, puis dans le menu contextuel ouvert d'un clic droit de la souris, choisissez l'option requise : **Démarrer** ou **Arrêter**.

   ou

   Sélectionnez la tâche souhaitée dans la liste et cliquez sur le bouton **Propriétés**. Lancez ou arrêtez l'exécution de la tâche à l'aide des boutons correspondants sous l'onglet **Général** de la fenêtre des propriétés de la tâche qui s'ouvre.

CREATION DES TACHES

Lorsque vous gérez Kaspersky Endpoint Security via Kaspersky Administration Kit, vous avez la possibilité de créer les types de tâche suivantes:

- des tâches locales, définies pour un ordinateur client distinct ;
- des tâches de groupe, définies pour les ordinateurs appartenant à un groupe d'administration donné ;
- des tâches pour une sélection d'ordinateurs, définies pour certains ordinateurs d'un groupe d'administration donné ;
- des tâches Kaspersky Administration Kit , dédicacées au Serveur de mise à jour: tâches de mise à jour, tâches de copie de sauvegarde et tâches d'envoi de rapports.

> Les tâches pour une sélection d'ordinateurs ne sont exécutées que sur les ordinateurs faisant partie de la sélection. La tâche d'installation à distance définie pour les ordinateurs d'un groupe ne sera pas appliquée aux nouveaux ordinateurs clients qui seraient ajoutés à ce groupe. Il faudra donc créer une nouvelle tâche ou modifier comme il se doit les paramètres de la tâche existante.

Pour créer une tâche locale, procédez comme suit:

1. Ouvrez la fenêtre des propriétés du poste client (cf. section "Administration de l'application" à la page 125) sous l'onglet **Tâches** (cf. ill. ci-dessus).
2. Cliquez sur le bouton **Ajouter**. L'Assistant de création d'une tâche s'ouvre (cf. page 144). Suivez les instructions afin de créer une tâche pour le poste client.

Pour créer une tâche de groupe, procédez comme suit:

1. Lancez la console d'administration Kaspersky Administration Kit.
2. Déployez le nœud **Serveur d'administration**.
3. Sélectionnez, dans le dossier **Ordinateurs administrés**, le dossier portant le nom du groupe d'ordinateurs pour lesquels vous souhaitez créer une tâche, puis choisissez le sous-dossier **Tâches de groupe**.
4. Cliquez sur le lien **Créer une tâche** dans le volet des tâches pour ouvrir l'Assistant de création d'une tâche. Suivez les instructions pour créer la tâche de groupe. Pour de plus amples informations sur la création des tâches de groupe, référez-vous au Manuel de référence de Kaspersky Administration Kit.

Pour créer une tâche destinée à une sélection d'ordinateurs (tâche Kaspersky Administration Kit), procédez comme suit:

1. Lancez la Console d'administration de Kaspersky Administration Kit.
2. Sélectionnez le dossier **Tâches pour les sélections d'ordinateurs** (**Tâches de Kaspersky Administration Kit**).
3. Cliquez sur le lien **Créer une tâche** dans le volet des tâches pour ouvrir l'Assistant de création d'une tâche. Suivez les instructions pour créer la tâche pour la sélection d'ordinateurs ou la tâche de Kaspersky Administration Kit. Pour de plus amples informations sur la création des tâches de Kaspersky Administration Kit

ou des tâches pour la sélection d'ordinateurs, référez-vous au Manuel de référence de Kaspersky Administration Kit.

ASSISTANT DE CREATION D'UNE TACHE

Vous pouvez créer des tâches pour les applications de Kaspersky Lab installées sur un poste client distinct à l'aide de l'Assistant de création d'une tâche.

L'Assistant se présente sous la forme d'une succession de fenêtre (étapes) entre lesquelles vous pouvez naviguer à l'aide des boutons **Précédent** et **Suivant**. Vous pouvez arrêter l'Assistant en cliquant sur **Terminer**. Pour arrêter l'Assistant à n'importe quelle étape, cliquez sur **Annuler**.

Pour ouvrir l'Assistant de création d'une tâche, procédez comme suit :

1. Ouvrez la fenêtre des propriétés du poste client (cf. section "Administration de l'application" à la page 125) sous l'onglet **Tâches**.

2. Cliquez sur le bouton **Ajouter**.

ETAPE 1. SAISIE DES DONNEES GENERALES SUR LA TACHE

Dans le champ **Nom** de la de la fenêtre **Nom de la tâche**, saisissez le nom de la tâche créée.

ETAPE 2. SELECTION DE L'APPLICATION ET DU TYPE DE TACHE

Dans la fenêtre **Type de tâche**, sélectionnez l'application de Kaspersky Lab pour laquelle la tâche est créée, par exemple : **Kaspersky Endpoint Security 8 for Mac** ou **Agent d'administration**, puis le type de tâche à créer. Kaspersky Endpoint Security accepte les types de tâche suivants :

- **Mise à jour** – tâche permettant de télécharger et d'installer des mises à jour pour l'application.
- **Annulation de la mise à jour** – tâche permettant d'annuler la dernière mise à jour de l'application.
- **Analyse** – tâche permettant de rechercher des virus dans les zones spécifiées par l'utilisateur.
- **Installation du fichier clé** : tâche d'installation du fichier clé de la nouvelle licence.

L'Agent d'administration accepte la création de la tâche **Modification du Serveur d'administration**[18].

ETAPE 3. CONFIGURATION DES PARAMETRES DU TYPE DE TACHE SELECTIONNE

Selon le type de tâche sélectionné lors de l'étape précédente, le contenu de la fenêtre des paramètres varie.

Analyse

Réalisez les opérations suivantes dans la fenêtre **Analyse** :

1. Composez la liste des objets à analyser pour la tâche d'analyse. Vous pouvez ajouter des objets à la liste ou en supprimer, le cas échéant. Cliquez sur le bouton **Suivant** pour continuer la configuration.

2. Indiquez l'action qui sera exécutée par Kaspersky Endpoint Security lors de la découverte d'un objet infecté ou potentiellement infecté.

[18] Lisez attentivement l'aide de Kaspersky Administration Kit.

Mise à jour

Pour la tâche de mise à jour des bases antivirus et des modules de l'application, il faut saisir dans la fenêtre **Mise à jour** la source d'où les mises à jour seront téléchargées. La mise à jour est réalisée par défaut depuis le serveur d'administration et depuis les serveurs de mises à jour de Kaspersky Lab. Modifiez la liste des sources de mises à jour, s'il est nécessaire.

Remise à l'état antérieur de la mise à jour

Une tâche d'annulation de mises à jour ne présente aucun paramètre spécifique.

Installation du fichier clé

Dans la fenêtre **Gestion des licences**, cliquez sur le bouton **Parcourir** et dans la fenêtre standard qui s'ouvre, saisissez le chemin d'accès au fichier clé. Si le fichier clé est ajouté en tant que fichier clé pour une licence complémentaire, cochez la case **Ajouter en tant que fichier clé de réserve**. Une licence complémentaire devient active lorsque la clé active arrive à échéance.

Les informations relatives au fichier clé installé (numéro de la clé, son type, date de fin de validité) sont présentées en dessous.

Changement du Serveur d'administration.

Dans la fenêtre **Paramètres**, indiquez les paramètres que l'Agent d'administration, installé sur les postes clients, va utiliser pour la connexion au nouveau Serveur d'administration.[19]

ETAPE 4. CONFIGURATION DE LA PROGRAMMATION

Dans la fenêtre **Planification de l'exécution de la tâche**, sélectionnez le mode de lancement de la tâche : manuel ou selon un horaire défini.

Pour ce faire, sélectionnez dans la liste déroulante la fréquence de lancement de la tâche et indiquez l'heure de lancement de la tâche.

ETAPE 5. FIN DE LA CREATION D'UNE TACHE

La dernière fenêtre de l'Assistant vous informe de la réussite de la création de la tâche. Cliquez sur le bouton **Terminer** pour quitter l'Assistant.

CONFIGURATION DES TACHES

La configuration des paramètres d'une tâche de Kaspersky Endpoint Security via l'interface de Kaspersky Administration Kit est identique à la configuration via l'interface locale de l'application. La seule exception se situe au niveau des paramètres qui sont configurés individuellement pour chaque utilisateur, ainsi que les paramètres propres à Kaspersky Administration Kit, par exemple les paramètres qui autorisent (ou interdisent) à l'utilisateur d'administrer la tâche locale d'analyse.

Si une stratégie, interdisant la modification de certains paramètres a été créée, la modification de la configuration de la tâche sera impossible.

Tous les onglets de la fenêtre des propriétés de la tâche, excepté celui intitulé **Paramètres** sont des onglets standards de Kaspersky Administration Kit[20]. L'onglet **Paramètres** contient les paramètres spécifiques de Kaspersky Endpoint Security qui varient en fonction du type de tâche sélectionné.

[19] Lisez attentivement l'aide de Kaspersky Administration Kit.
[20] Lisez attentivement l'aide de Kaspersky Administration Kit.

Pour visualiser ou modifier une tâche locale, procédez comme suit :

1. Ouvrez la fenêtre des propriétés du poste client (cf. section "Administration de l'application" à la page 125) sous l'onglet **Tâches**.

2. Sélectionnez la tâche souhaitée dans la liste et cliquez sur le bouton **Propriétés**. La fenêtre des propriétés de la tâche s'ouvre (cf. ill. ci-après).

Pour visualiser ou modifier les paramètres des tâches de groupe, procédez comme suit :

1. Lancez la Console d'administration de Kaspersky Administration Kit.

2. Déployez le nœud **Serveur d'administration**.

3. Dans le dossier **Ordinateurs administrés**, sélectionnez le dossier portant le nom du groupe requis, puis sélectionnez le sous-dossiers **Tâches de groupe** à l'intérieur de celui-ci.

4. Sélectionnez la tâche souhaitée dans l'arborescence de la console pour visualiser ou modifier ses propriétés.

   Le panneau des tâches présente quelques informations sur la tâche ainsi que des liens permettant de gérer son exécution et de modifier ses paramètres. Pour de plus amples informations sur les tâches de groupe, référez-vous au Manuel de référence de Kaspersky Administration Kit.

Pour passer à la consultation et à la configuration des paramètres des tâches pour une sélection d'ordinateurs (tâches de Kaspersky Administration Kit), procédez comme suit :

1. Lancez la Console d'administration de Kaspersky Administration Kit.

2. Sélectionnez le dossier **Tâches pour les sélections d'ordinateurs** (**Tâches de Kaspersky Administration Kit**).

3. Sélectionnez la tâche souhaitée dans l'arborescence de la console pour visualiser ou modifier ses propriétés.

   Le panneau des tâches présente quelques informations sur la tâche ainsi que des liens permettant de gérer son exécution et de modifier ses paramètres. Pour de plus amples informations sur les tâches Kaspersky Administration Kit et tâches destinées à une sélection d'ordinateurs, référez-vous au Manuel de référence de Kaspersky Administration Kit.

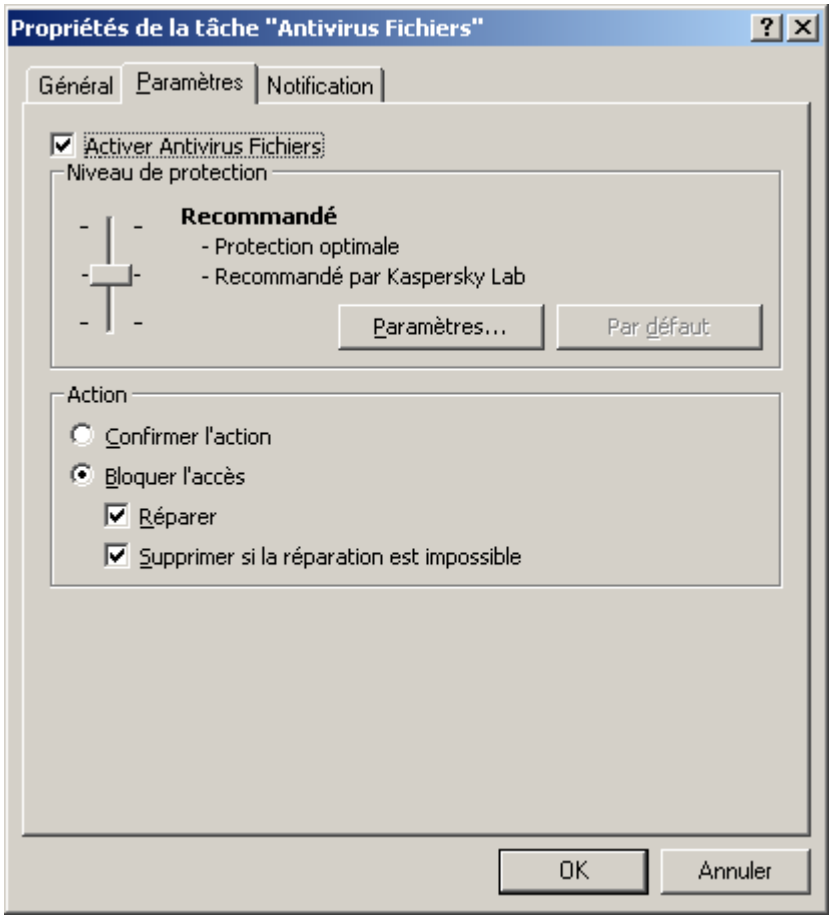


Illustration 69. Fenêtre Propriétés de la tâche "Antivirus Fichiers". Onglet Paramètres

CONFIGURATION DE L'ANTIVIRUS FICHIERS

Pour consulter et modifier les paramètres de l'Antivirus Fichiers, procédez comme suit :

1. Ouvrez la fenêtre des propriétés du poste client (cf. section "Administration de l'application" à la page 125) sous l'onglet **Tâches**.

2. Sélectionnez la tâche **Antivirus Fichiers** dans la liste, puis cliquez sur le bouton **Propriétés**.

3. Dans la fenêtre des propriétés de la tâche qui s'ouvre, configurez les paramètres suivants sous l'onglet **Paramètres** (cf. ill. ci-dessus) :

   - Activez ou désactivez l'Antivirus Fichiers sur l'ordinateur distant via la case correspondante.

   - Dans le groupe **Niveau de protection**, sélectionnez le niveau de protection du système de fichiers de l'ordinateur distant en déplaçant le curseur ou en cliquant sur le bouton **Paramètres** pour modifier les paramètres du niveau actuel de la protection. Dans la fenêtre **Configuration: Antivirus Fichiers** qui s'ouvre (cf. ill. ci-après), modifiez les paramètres de la protection des fichiers :

     - Sous l'onglet **Général**, indiquez les formats d'objet qui seront analysés par Kaspersky Endpoint Security à l'ouverture, à l'exécution et à l'enregistrement (groupe **Types de fichiers**), configurez la performance de l'analyse et sélectionnez la technologie d'analyse (groupe **Optimisation**), sélectionnez les objets composés qu'il faut analyser et définissez les restrictions sur l'analyse des objets volumineux (groupe **Objets composés**) ;

     - Sous l'onglet **Zone de protection**, définissez les disques ou les répertoires que l'Antivirus Fichiers doit contrôler. La protection est active par défaut pour tous les objets se trouvant sur des disques fixes, des

supports amovibles et les unités réseau connectées à l'ordinateur. Vous pouvez ajouter un objet à analyser, modifier un objet de la liste, désactiver temporairement l'analyse de l'objet ou le supprimer ;

- Sous l'onglet **Avancé**, sélectionnez le mode de fonctionnement de l'Antivirus Fichiers (groupe **Mode d'analyse**), activez la suspension programmée de l'Antivirus Fichiers et configurez la programmation (groupe **Suspension de la tâche**), configurez l'utilisation de l'analyseur heuristique par l'Antivirus Fichier (groupe **Analyseur heuristique**).

- Dans le groupe **Action**, sélectionnez l'action que l'Antivirus Fichiers va exécuter en cas de découverte d'un objet infecté ou potentiellement infecté.

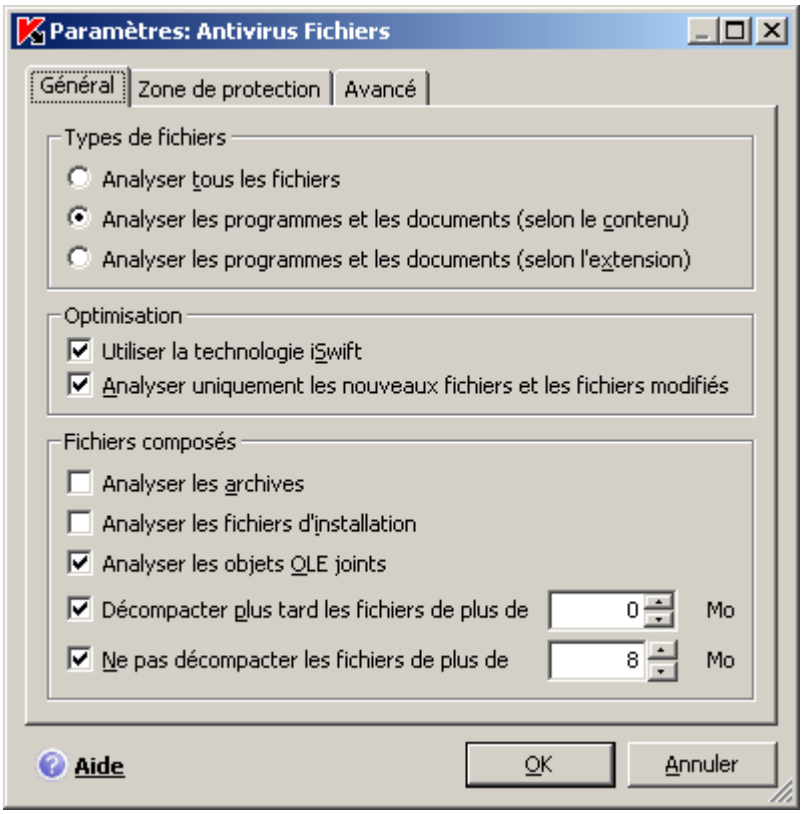


Illustration 70. Fenêtre Configuration: Antivirus Fichiers

CONFIGURATION DES TACHES LIEES A LA RECHERCHE DE VIRUS

Pour consulter et modifier les paramètres de la tâche d'analyse, procédez comme suit :

1. Ouvrez la fenêtre des propriétés du poste client (cf. section "Administration de l'application" à la page 125) sous l'onglet **Tâches**.

2. Sélectionnez la tâche d'analyse dans la liste, puis cliquez sur le bouton **Propriétés**.

3. Dans la fenêtre des propriétés de la tâche qui s'ouvre, configurez les paramètres suivants sous l'onglet **Paramètres** (cf. ill. ci-dessous) :

   - Dans le groupe **Niveau de protection**, sélectionnez le niveau auquel la tâche d'analyse va être exécutée sur l'ordinateur distant en déplaçant le curseur sur l'échelle ou cliquez sur le bouton **Paramètres** pour modifier les paramètres du niveau de protection actuel. Dans la fenêtre qui s'ouvre (cf. ill. ci-après), modifiez les paramètres du niveau de protection :

     - Sous l'onglet **Général**, désignez le format des fichiers qui seront analysés par Kaspersky Endpoint Security dans le cadre de la tâche d'analyse (groupe **Types de fichiers**), configurez les performances

de l'analyse (groupe **Optimisation**), sélectionnez les fichiers composés à analyser (groupe **Fichiers composés**) ;

- Sous l'onglet **Avancé**, configurez l'utilisation des technologies d'analyse et la possibilité de restaurer la tâche arrêtée (groupe **Paramètres complémentaires**), ainsi que l'utilisation de l'analyseur heuristique dans les tâches de recherche de virus (groupe **Analyseur heuristique**).

- Dans le groupe **Action**, sélectionnez l'action que Kaspersky Endpoint Security va exécuter en cas de découverte d'un objet infecté ou potentiellement infecté ;

- Dans le groupe **Objets à analyser**, désignez les objets que Kaspersky Endpoint Security va analyser dans le cadre de la tâche. Vous pouvez ajouter un objet à analyser dans la liste, désactiver temporairement l'analyse de l'objet ou le supprimer.

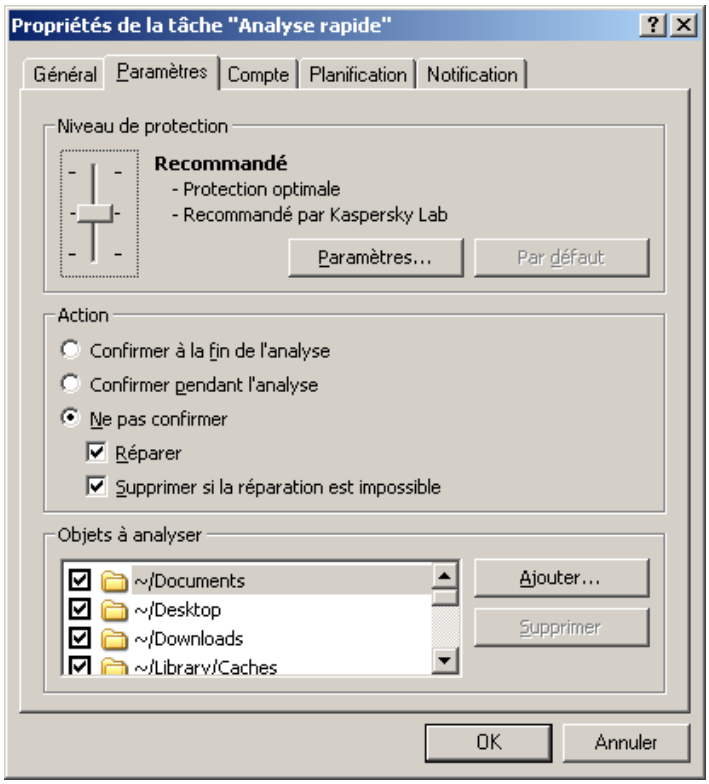


Illustration 71. Fenêtre Propriétés de la tâche "Analyse express". Onglet Paramètres

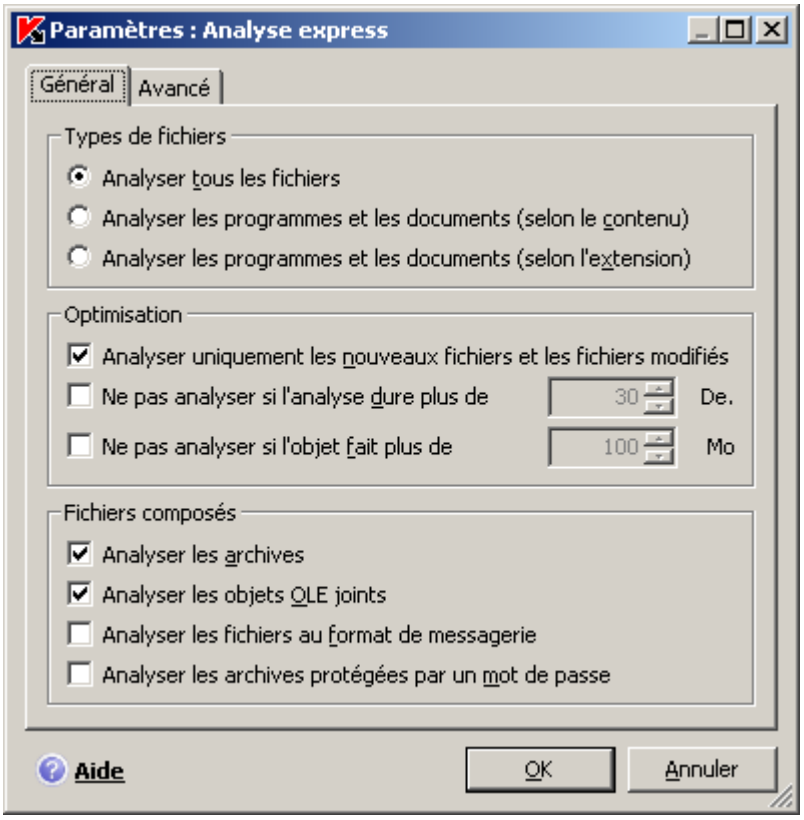


Illustration 72. Fenêtre Configuration : Analyse express

CONFIGURATION DE LA TACHE DE MISE A JOUR

Pour consulter et modifier les paramètres de la tâche de mise à jour, procédez comme suit :

1. Ouvrez la fenêtre des propriétés du poste client (cf. section "Administration de l'application" à la page 125) sous l'onglet **Tâches**.

2. Sélectionnez la tâche de mise à jour dans la liste et cliquez sur le bouton **Propriétés**.

3. Dans la fenêtre des propriétés de la tâche qui s'ouvre, configurez les paramètres suivants sous l'onglet **Paramètres** (cf. ill. ci-dessous) :

   - Dans le groupe **Paramètres de la mise à jour**, indiquez s'il faut copier et installer non seulement les bases antivirus, mais aussi les modules de l'application lors de la mise à jour de l'application. Pour ce faire, cochez la case **Mettre à jour les modules de l'application**. Vous pouvez également sélectionner la source des mises à jour et configurer la copie des mises à jour récupérées dans une source locale. Pour ce faire, cliquez sur **Paramètres**. La fenêtre **Configuration de la mise à jour** s'ouvre (cf. ill. ci-après). Elle permet de réaliser les opérations suivantes :

     - Sous l'onglet **Source de mise à jour**, désigner la source d'où seront téléchargées les mises à jour des bases antivirus et des modules de l'application. La mise à jour est réalisée par défaut depuis le serveur d'administration et depuis les serveurs de mises à jour de Kaspersky Lab. Vous pouvez ajouter une nouvelle source de mises à jour dans la liste, modifier une source de mises à jour, désactiver temporairement la récupération des mises à jour depuis la source et supprimer une source de la liste ;

     - sous l'onglet **Avancé**, activer le service de copie des mises à jour dans la source locale et indiquer le chemin d'accès au dossier partagé où seront conservées les mises à jour obtenues.

   - Dans le groupe **Action après la mise à jour**, indiquez si Kaspersky Endpoint Security doit lancer l'analyse des objets placés en quarantaine après la mise à jour de l'application.

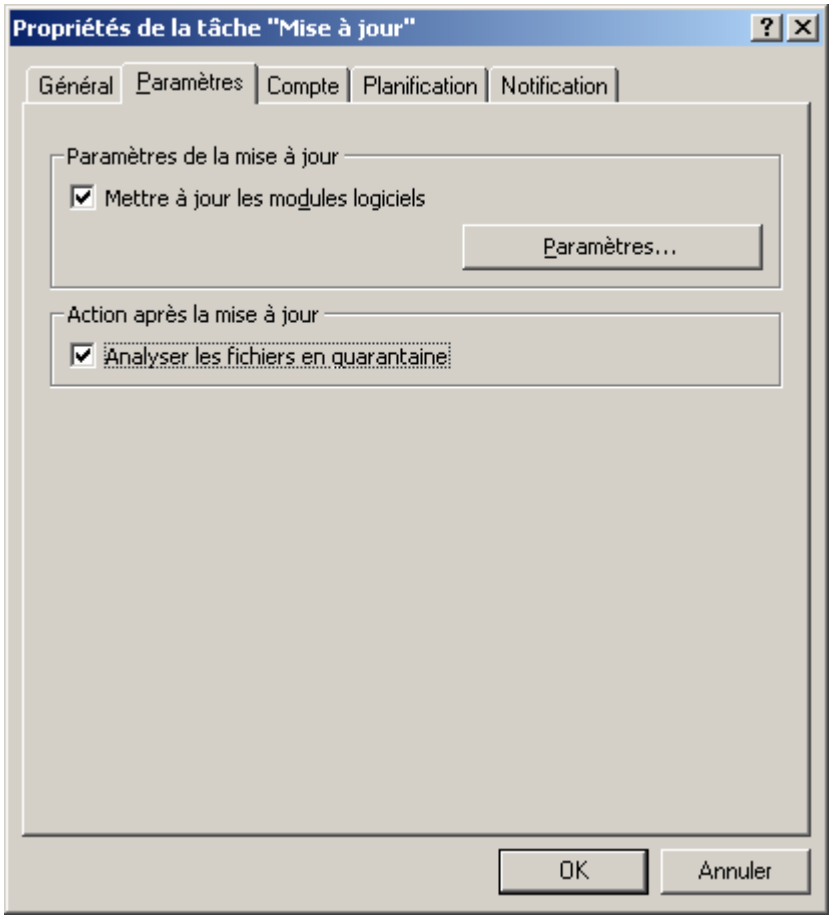


Illustration 73. Fenêtre Propriétés de la tâche "Mise à jour". Onglet Paramètres

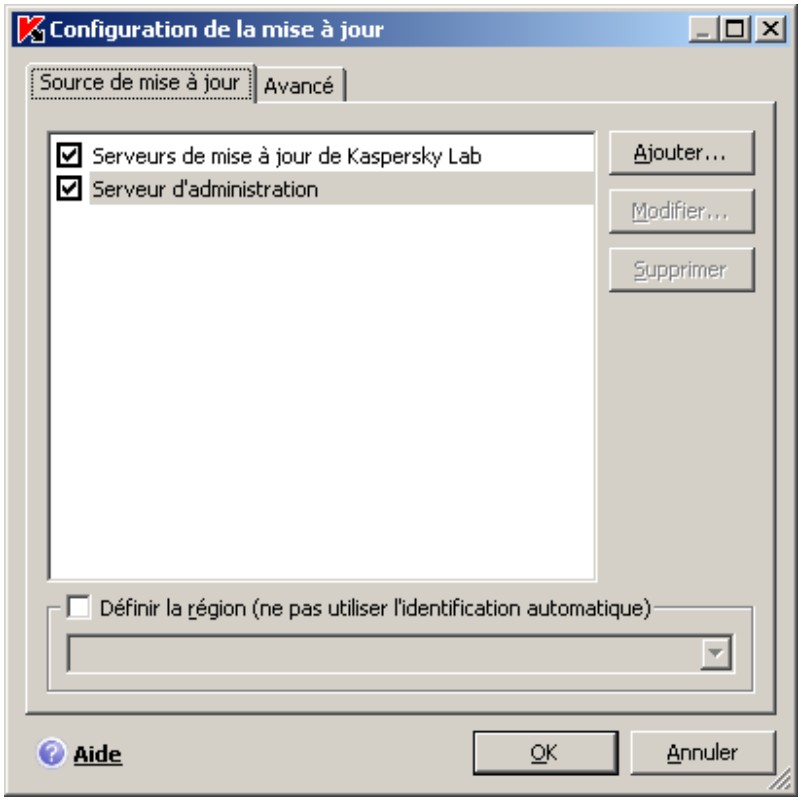


Illustration 74. Fenêtre Configuration de la mise à jour

ADMINISTRATION DES STRATEGIES

La définition de stratégie est un moyen permettant d'appliquer une configuration des tâches et de l'application identique à tous les ordinateurs clients faisant partie d'un groupe d'administration.

Cette section fournit des informations sur la création et la configuration de stratégies pour Kaspersky Endpoint Security[21].

Pendant la création et la configuration de la stratégie, vous pouvez empêcher complètement ou partiellement la modification des paramètres de groupes imbriqués, de tâche ou d'application. Pour ce faire, cliquez sur  . Pour les paramètres qui ne peuvent pas être modifiés, l'icône doit ressembler à  .

Les stratégies peuvent être associées aux actions suivantes :

- Créer des stratégies ;
- Configurer les paramètres de stratégies ;
- Copier et transférer les stratégies d'un groupe à un autre et supprimer les stratégies à l'aide du menu contextuel ;
- Importer et exporter les paramètres des stratégies.

Pour ouvrir la liste des stratégies concernant Kaspersky Endpoint Security, procédez comme suit :

1. Lancez la Console d'administration de Kaspersky Administration Kit.
2. Déployez le nœud **Serveur d'administration**.
3. Dans le dossier **Ordinateurs administrés** sélectionnez le dossier avec le nom du groupe, contenant le poste client.
4. Dans le groupe sélectionné, choisissez le sous-dossier **Stratégies**. L'arborescence de la console présentera toutes les stratégies créées pour ce groupe.

DANS CETTE SECTION

CREATION D'UNE STRATEGIE

Lorsque vous gérez Kaspersky Endpoint Security via Kaspersky Administration Kit, vous avez la possibilité de créer des stratégies pour l'application.

Pour créer une stratégie, procédez comme suit :

1. Lancez la Console d'administration de Kaspersky Administration Kit.
2. Déployez le nœud **Serveur d'administration**.

[21] Lisez attentivement le Guide de l'administrateur de Kaspersky Administration Kit.

3. Dans le dossier **Ordinateurs administrés** sélectionnez le dossier avec le nom du groupe, contenant le poste client.

4. Dans le groupe sélectionné, choisissez le sous-dossier **Stratégies**. L'arborescence de la console présentera toutes les stratégies créées pour ce groupe.

5. Cliquez sur le lien **Créer une stratégie** dans le volet des tâches pour lancer l'Assistant de création d'une stratégie (à la page 153). Suivez les instructions pour créer une stratégie pour Kaspersky Endpoint Security.

ASSISTANT DE CREATION DE STRATEGIE

Vous pouvez créer des stratégies qui définissent des paramètres uniques pour l'application et les tâches des postes clients appartenant à un groupe d'administration à l'aide de l'Assistant de création de stratégie.

L'Assistant se présente sous la forme d'une succession de fenêtre (étapes) entre lesquelles vous pouvez naviguer à l'aide des boutons **Précédent** et **Suivant**. Vous pouvez arrêter l'Assistant en cliquant sur **Terminer**. Pour arrêter l'Assistant à n'importe quelle étape, cliquez sur **Annuler**.

ETAPE 1. SAISIE DES DONNEES GENERALES SUR LA STRATEGIE

Dans le champ **Nom** de la de la fenêtre **Nom de la stratégie**, saisissez le nom de la tâche créée.

ETAPE 2. SELECTION D'UNE APPLICATION

Dans la fenêtre **Application**, sélectionnez l'application de "Kaspersky Lab" pour laquelle la stratégie est créée : **Kaspersky Endpoint Security 8 for Mac**.

ETAPE 3. SELECTION DE L'ETAT DE LA STRATEGIE

Dans la fenêtre **Création d'une stratégie**, sélectionnez l'état de la stratégie[22] qui lui sera attribué après la création. Les états suivants peuvent être attribués à la stratégie :

- stratégie active ;
- stratégie inactive.
- stratégie pour utilisateur nomade.

Plusieurs stratégies peuvent être créées dans le groupe des ordinateurs pour une application mais il ne peut y avoir qu'une seule stratégie active.

ETAPE 4. CONFIGURATION DES PARAMETRES DE PROTECTION

Dans la fenêtre **Protection**, activez ou désactivez les composants de la protection à utiliser dans la stratégie.

Tous les composants de la protection sont activés par défaut. Pour désactiver un composant quelconque, désélectionnez la case qui se trouve en regard de son nom. Si vous souhaitez procéder à une configuration détaillée d'un composant de la protection, sélectionnez-le dans la liste et cliquez sur **Paramètres**.

[22] Lisez attentivement l'aide de Kaspersky Administration Kit.

VOIR EGALEMENT

ETAPE 5. CONFIGURATION DES PARAMETRES DE LA RECHERCHE DE VIRUS

Dans la fenêtre **Analyse**, configurez les paramètres par défaut selon lesquels la tâche d'analyse sera exécutée.

VOIR EGALEMENT

ETAPE 6. CONFIGURATION DE LA MISE A JOUR

Dans la fenêtre **Mise à jour**, indiquez les paramètres par défaut selon lesquels les tâches de mise à jour de l'application seront exécutées.

VOIR EGALEMENT

ETAPE 7. CONFIGURATION DU RESEAU

Dans la fenêtre **Configuration du réseau**, indiquez les paramètres de connexion au serveur proxy.

Si vous ne souhaitez pas utiliser le serveur proxy pour vous connecter à Internet pendant la mise à jour des bases antivirus et des modules de l'application, décochez la case **Utiliser le serveur proxy**.

Si la case est cochée, il est possible de configurer les paramètres suivants de connexion au serveur proxy :

- utilisation par Kaspersky Endpoint Security des paramètres du serveur proxy, définis dans les paramètres système de Mac OS X ou les adresses et les ports de serveur proxy définis par l'utilisateur ;
- possibilité d'utiliser le serveur proxy lors de la mise à jour depuis un dossier local ou réseau ;
- paramètres d'authentification pour la connexion au serveur proxy.

VOIR EGALEMENT

ETAPE 8. CONFIGURATION DES PARAMETRES D'INTERACTION AVEC L'UTILISATEUR

Dans la fenêtre **Interaction avec l'utilisateur**, indiquez la forme que prendra l'interaction de l'utilisateur avec Kaspersky Endpoint Security sur l'ordinateur distant.

Vous pouvez configurer la réception des notifications par l'utilisateur et modifier l'affichage de l'icône de Kaspersky Endpoint Security sur l'ordinateur distant.

VOIR EGALEMENT

ETAPE 9. CONFIGURATION DES RAPPORTS ET DES BANQUES

Dans la fenêtre **Rapports et Stockages**, indiquez les paramètres de composition et de conservation des rapports ainsi que les paramètres de conservation des objets dans la quarantaine et la sauvegarde.

VOIR EGALEMENT

ETAPE 10. FIN DE LA CREATION D'UNE STRATEGIE

La dernière fenêtre de l'Assistant vous informe de la réussite de la création de la stratégie. Cliquez sur le bouton **Terminer** pour quitter l'Assistant.

La stratégie créée apparaît dans l'arborescence de la console dans le dossier **Stratégies** du groupe d'administration correspondant.

Vous pouvez ensuite modifier les paramètres de la stratégie créée et empêcher leur modification à l'aide des boutons  et  pour chaque groupe de paramètres. Si la case  est cochée, alors l'utilisateur sur le poste client ne peut pas modifier les paramètres. Les paramètres, marqués par l'icône  , peuvent être modifiés par l'utilisateur.

La stratégie sera appliquée aux postes clients après la première synchronisation des clients avec le Serveur d'administration.

CONFIGURATION DE LA STRATEGIE

Kaspersky Administration Kit permet de modifier la stratégie créée et d'interdire la modification des paramètres dans les stratégies des sous-groupes, des paramètres de l'application et des paramètres des tâches. Les paramètres de la stratégie peuvent être modifiés dans la fenêtre des propriétés de la stratégie sous l'onglet **Paramètres** (cf. ill. ci-après).

Tous les onglets de la fenêtre des propriétés de la stratégie, à l'exception de l'onglet **Paramètres**, sont standards pour l'application Kaspersky Administration Kit[23].

[23] Lisez attentivement le Guide de l'administrateur de Kaspersky Administration Kit.

Les paramètres de la stratégie pour Kaspersky Endpoint Security reprennent les paramètres de l'application (cf. section "Configuration des paramètres de l'application" à la page 128) et les paramètres des tâches (cf. section "Configuration des paramètres d'une tâche" à la page 145).

Pour visualiser ou modifier les paramètres de la stratégie, procédez comme suit:

1. Lancez la Console d'administration de Kaspersky Administration Kit.
2. Déployez le nœud **Serveur d'administration**.
3. Dans le dossier **Ordinateurs administrés** sélectionnez le dossier avec le nom du groupe, contenant le poste client.
4. Dans le groupe sélectionné, choisissez le sous-dossier **Stratégies**. L'arborescence de la console présentera toutes les stratégies créées pour ce groupe.
5. Sélectionnez la stratégie souhaitée dans l'arborescence de la console pour visualiser ou modifier ses propriétés.

   Le panneau des tâches présente quelques informations sur la stratégie ainsi que des liens permettant de gérer son état et de modifier ses paramètres.

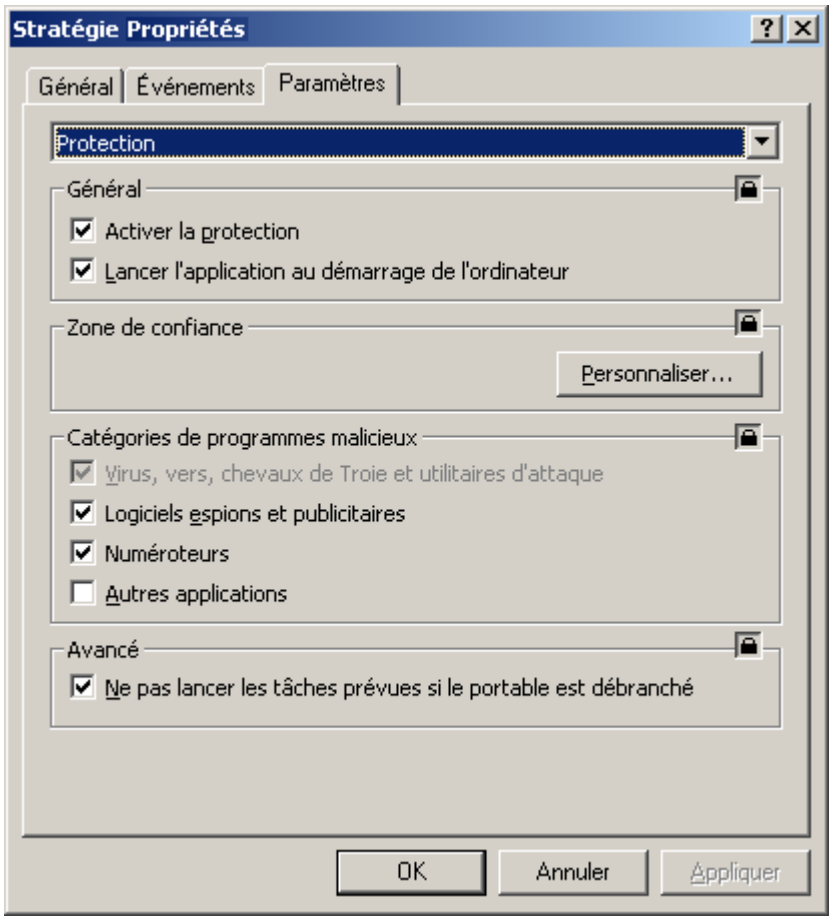


Illustration 75. Fenêtre des propriétés de la stratégie. Onglet Paramètres

CONTACTER LE SERVICE D'ASSISTANCE TECHNIQUE

Si vous avez acheté Kaspersky Endpoint Security, vous pouvez obtenir des renseignements sur cette application auprès des opérateurs du service d'assistance technique, par téléphone ou via Internet. Les experts du service d'assistance technique répondront à vos questions sur l'installation et l'utilisation de l'application et, en cas d'infection de votre ordinateur, ils vous aideront à éliminer les conséquences de l'action des programmes malveillants.

Pour consulter les informations sur les moyens d'obtenir une assistance pour Kaspersky Endpoint Security,

ouvrez la fenêtre principale de l'application (à la page 33) et cliquez sur le bouton  .

Avant de contacter le Service d'assistance technique, veuillez prendre connaissance des règles d'assistance (http://support.kaspersky.com/fr/support/rules).

Si des problèmes surviennent pendant votre utilisation de Kaspersky Endpoint Security, assurez-vous que la solution n'est pas proposée dans cette aide, dans la documentation, dans la Banque de solutions du site Web de l'Assistance technique de Kaspersky Lab ou dans le Forum des utilisateurs (cf. section "Sources d'informations complémentaires" à la page 15). Si vous n'avez pas trouvé la solution à votre problème, nous vous conseillons de contacter le Service d'assistance technique de Kaspersky Lab.

N'oubliez pas que pour bénéficier des services d'assistance technique, vous devez être un utilisateur enregistré avec une version commerciale de Kaspersky Endpoint Security. L'assistance des utilisateurs de versions d'évaluation n'est pas prévue.

Si Kaspersky Endpoint Security est activé à l'aide du code d'activation, l'enregistrement de l'utilisateurs sera réalisé par l'Assistant d'activation (cf. section "Activation de Kaspersky Endpoint Security" à la page 28).

Si vous activez Kaspersky Endpoint Security à l'aide d'un fichier clé, réalisez la procédure d'enregistrement directement sur le site Web du Service d'assistance technique (http://support.kaspersky.com/fr/).

Le numéro de client et le mot de passe obtenus après l'enregistrement sont indispensables pour accéder à votre Espace personnel : il s'agit d'un espace réservé au client sur le site Web du Service d'assistance technique. L'Espace personnel permet de réaliser les opérations suivantes :

- envoyer des requêtes au service d'assistance sans devoir saisir les données d'enregistrement ;
- communiquer avec le service d'assistance technique sans envoyer de courrier électronique ;
- suivre l'état de vos demandes en temps réel ;
- consulter l'historique complet de vos contacts avec le service d'assistance ;
- obtenir une copie de sauvegarde du fichier de licence.

Requête électronique adressée au Service d'assistance technique

Pour contacter le service d'assistance technique, ouvrez le formulaire en ligne du système de traitement des requêtes des clients baptisé Helpdesk (https://my.kaspersky.com/fr/support). Sur la page Web du Service d'assistance technique qui s'ouvre, accédez à votre espace personnel et remplissez le formulaire en ligne.

Vous pouvez envoyer vos messages en anglais et en français.

Pour envoyer une requête par voie électronique, vous devez indiquer le **code client** obtenu lors de l'enregistrement sur le site Web du Service d'assistance technique, ainsi que le **mot de passe**.

Décrivez le plus exactement possible le problème que vous rencontrez sur le formulaire en ligne. Dans les champs obligatoires, indiquez :

- **Le type de requête**. Sélectionnez le sujet qui correspond le mieux au problème rencontré, par exemple, "Problème d'installation/de suppression du logiciel" ou "Problème de recherche/de suppression de virus". Si vous ne trouvez pas de sujet se rapprochant le plus de votre situation, choisissez "Question générale".
- **Nom et numéro de 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 obtenus lors de l'enregistrement sur le site du service d'assistance technique.
- **Adresse de messagerie**. Il s'agit de l'adresse à laquelle les experts du service d'assistance technique enverront la réponse à votre question.

L'opérateur du Service d'assistance technique vous enverra sa réponse à l'adresse électronique que vous avez indiquée dans votre Espace personnel.

Assistance technique par téléphone

Si le problème est urgent, vous pouvez contacter le service d'assistance technique dans votre ville. Si vous contactez l'assistance technique russe (http://support.kaspersky.ru/support/support_local) ou internationale (http://support.kaspersky.com/fr/support/international), veuillez fournir les informations (http://support.kaspersky.com/fr/support/details) sur votre ordinateur et l'application antivirus installée. Cela permettra à nos experts de vous venir en aide le plus vite possible.

Création d'un fichier de trace

Des échecs peuvent survenir pendant l'utilisation de Kaspersky Endpoint Security. Ils sont provoqués dans la majorité des cas par un conflit entre Kaspersky Endpoint Security et une autre application installée sur votre ordinateur. Afin de résoudre ce problème, les experts du Service d'assistance technique de Kaspersky Lab pourraient vous demander de créer un fichier de traçage.

Pour créer un fichier de trace, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'app **Rapports**.
2. Dans le groupe **Traçage**, cochez la case **Activer le traçage**.
3. Relancez Kaspersky Endpoint Security pour lancer le processus de traçage.

Utilisez cette fenêtre uniquement sous le pilotage du spécialiste du Service d'assistance technique de Kaspersky Lab.

Les fichiers de trace peuvent occuper beaucoup d'espace sur le disque. Quand vous avez fini d'utiliser les fichiers de trace, il est conseillé de suspendre leur création en décochant la case **Activer le traçage** sous l'onglet **Rapports** de la fenêtre de configuration de l'application. Après cette opération relancez l'application Kaspersky Endpoint Security.

APPLICATIONS

Cette section du manuel contient l'information d'aide sur les formats des fichiers analysés et des masques d'exclusion autorisés, utilisés lors de la configuration des paramètres de Kaspersky Endpoint Security.

DANS CETTE SECTION

LISTE DES OBJETS ANALYSES EN FONCTION DE L'EXTENSION

Si lors de la configuration de l'Antivirus Fichiers (cf. section "Définition du type de fichiers analysés" à la page 61) ou des tâches liées à la recherche de virus (cf. section "Définition du type d'objet analysé" à la page 76), vous avez sélectionné l'option **Analyser les programmes et les documents (selon l'extension)**, alors les objets avec les extensions citées ci-dessous seront analysés sur la présence de virus :

com : fichier exécutable d'un programme Microsoft Windows dont la taille est inférieure à 64 Ko ;

exe : fichier exécutable, archive auto extractible Microsoft Windows ;

sys : fichier système Microsoft Windows ;

prg : texte du programme dBase, Clipper ou Microsoft Visual FoxPro, programme de la suite WAVmaker ;

bin : fichier binaire Microsoft Windows ;

bat : fichier de tâche en lot Microsoft Windows ;

cmd : fichier de commande Microsoft Windows NT (semblable au fichier bat pour DOS), OS/2 ;

dpl : bibliothèque Borland Delphi compactée ;

dll : bibliothèque de chargement dynamique Microsoft Windows ;

scr : fichier d'économiseur d'écran de Microsoft Windows ;

cpl : module du panneau de configuration de Microsoft Windows ;

ocx : objet Microsoft OLE (Object Linking and Embedding) ;

tsp : programme Microsoft Windows, qui fonctionne en mode de partage du temps ;

drv : pilote d'un périphérique quelconque de Microsoft Windows ;

vxd : pilote d'un périphérique virtuel Microsoft Windows ;

pif : fichier Microsoft Windows avec des informations sur un programme ;

lnk : fichier lien dans Microsoft Windows ;

reg : fichier d'enregistrement des clés de la base de registres de Microsoft Windows ;

ini : fichier d'initialisation de Microsoft Windows ;

cla : classe Java ;

vbs : script Visual Basic ;

vbe : extension vidéo BIOS ;

js, jse : texte source JavaScript ;

htm : document hypertexte ;

htt : préparation hypertexte de Microsoft Windows ;

hta : programme hypertexte pour Microsoft Internet Explorer ;

asp : script Active Server Pages ;

chm : fichier HTML compilé ;

pht : fichier HTML avec scripts PHP intégrés ;

php : script intégré dans les fichiers HTML ;

wsh : fichier Microsoft Windows Script Host ;

wsf : script Microsoft Windows ;

the : fichier du bureau de Microsoft Windows 95 ;

hlp : fichier d'aide au format Win Help ;

eml : message électronique de Microsoft Outlook Express ;

nws : nouveau message électronique de Microsoft Outlook Express ;

msg : message électronique de Microsoft Mail ;

plg : message électronique ;

mbx : extension des messages Microsoft Office Outlook sauvegardés ;

*doc** : document Microsoft Office Word, par exemple : doc – document Microsoft Office Word, docx – document Microsoft Office Word 2007 avec prise en charge de XML, docm – document Microsoft Office Word 2007 avec prise en charge des macros ;

dot :* modèle de document Microsoft Office Word, par exemple : dot – modèle de document Microsoft Office Word, dotx – modèle de document Microsoft Office Word 2007, dotm – modèle de document Microsoft Office Word 2007 avec prise en charge des macros ;

fpm : programme de bases de données, fichier de départ de Microsoft Visual FoxPro ;

rtf : document au format Rich Text Format ;

shs : fragment de Shell Scrap Object Handler ;

dwg : base de données de dessins AutoCAD ;

msi : paquet Microsoft Windows Installer ;

otm : projet VBA pour Microsoft Office Outlook ;

pdf : document Adobe Acrobat ;

swf : objet d'un paquet Shockwave Flash ;

jpg, *jpeg*, *png* : fichier de conservation de données compressées ;

emf : fichier au format Enhanced Metafile. Nouvelle génération de métafichiers du système d'exploitation Microsoft Windows ;

ico : fichier d'icône d'un objet ;

ov? : fichiers exécutable MS DOS ;

*xl** : documents et fichiers Microsoft Office Excel tels que : xla – extension Microsoft Office Excel, xlc – diagramme, xlt – modèle de documents, xlsx – classeur Microsoft Office Excel 2007, xltm – classeur Microsoft Office Excel 2007 avec prise en charge des macros, xlsb – classeur Microsoft Office Excel 2007 au format binaire (pas XML), xltx – modèle Microsoft Office Excel 2007, xlsm – modèle Microsoft Office Excel 2007 avec prise en charge des macros, xlam – complément de Microsoft Office Excel 2007 avec prise en charge des macros ;

*pp** : documents et fichiers Microsoft Office PowerPoint tels que : pps – dia Microsoft Office PowerPoint, ppt – présentation, pptx – présentation Microsoft Office PowerPoint 2007, pptm – présentation Microsoft Office PowerPoint 2007 avec prise en charge de macros, potx – modèle de présentation Microsoft Office PowerPoint 2007, potm – modèle de présentation Microsoft Office PowerPoint 2007 avec prise en charge des macros, ppsx – diaporama Microsoft Office PowerPoint 2007, ppsm – diaporama Microsoft Office PowerPoint 2007 avec prise en charge des macros, ppam – complément de Microsoft Office PowerPoint 2007 avec prise en charge des macros ;

*md** : documents et fichiers Microsoft Office Access tels que : mda : groupe de travail Microsoft Office Access, mdb : base de données, etc. ;

sldx : diaporama Office PowerPoint 2007 ;

sldm – dia de Microsoft Office PowerPoint 2007 avec prise en charge des macros ;

thmx : thème Microsoft Office 2007.

Le format du fichier peut ne pas correspondre au format indiqué par l'extension du fichier.

MASQUES AUTORISES POUR L'EXCLUSION DES FICHIERS

Voici des exemples de masques autorisés que vous pouvez utiliser dans la composition de la liste des fichiers à exclure :

1. Masques sans chemins d'accès aux fichiers :
   - ***.zip** : tous les fichiers portant l'extension zip ;
   - ***.zi?** : tous les fichiers portant l'extension zi?, où ? peut représenter n'importe quel caractère unique ;
   - **test** : tous les fichiers portant le nom test .
2. Masques avec chemins d'accès absolus aux fichiers :
   - **/dir/*** ou **/dir/** : tous les fichiers du répertoire /dir/ ;
   - **/dir/*.zip** : tous les fichiers portant l'extension zip dans le répertoire /dir/ ;

- **/dir/*.zi?** – tous les fichiers portant l'extension zi? dans le répertoire /dir/, où ? peut représenter n'importe quel caractère unique ;
- **/dir/test** : tous les fichiers portant le nom test dans le dossier /dir/ et tous les sous-dossiers.

3. Masques avec chemins d'accès relatifs aux fichiers :
   - **dir/* ou** dir/ : tous les fichiers dans tous les répertoires dir/ ;
   - **dir/*.zip** : tous les fichiers portant l'extension zip dans tous les répertoires dir/ ;
   - **/dir/*.zi?** – tous les fichiers portant l'extension zi? dans tous les répertoires dir/, où ? peut représenter n'importe quel caractère unique ;
   - **dir/test** : tous les dossiers portant le nom test dans tous les dossiers dir/ et leur sous-dossiers.

L'utilisation du masque d'exclusion * est possible uniquement en cas d'indication du type de menace exclue selon le classement de l'Encyclopédie des virus. Dans ce cas, la menace indiquée ne sera pas décelée dans tous les objets. L'utilisation de ces masques sans indication du type de menace revient à désactiver la protection.

MASQUES D'EXCLUSION AUTORISES SELON LE CLASSEMENT DE L'ENCYCLOPEDIE DES VIRUS

Pour ajouter des menaces d'un verdict particulier (conforme au classement de l'encyclopédie des virus) en guise d'exclusion, vous pouvez indiquer :

- Le nom complet de la menace, tel qu'il figure dans l'Encyclopédie des virus à l'adresse www.securelist.com /fr (http://www.securelist.com/fr/) (par exemple, **not-a-virus:RiskWare.RemoteAdmin.RA.311** ou **Flooder.Win32.Fuxx**).
- Le nom de la menace selon un masque, par exemple :
  - **not-a-virus*** : exclut de l'analyse les logiciels licites mais potentiellement dangereux, ainsi que les jokewares ;
  - ***Riskware.*** : exclut de l'analyse tous les types de logiciels présentant un risque potentiel de type Riskware ;
  - ***RemoteAdmin.*** : exclut de l'analyse toutes les versions de logiciel d'administration à distance.

Des exemples de noms de menaces sont fournis dans la fenêtre des rapports sous l'onglet **Détectés**, dans la quarantaine et dans la sauvegarde, ainsi que dans les fenêtres contextuelles de notification (cf. section "Fenêtres de notification et fenêtres contextuelles" à la page 36) sur la découverte d'objets dangereux.

GLOSSAIRE

A

Activation de l'application

L'application devient entièrement fonctionnelle. L'utilisateur doit avoir une licence pour activer l'application.

Administrateur de Kaspersky Administration Kit

Personne qui gère les travaux du programme grâce à un système d'administration centralisé à distance de Kaspersky Administration Kit.

Agent d'administration

Composant de l'application Kaspersky Administration Kit qui coordonne les interactions entre le Serveur d'administration et les applications Kaspersky Lab installées sur un poste spécifique du réseau (un poste de travail ou un serveur). Ce composant prend en charge toutes les applications Windows présentes dans la gamme de produits Kaspersky Lab. Il existe des versions de l'Agent d'administration spécifiques aux applications Kaspersky Lab fonctionnant sur Novell, Unix ou Mac.

Analyseur heuristique

Technologie d'identification des menaces qui n'ont pas été identifiées à l'aide des bases des applications de Kaspersky Lab. Celle-ci permet d'identifier les objets soupçonnés d'être infectés par un virus inconnu ou par une nouvelle modification d'un virus connu.

L'analyseur heuristique permet d'identifier jusqu'à 92% des nouvelles menaces. Ce mécanisme est assez efficace et entraîne rarement des faux-positifs.

Les fichiers identifiés à l'aide de l'analyseur heuristique sont considérés comme des fichiers suspects.

Archive

Fichier qui contient un ou plusieurs autres objets qui peuvent être des archives.

B

Bases

Les bases de données sont créées par les experts de Kaspersky Lab et elles contiennent une description détaillée de toutes les menaces informatiques qui existent à l'heure actuelle ainsi que les moyens de les identifier et de les neutraliser. Les bases sont actualisées en permanence par Kaspersky Lab au fur et à mesure que de nouvelles menaces sont découvertes.

Blocage d'un objet

Interdiction de l'accès d'applications tiers à l'objet. L'objet bloqué ne peut être lu, exécuté ou modifié.

C

Client du Serveur d'administration (poste client)

L'ordinateur, serveur ou poste de travail sur lequel l'Agent d'administration est installé, ainsi que les applications administrées de Kaspersky Lab.

D

DOSSIER DE SAUVEGARDE

Le stockage spécial est conçu pour l'enregistrement des copies de sauvegarde des objets, créées avant leur première réparation ou suppression.

E

ETAT DE PROTECTION

État actuel de la protection caractérisé par le niveau de sécurité de l'ordinateur.

EXCLUSION

Objet exclu de l'analyse de l'application de Kaspersky Lab. Vous pouvez exclure de l'analyse des fichiers d'un format défini, des fichiers selon un masque, certains secteurs (par exemple :un répertoire ou un programme), des processus ou des objets selon un type de menace conforme à la classification de l'encyclopédie des virus. Des exclusions peuvent être définies pour chaque tâche.

F

FAUX-POSITIFS

Situation qui se présente lorsqu'un objet sain est considéré par l'application de Kaspersky Lab comme étant infecté car son code évoque celui d'un virus.

G

GROUPE D'ADMINISTRATION

Sélection d'ordinateurs regroupés selon les fonctions exécutées et les applications de Kaspersky Lab installées. Les ordinateurs sont regroupés pour en faciliter la gestion dans son ensemble. Le groupe peut se trouver à l'intérieur d'autres groupes. Il est possible de créer dans le groupe les stratégies de groupe pour chacune des applications installées et chacune des tâches de groupe créées.

L

LES SERVEURS DE MISE A JOUR DE KASPERSKY LAB

Liste de serveurs HTTP et FTP de Kaspersky Lab d'où l'application peut récupérer les bases et les mises à jour des modules.

LICENCE ACTIVE

Licence en cours d'utilisation par l'application de Kaspersky Lab. La licence détermine la durée de validité du fonctionnement complet de l'application ainsi que la politique de licence de l'application. L'application ne peut avoir qu'une application active à la fois.

LICENCE COMPLEMENTAIRE

Licence ajoutée pour le fonctionnement de l'application de Kaspersky Lab mais qui n'a pas été activée. La licence complémentaire entre en vigueur lorsque la licence active est arrivée à échéance.

M

MASQUE DE FICHIER

Représentation du nom et de l'extension d'un fichier par des caractères génériques. Les deux caractères principaux utilisés à cette fin sont * et ? (où * représente n'importe quel nombre de n'importe quels caractères et ? représente un

caractère unique). A l'aide de ces caractères, il est possible de représenter n'importe quel fichier. Attention! le nom et l'extension d'un fichier sont toujours séparés par un point.

MISE A JOUR

Procédure de remplacement/d'ajout de nouveaux fichiers (bases ou modules logiciels), récupérés des serveurs de mise à jour de Kaspersky Lab.

MISE A JOUR DES BASES

Une des fonctions de l'application de Kaspersky Lab qui permet de garantir l'actualité de la protection. Dans ce scénario, les bases sont copiées depuis les serveurs de mise à jour de Kaspersky Lab sur l'ordinateur et elles sont installées automatiquement.

N

NIVEAU RECOMMANDE

Niveau de protection qui repose sur les paramètres de fonctionnement définis par les experts de Kaspersky Lab et qui garantit la protection optimale de votre ordinateur. Ce niveau de protection est activé par défaut à l'installation.

O

OBJET DANGEREUX

Objet contenant un virus. Nous vous déconseillons de manipuler de tels objets car ils pourraient infecter votre ordinateur. Suite à la découverte d'un objet infecté, il est conseillé de le réparer à l'aide d'une application de Kaspersky Lab ou de le supprimer si la réparation est impossible.

OBJET INFECTE

Objet contenant un code malveillant : l'analyse de l'objet a mis en évidence une équivalence parfaite entre une partie du code de l'objet et le code d'une menace connue. Les experts de Kaspersky Lab vous déconseillent de manipuler de tels objets car ils pourraient infecter votre ordinateur.

OBJET OLE

Objet uni ou intégré à un autre fichier. L'application de Kaspersky Lab permet de rechercher la présence éventuelle de virus dans les objets OLE. Par exemple, si vous insérez un tableau Excel dans un document Microsoft Office Word, ce tableau sera analysé comme un objet OLE.

OBJET POTENTIELLEMENT INFECTE

Objet qui, en raison de son format ou de sa structure, peut être utilisé par un individu mal intentionné en tant que "conteneur" pour abriter et diffuser un objet malveillant. En règle générale, il s'agit d'objets exécutables avec, par exemple, les extensions com, exe, dll, etc. Le risque d'infection par un code malveillant est très élevé pour ces fichiers.

OBJET POTENTIELLEMENT INFECTE

Objet dont le code contient le code modifié d'un virus connu ou un code semblable à celui d'un virus mais inconnu de Kaspersky Lab. Les objets potentiellement infectés sont identifiés à l'aide de l'analyseur heuristique.

OBJET SUSPECT

Objet dont le code contient le code modifié d'un virus connu ou un code semblable à celui d'un virus mais inconnu de Kaspersky Lab. Les objets suspects sont détectés grâce à l'analyseur heuristique.

P

PAQUET DE MISE A JOUR

Ensemble de fichiers provenant d'Internet et s'installant sur votre ordinateur afin de mettre à jour une application.

PORT DE RESEAU

Paramètre des protocoles TCP et UDP déterminant la destination des paquets de données IP transmis vers l'hôte via le réseau et permettant aux divers programmes utilisés sur ce même hôte de recevoir des données indépendamment les uns des autres. Chaque programme traite les données envoyées sur un port bien défini (en d'autres termes, le programme "écoute" ce port).

Certains ports standards sont destinés aux protocoles réseau les plus courants (par exemple, les serveurs Web réceptionnent généralement les données envoyées via le protocole HTTP sur le port TCP 80). Néanmoins, un programme peut utiliser n'importe quel protocole et n'importe quel port. Valeurs possibles: de 1 à 65535.

PROTECTION

Mode de fonctionnement pendant lequel l'application analyse en temps réel la présence de code malveillant.

L'application intercepte toutes les tentatives d'ouverture d'un objet en lecture, écriture et exécution et recherche la présence éventuelle de menaces. Les objets sains sont ignorés alors que les objets (potentiellement) malveillants sont traités conformément aux paramètres de la tâche (réparation, suppression, mise en quarantaine).

PROTECTION MAXIMALE

Niveau de protection le plus élevé que l'application peut garantir pour votre ordinateur. Ce niveau de protection antivirus permet d'analyser tous les fichiers présents sur l'ordinateur, les supports amovibles et les disques réseau éventuellement connectés.

Q

QUARANTAINE

Répertoire défini dans lequel sont placés tous les objets potentiellement infectés découverts pendant l'analyse ou par la protection en temps réel.

R

RESTAURATION

Déplacement d'un objet original depuis le dossier de quarantaine ou de sauvegarde vers l'emplacement où il était avant sa mise en quarantaine, sa réparation ou sa suppression ou vers un dossier spécifié par l'utilisateur.

REPARATION D'OBJETS

Mode de traitement des objets infectés qui débouche sur la restauration totale ou partielle des données ou sur le constat de l'impossibilité de réparer les objets. La réparation des objets s'opère sur la base des enregistrements des bases. Une partie des données peut être perdue lors de la réparation.

S

SERVEUR D'ADMINISTRATION

Composant de l'application Kaspersky Administration Kit qui remplit la fonction d'enregistrement centralisé des informations sur les applications Kaspersky Lab installées sur le réseau local de la société, et d'un outil efficace de gestion de ces applications.

STRATEGIE

Sélection des paramètres de fonctionnement de l'application dans le groupe d'administration en cas d'administration à l'aide de Kaspersky Administration Kit. Les paramètres de fonctionnement de l'application peuvent varier en fonction des groupes. Une stratégie propre à chaque application peut être définie. La stratégie contient les paramètres de la configuration complète de toutes les fonctions de l'application.

STRATEGIE DE GROUPE

cf. Stratégie

T

TECHNOLOGIE GROWL

Système universel de notification de l'utilisateur sous Mac OS X. Il prend en charge les styles de notification configurés : outre les fenêtres contextuelles, il est possible d'utiliser la synthèse vocale, l'envoi d'un SMS ou l'envoi d'un courrier.

L'apparence des notifications émises par Growl peut être configurée dans la section Autres des Préférence Système à laquelle Growl est ajouté après l'installation.

TACHE DE GROUPE

Tâche définie pour un groupe et exécutée sur tous les postes clients de ce groupe d'administration.

TACHE POUR UNE SELECTION D'ORDINATEURS

Tâche définie pour une sélection des postes clients parmi des groupes d'administration aléatoires et exécutée sur ceux-ci.

V

VIRUS INCONNU

Nouveau virus pour lequel aucune information ne figure dans les bases. En règle générale, les virus inconnus sont découverts dans les objets à l'aide de l'analyse heuristique et ces objets reçoivent l'état potentiellement infecté.

KASPERSKY LAB

Kaspersky Lab est un éditeur de renommée mondiale de systèmes de protection contre les menaces informatiques : virus et autres programmes malveillants, courrier indésirable, attaques de réseau et attaques de pirates.

En 2008, Kaspersky Lab a fait son entrée dans le Top 4 des leaders mondiaux du marché des solutions de sécurité informatique pour les utilisateurs finaux (classement " IDC Worldwide Endpoint Security Revenue by Vendor "). Selon les résultats d'une étude réalisée par KomKon TGI-Russia 2009, Kaspersky Lab est l'éditeur de système de protection préféré des utilisateurs particuliers en Russie.

Kaspersky Lab a vu le jour en Russie en 1997. Aujourd'hui, Kaspersky Lab est devenu un groupe international de sociétés dont le siège principal est basé à Moscou. La société compte cinq filiales régionales qui gèrent les activités de la société en Russie, en Europe de l'Ouest et de l'Est, au Moyen Orient, en Afrique, en Amérique du Nord et du Sud, au Japon, en Chine et dans d'autres pays de la région Asie-Pacifique. La société emploie plus de 2 000 experts qualifiés.

Produits. Les produits développés par Kaspersky Lab protègent aussi bien les ordinateurs des particuliers que les ordinateurs des réseaux d'entreprise.

La gamme de logiciels pour particuliers reprend des logiciels antivirus pour ordinateurs de bureau et ordinateurs portables ainsi que des applications pour la protection des ordinateurs de poche, des smartphones et d'autres appareils nomades.

La société propose des applications et des services pour la protection des postes de travail, des serveurs de fichiers et Internet, des passerelles de messagerie et des pare-feu. L'utilisation de ces solutions en combinaison avec des outils d'administration centralisés permet de mettre en place et d'exploiter une protection efficace automatisée de l'organisation contre les menaces informatiques. Les logiciels de Kaspersky Lab ont obtenu les certificats des plus grands laboratoires d'essai. Ils sont compatibles avec les applications de nombreux éditeurs et ils sont optimisés pour de nombreuses plateformes matérielles.

Les experts de la lutte antivirus de Kaspersky Lab travaillent 24h/24. Chaque jour, ils trouvent des centaines de nouvelles menaces informatiques, développent les outils d'identification et de neutralisation de ces menaces et les ajoutent aux bases utilisées par les applications de Kaspersky Lab. *Les bases antivirus de Kaspersky Lab sont actualisées toutes les heures*, tandis que *les bases antispam* sont actualisées *toutes les 5 minutes*.

Technologies. Kaspersky Lab est à l'origine de nombreuses technologies sans lesquelles il est impossible d'imaginer un logiciel antivirus moderne. Ce n'est donc pas un hasard si le moteur logiciel de Kaspersky Anti-Virus est intégré aux logiciels de plusieurs autres éditeurs : citons notamment Safenet (É-U), Alt-N (É-U), Blue Coat (É-U), Check Point (Israël), Clearswift (R-U), Communigate Systems (É-U), Critical Path (Irlande), D-Link (Taïwan), Finjan (É-U), GFI (Malte), IBM (É-U), Juniper (É-U), LANDesk (É-U), Microsoft (É-U), Netasq (France), Netgear (É-U), Parallels (Russie), Sonicwall (É-U), WatchGuard (É-U), ZyXEL (Taïwan). De nombreuses technologies novatrices développées par la société sont brevetées.

Réalisations. Au cours de ces années de lutte contre les menaces informatiques, Kaspersky Lab a décroché des centaines de récompenses. Ainsi, en 2010, Kaspersky Anti-Virus a obtenu la note la plus élevée Advanced+ à l'issue de tests réalisés par le laboratoire antivirus autrichien renommé AV-Comparatives. Mais la récompense la plus importante de Kaspersky Lab, c'est la fidélité de ses utilisateurs à travers le monde. Les produits et les technologies de la société protègent plus de 300 millions d'utilisateurs. Elle compte également plus de 200 000 entreprises parmi ses clients.

Site Web de Kaspersky Lab :	http://www.kaspersky.com/fr
Encyclopédie des virus :	http://www.securelist.com/fr/
Laboratoire antivirus :	mailto:newvirus@kaspersky.com
	(uniquement pour l'envoi d'objets suspects sous forme d'archive)
	http://support.kaspersky.ru/virlab/helpdesk.html?LANG=fr
	(pour les demandes auprès des experts en virus)
Forum de Kaspersky Lab :	http://forum.kaspersky.com

INFORMATIONS SUR LE CODE TIERS

Du code développé par des éditeurs tiers a été utilisé pour créer l'application.

DANS CETTE SECTION

CODE D'APPLICATION

Du code de programme développé par des éditeurs tiers a été utilisé pour créer l'application.

DANS CETTE SECTION

ADOBE ABI-SAFE CONTAINERS 1.0

BOOST 1.39.0

CURL 7.19.3

EXPAT 1.2

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

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

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,

EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF

MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT.

IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR ANYONE DISTRIBUTING THE SOFTWARE BE LIABLE FOR ANY DAMAGES OR OTHER LIABILITY, WHETHER IN CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

FMT.H

Copyright (C) 2002, Lucent Technologies

Permission to use, copy, modify, and distribute this software for any purpose without fee is hereby granted, provided that this entire notice is included in all copies of any software which is or includes a copy or modification of this software and in all copies of the supporting documentation for such software.

THIS SOFTWARE IS BEING PROVIDED "AS IS", WITHOUT ANY EXPRESS OR IMPLIED WARRANTY. IN PARTICULAR, NEITHER THE AUTHORS NOR LUCENT TECHNOLOGIES MAKE ANY REPRESENTATION OR WARRANTY OF ANY KIND CONCERNING THE MERCHANTABILITY OF THIS SOFTWARE OR ITS FITNESS FOR ANY PARTICULAR PURPOSE.

GROWL 1.1.5

Copyright (C) 2004, The Growl Project

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of Growl nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)

HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

INFO-ZIP 5.51

Copyright (C) 1990-2007, Info-ZIP

For the purposes of this copyright and license, "Info-ZIP" is defined as the following set of individuals:

Mark Adler, John Bush, Karl Davis, Harald Denker, Jean-Michel Dubois, Jean-loup Gailly, Hunter Goatley, Ed Gordon, Ian Gorman, Chris Herborth, Dirk Haase, Greg Hartwig, Robert Heath, Jonathan Hudson, Paul Kienitz, David Kirschbaum, Johnny Lee, Onno van der Linden, Igor Mandrichenko, Steve P. Miller, Sergio Monesi, Keith Owens, George Petrov, Greg Roelofs, Kai Uwe Rommel, Steve Salisbury, Dave Smith, Steven M. Schweda, Christian Spieler, Cosmin Truta, Antoine Verheijen, Paul von Behren, Rich Wales, Mike White.

This software is provided "as is", without warranty of any kind, express or implied. In no event shall Info-ZIP or its contributors be held liable for any direct, indirect, incidental, special or consequential damages arising out of the use of or inability to use this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the above disclaimer and the following restrictions:

1. Redistributions of source code (in whole or in part) must retain the above copyright notice, definition, disclaimer, and this list of conditions.

2. Redistributions in binary form (compiled executables and libraries) must reproduce the above copyright notice, definition, disclaimer, and this list of conditions in documentation and/or other materials provided with the distribution. The sole exception to this condition is redistribution of a standard UnZipSFX binary (including SFXWiz) as part of a self-extracting archive; that is permitted without inclusion of this license, as long as the normal SFX banner has not been removed from the binary or disabled.

3. Altered versions--including, but not limited to, ports to new operating systems, existing ports with new graphical interfaces, versions with modified or added functionality, and dynamic, shared, or static library versions not from Info-ZIP--must be plainly marked as such and must not be misrepresented as being the original source or, if binaries, compiled from the original source. Such altered versions also must not be misrepresented as being Info-ZIP releases--including, but not limited to, labeling of the altered versions with the names "Info-ZIP" (or any variation thereof, including, but not limited to, different capitalizations), "Pocket UnZip," "WiZ" or "MacZip" without the explicit permission of Info-ZIP. Such altered versions are further prohibited from misrepresentative use of the Zip-Bugs or Info-ZIP e-mail addresses or the Info-ZIP URL(s), such as to imply Info-ZIP will provide support for the altered versions.

4. Info-ZIP retains the right to use the names "Info-ZIP," "Zip," "UnZip," "UnZipSFX," "WiZ," "Pocket UnZip," "Pocket Zip," and "MacZip" for its own source and binary releases.

LIBPNG 1.2.8

Copyright (C) 2004, 2006-2009, Glenn Randers-Pehrson

LIBUTF

Copyright (C) 2002, Lucent Technologies

Permission to use, copy, modify, and distribute this software for any purpose without fee is hereby granted, provided that this entire notice is included in all copies of any software which is or includes a copy or modification of this software and in all copies of the supporting documentation for such software.

THIS SOFTWARE IS BEING PROVIDED "AS IS", WITHOUT ANY EXPRESS OR IMPLIED WARRANTY. IN PARTICULAR, NEITHER THE AUTHORS NOR LUCENT ECHNOLOGIES MAKE ANY REPRESENTATION OR WARRANTY OF ANY KIND CONCERNING THE MERCHANTABILITY OF THIS SOFTWARE OR ITS FITNESS FOR ANY PARTICULAR PURPOSE.

LZMALIB 4.43

MD5.H

Copyright (C) 1999, Aladdin Enterprises

MD5.H

Copyright (C) 1990, RSA Data Security, Inc

License to copy and use this software is granted provided that it is identified as the "RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing this software or this function.

License is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing the derived work.

RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind.

These notices must be retained in any copies of any part of this documentation and/or software.

RFC1321-BASED (RSA-FREE) MD5 LIBRARY

Copyright (C) 1999, 2002, Aladdin Enterprises

SHA1.C 1.2

STLPORT 5.2.1

Copyright (C) 1994, Hewlett-Packard Company

Copyright (C) 1996-1999, Silicon Graphics Computer Systems, Inc.

Copyright (C) 1997, Moscow Center for SPARC Technology

Copyright (C) 1999-2003, Boris Fomitchev

This material is provided "as is", with absolutely no warranty expressed or implied. Any use is at your own risk.

Permission to use or copy this software for any purpose is hereby granted without fee, provided the above notices are retained on all copies. Permission to modify the code and to distribute modified code is granted, provided the above notices are retained, and a notice that the code was modified is included with the above copyright notice.

TINYXML 2.5.3

Copyright (C) 2000-2006, Lee Thomason

ZLIB 1.0.8, 1.2.3

Copyright (C) 1995-2010, Jean-loup Gailly and Mark Adler

MOYENS D'EXPLOITATION

Les moyens d'exploitation, les instruments et les autres moynes des éditeurs tiers ont été utilisés pour créer l'application.

DANS CETTE SECTION

GCC 4.0.1

Copyright (C) 1987, 1989, 1992, 1993, 1994, 1995, 1996, 1997, 1998, 1999, 2000, 2001, 2002, 2003, 2004, 2005 Free Software Foundation, Inc

---

GNU GENERAL, PUBLIC, and LICENSE:

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

one line to give the program's name and an idea of what it does.

Copyright (C) yyyy name of author

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author

Gnomovision comes with ABSOLUTELY NO WARRANTY; for details

type `show w'. This is free software, and you are welcome

to redistribute it under certain conditions; type `show c'

for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program `Gnomovision'

(which makes passes at compilers) written

by James Hacker.

signature of Ty Coon, 1 April 1989

Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License.

AUTRE INFORMATION

Informations supplémentaire sur le code tiers.

La composition et l'analyse de la signature numérique électronique dans Kaspersky Anti-Virus repose sur la bibliothèque logicielle de protection de l'information "Agava-C" développée par OOO "R-Alpha".

Le Logiciel peut comprendre des programmes concédés à l'utilisateur sous licence (ou sous-licence) dans le cadre d'une licence publique générale GNU (General Public License, GPL) ou d'autres licences de logiciel gratuites semblables, qui entre autres droits, autorisent l'utilisateur à copier, modifier et redistribuer certains programmes, ou des portions de ceux-ci, et à accéder au code source (" Logiciel libre "). Si ces licences exigent que, pour tout logiciel distribué à quelqu'un au format binaire exécutable, le code source soit également mis à la disposition de ces utilisateurs, le code source sera être communiqué sur demande adressée à source@kaspersky.com ou fourni avec le Logiciel.

INDEX

A

B

C

D

F

G

I

L

M

N

O

P

Q

R

S

T

V

Z