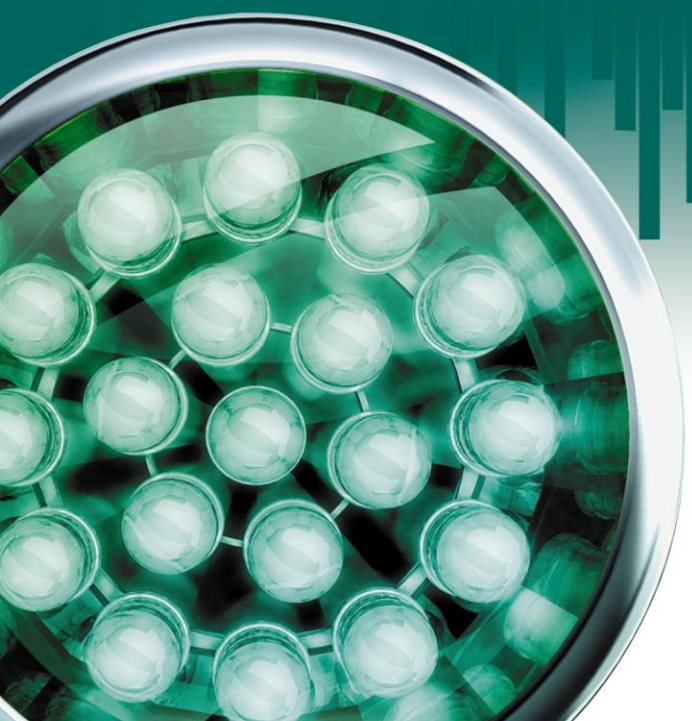
# Kaspersky Internet Security 2011

# MANUEL DE L'UTILISATEUR

VERSION DE L'APPLICATION : 11.0



KASPERSKY lab

Chers utilisateurs !

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



Ce document peut être modifié sans un avertissement préalable. La version la plus récente de ce document est accessible sur le site de Kaspersky Lab à l'adresse http://www.kaspersky.com/fr/docs.



Date d'édition : 30/04/10



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

# CONTENU

# 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 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.

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. Le Titulaire des droits convient par la présente de Vous accorder 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 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 auprès du Titulaire des droits, *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. Vous pouvez transférer la licence non exclusive d'utilisation du Logiciel à d'autres personnes physiques dans la limite du champ d'application de la licence qui Vous est accordée par le Titulaire des droits, à condition que son destinataire accepte de respecter les conditions générales de ce Contrat et se substitue pleinement à vous dans le cadre de la licence que vous accorde le Titulaire des droits. Si Vous transférez intégralement les droits d'utilisation du Logiciel que vous accorde le Titulaire des droits, Vous devrez détruire toutes les copies du Logiciel, y compris la copie de sauvegarde. Si Vous êtes le destinataire du transfert d'une licence, Vous devez accepter de respecter toutes les conditions générales de ce Contrat. Si vous n'acceptez pas de respecter toutes les conditions générales de ce Contrat, Vous n'êtes pas autorisé à installer ou utiliser le Logiciel. Vous acceptez également, en qualité de destinataire de la licence transférée, de ne jouir d'aucun droit autre que ceux de l'Utilisateur final d'origine qui avait acquis le Logiciel auprès du Titulaire des droits.

2.6. 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. Si le Titulaire des droits fixe une autre durée pour la période d'évaluation unique applicable, Vous serez informé(e) par notification.

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 d'utilisation du Logiciel 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.

3.10. Le détenteur des droits se réserve le droit de limiter la possibilité d'activation en dehors de la région dans laquelle le logiciel a été acquis auprès du détenteur des droits et/ou de ses partenaires.

3.11. Si vous avez acheté le logiciel avec un code d'activation valide pour la localisation de la langue parlée dans la région où il a été acquis auprès du détenteur des droits ou de ses partenaires, vous ne pouvez pas activer le logiciel avec le code d'activation prévu pour la localisation d'une autre langue.

3.12. En cas de restrictions précisées dans les clauses 3.10 et 3.11, vous trouverez des informations concernant ces restrictions sur l'emballage et/ou le site Web du détenteur et/ou de ses partenaires.

**4. Assistance technique**

4.1 L'assistance technique décrite dans la Clause 2.6 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

**5 Recueil d'informations**

5.1. Conformément aux conditions générales de ce Contrat, Vous consentez à communiquer au Titulaire des droits des informations relatives aux fichiers exécutables et à leurs sommes de contrôle pour améliorer Votre niveau de protection et de sécurité.

5.2. Pour sensibiliser le public aux nouvelles menaces et à leurs sources, et dans un souci d'amélioration de Votre sécurité et de Votre protection, le Titulaire des droits, avec votre consentement explicitement confirmé dans le cadre de la déclaration de recueil des données du réseau de sécurité Kaspersky, est autorisé à accéder à ces informations. Vous pouvez désactiver le réseau de sécurité Kaspersky pendant l'installation. Vous pouvez également activer et désactiver le réseau de sécurité Kaspersky à votre guise, à la page des options du Logiciel.

Vous reconnaissez par ailleurs et acceptez que toutes les informations recueillies par le Titulaire des droits pourront être utilisées pour suivre et publier des rapports relatifs aux tendances en matière de risques et de sécurité, à la seule et exclusive appréciation du Titulaire des droits.

5.3. Le Logiciel ne traite aucune information susceptible de faire l'objet d'une identification personnelle et ne combine les données traitées avec aucune information personnelle.

5.4. Si vous ne souhaitez pas que les informations recueillies par le Logiciel soient transmises au Titulaire des droits, n'activez pas ou ne désactivez pas le réseau de sécurité Kaspersky.

**6. Limitations**

6.1. 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.

6.2. Vous ne devrez transférer les droits d'utilisation du Logiciel à aucune tierce partie sauf aux conditions énoncées dans la Clause 2.5 de ce Contrat.

6.3. 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, et vous prendrez toutes les mesures raisonnables nécessaires à la protection du code d'activation et/ou du fichier clé de licence, étant entendu que vous pouvez transférer le code d'activation et/ou le fichier clé de licence à de tierces parties dans les conditions énoncées dans la Clause 2.5 de ce Contrat.

6.4. Vous vous engagez à ne louer, donner à bail ou prêter le Logiciel à aucune tierce partie.

6.5. 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.

6.6. Le Titulaire des droits a le droit de bloquer le fichier clé de licence ou de mettre fin à votre Licence d'utilisation du Logiciel en cas de non-respect de Votre part des conditions générales de ce Contrat, et ce, sans que vous puissiez prétendre à aucun remboursement.

6.7. 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.

7. **Garantie limitée et avis de non-responsabilité**

7.1. 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.

7.2. 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 adaptés à Votre cas.

7.3. 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.

7.4. 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 2.6 de ce Contrat.

7.5. 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.

7.6. 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, LE " 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.

**8. Exclusion et Limitation de responsabilité**

8.1 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, 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 DE TOUT PARTENAIRE DE CELUI-CI, MÊME SI LE TITULAIRE DES DROITS 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 SERA 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.

## 9. Licence GNU et autres licences de tierces parties

9.1 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 être 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.

## 10. Droits de propriété intellectuelle

10.1 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 Etats-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.

10.2 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.

## 11. Droit applicable ; arbitrage

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 11 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.

**12. Délai de recours.**

12.1 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.

**13. Intégralité de l'accord ; divisibilité ; absence de renoncement.**

13.1 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 equity 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.

**14. 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

# PRESENTATION DU GUIDE

Ce document est le guide d'installation, de configuration et d'utilisation de l'application Kaspersky Internet Security 2011 (ci-après Kaspersky Internet Security). Ce document est prévu pour un large public. L'utilisateur de l'application doit posséder des connaissances de base sur l'utilisation de l'ordinateur : connaissance de l'interface du système d'exploitation Windows, maîtrise des principales tâches, maîtrise des logiciels les plus utilisés pour le courrier électronique et Internet, par exemple Microsoft Office Outlook et Microsoft Internet Explorer.

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 ;
- Offrir un accès rapide aux informations pour répondre aux questions liées à l'application ;
- Présenter les autres sources d'informations sur l'application et les méthodes pour obtenir une assistance technique.

### DANS CETTE SECTION



# DANS CE DOCUMENT

Les sections suivantes sont présentées dans ce document :

### Sources d'informations complémentaires

Cette rubrique décrit les sources d'informations complémentaires sur l'application et les sites sur lesquels il est possible de discuter de l'application, de partager des idées, de poser des questions et d'obtenir des réponses.

### Kaspersky Internet Security 2011

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

### Installation de l'application

Cette rubrique contient les instructions qui vous aideront à installer l'application sur l'ordinateur et à effectuer sa configuration initiale. Cette rubrique aussi décrit comment supprimer l'application de l'ordinateur.

### Gestionnaire de licences

Cette rubrique contient les informations sur les notions générales utilisées dans le contexte de l'octroi de licences de l'application. Dans cette rubrique, vous apprendrez également comment prolonger automatiquement la durée de validité de la licence et où trouver les informations sur la licence actuelle.

### Interface de l'application

Cette rubrique 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, 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. Cette rubrique explique aussi comment activer ou désactiver la suspension temporaire de la protection pendant l'utilisation de Kaspersky Internet Security.

### Résolution des problèmes types

Cette rubrique contient des instructions sur les principales tâches de l'application réalisées le plus souvent par l'utilisateur.

### Configuration étendue de l'application

Cette rubrique 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.

### Validation de la configuration de l'application

Cette rubrique contient les recommandations sur la vérification de l'exactitude de la configuration des composants de l'application.

### Contacter le support technique

Cette rubrique contient les recommandations sur les demandes d'aide adressées à Kaspersky Lab depuis Mon Espace Personnel sur le site web du Service d'assistance technique et par téléphone.

### Annexes

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

### Glossaire

Cette rubrique 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 des informations importantes, par exemple, les informations liées aux actions critiques pour la sécurité de l'ordinateur. |

| EXEMPLE DE TEXTE | DESCRIPTION DE LA CONVENTION |
|---|---|
| Il est conseillé d'utiliser ... | Les remarques sont encadrées. Les remarques fournissent des conseils et des informations d'assistance. |
| **Exemple :**<br><br>... | Les exemples sont présentés sur un fond jaune sous le titre "Exemple". |
| La *mise à jour*, c'est ... | Les nouveaux termes sont en italique. |
| **ALT+F4** | Les noms des touches du clavier sont en caractères mi-gras et en lettres majuscules.<br><br>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.<br><br>Les phrases d'introduction sont en italique. |
| `help` | Les textes dans la ligne de commande ou les textes des messages affichés sur l'écran par l'application sont en caractères spéciaux. |
| <adresse IP de votre ordinateur> | Les variables sont écrites entre chevrons. La valeur correspondant à la variable remplace cette variable à chaque fois. Par ailleurs, les parenthèses angulaires sont omises. |

# SOURCES D'INFORMATIONS COMPLEMENTAIRES

Si vous avez des questions sur la sélection, l'achat, l'installation ou l'utilisation de Kaspersky Internet Security, vous pourrez trouver les réponses en utilisant diverses sources d'informations. Vous pouvez ainsi choisir celle qui s'adapte le mieux à votre situation en fonction de l'importance et de l'urgence de la question.

### DANS CETTE SECTION



# SOURCES D'INFORMATIONS POUR UNE AIDE AUTONOME

Kaspersky Lab propose les sources d'informations suivantes sur l'application :

- La page de l'application sur le site de Kaspersky Lab ;
- La page de l'application sur le site du support technique (dans la banque de solutions) ;
- La page du service d'assistance interactive ;
- Aide électronique.

**Page du site de Kaspersky Lab**

Cette page (http://www.kaspersky.com/fr/kaspersky_internet_security) fournit des informations générales sur l'application, ces possibilités et ses particularités.

**Page sur le site du service du support technique (banque de solutions)**

Cette page (http://support.kaspersky.com/fr/kis2011) reprend des articles publiés par les experts du service du support technique.

Ces articles proposent des informations utiles, des recommandations et des réponses aux questions fréquemment posées sur l'achat, l'installation et l'utilisation de l'application. Ils sont regroupés par sujet, par exemple "Utilisation de la licence de l'application", "Configuration des mises à jour" ou "Suppression des erreurs de fonctionnement". Les articles peuvent répondre à des questions en rapport non seulement avec cette application, mais également avec d'autres applications de Kaspersky Lab. De plus, ils peuvent fournir des informations sur le service d'assistance technique en général.

**Service d'assistance interactive**

La page de ce service propose une base actualisée fréquemment avec les questions fréquemment posées sur l'utilisation de l'application. L'utilisation du service requiert une connexion à Internet.

Pour accéder à la page du service, cliquez sur le lien **Assistance technique** dans la fenêtre principale, puis dans la fenêtre qui s'ouvre, cliquez sur le bouton **Assistance interactive**.

**Aide électronique**

La distribution de l'application reprend le fichier d'aide complète et contextuelle. Il contient les informations sur la gestion de la protection de l'ordinateur : consultation de l'état de la protection, analyse de divers secteurs de l'ordinateur, exécution d'autres tâches. En plus, dans le fichier d'aide contextuelle et complète 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 le fichier d'aide, cliquez sur le bouton **Aide** dans la fenêtre qui vous intéresse ou sur la touche **F1** du clavier.

# DISCUSSION SUR LES LOGICIELS DE KASPERSKY LAB DANS LE FORUM EN LIGNE

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

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

# CONTACTER LE SERVICE COMMERCIAL

Si vous avez des questions sur la sélection ou l'achat de Kaspersky Internet Security ou la prolongation de la licence, vous pouvez contacter le Service commercial (http://www.kaspersky.com/fr/contacts).

Contactez les collaborateurs du service commercial par courrier électronique à l'adresse sales@kaspersky.com.

# COMMUNICATION AVEC LE GROUPE DE REDACTION DE LA DOCUMENTATION

Si vous avez des questions sur la documentation, si vous avez découvert des erreurs ou si vous souhaitez envoyer des commentaires sur nos guides, vous pouvez contacter le groupe de rédaction de la documentation technique. Pour s'adresser au Groupe de rédaction de la documentation, envoyez la lettre à l'adresse docfeedback@kaspersky.com. Indiquez "Kaspersky Help Feedback: Kaspersky Internet Security" comme le sujet de la lettre.

# KASPERSKY INTERNET SECURITY 2011

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

### DANS CETTE SECTION



# NOUVEAUTES

Les innovations suivantes sont présentes dans Kaspersky Internet Security :

- Le nouveau composant de la protection Surveillance du système (cf. page 112) assure la surveillance de l'activité des applications dans le système et offre les informations aux autres composants de la protection. Outre cela, grâce à l'historique enregistré sur l'activité des applications, le composant peut annuler les actions d'un programme malveillant lors de la détection de l'activité malveillante par des différents composants de la protection.

- La fonctionnalité perfectionnée de l'Environnement protégé **Bureau sécurisé** (cf. page 155) représente un bureau isolé sur lequel vous pouvez lancer les applications suspectes sans causer des dommages au système d'exploitation principal.

- Pour augmenter la protection lors du travail sur Internet, de nouveaux modules ont été ajoutés :

    - Navigation sécurisée (cf. page 106) inclut le module d'analyse des liens, déjà présent dans la version précédente de l'application, et permet de bloquer l'accès aux sites Web dangereux, ce qui vous maintient dans les limites de la zone sécurisée d'Internet.

    - Filtrage par géo localisation (cf. page 106) permet d'autoriser ou d'interdire l'accès aux sites Web en vertu de leur appartenance à certains domaines. Il est ainsi possible, par exemple, d'interdire l'accès à des sites web appartenant à des domaines régionaux présentant un risque d'infection très élevé.

- Le Contrôle des Applications permet de déterminer plus efficacement les états des applications et de configurer les règles pour les applications, en utilisant les données de Kaspersky Security Network basées sur les statistiques du fonctionnement du Contrôle des Applications sur les ordinateurs d'une multitude d'utilisateurs.

- A l'aide de l'Analyse pendant les temps morts de l'ordinateur (cf. page 174), la recherche de virus peut être maintenant exécutée durant les périodes pendant lesquelles vous ne travaillez pas sur l'ordinateur et s'arrêter quand vous reprenez le travail. Ceci permet d'analyser régulièrement sans réduire les performances de l'ordinateur quand vous en avez besoin.

- La fonctionnalité du Contrôle Parental (cf. page 160) est élargie : il est maintenant possible de contrôler l'accès de l'utilisateur à l'ordinateur et à Internet, le lancement par l'utilisateur des applications, de limiter l'affichage de pages Web au contenu indésirable et le téléchargement de fichiers depuis Internet, de contrôler les contacts de l'utilisateur dans les réseaux sociaux et via les messageries instantanées. Il est aussi possible de consulter les

rapports sur les actions de l'utilisateur contrôlé. Pour optimiser les paramètres du Contrôle Parental, il est possible d'exporter ou d'importer les paramètres de fonctionnement du composant pour le compte.

# ORGANISATION DE LA PROTECTION DE VOTRE ORDINATEUR

Kaspersky Internet Security protège votre ordinateur contre les menaces connues et nouvelles, les attaques de réseau et les escroqueries, les messages non sollicités et d'autres données indésirables.

Chaque type de menaces est traité par un *composant de la protection* particulier (cf. description des composants dans cette section). Il est possible d'activer et de désactiver les composants indépendamment les uns des autres et de configurer leur fonctionnement de la manière qui vous convient.

En plus de la protection en temps réel réalisée par des composants de la protection, il est recommandé d'*analyser* périodiquement votre ordinateur pour déceler d'éventuels virus. Cette opération s'impose pour exclure la possibilité de propager des programmes malveillants qui n'auraient pas été décelés par les composants de la protection en raison, par exemple, d'un niveau de protection faible ou pour toute autre raison.

La *mise à jour* des bases et des modules logiciels utilisés dans le fonctionnement de l'application est requise pour que Kaspersky Internet Security garantisse l'actualité de la protection. Par défaut, l'application est actualisée automatiquement. En cas de besoin, vous pouvez toujours actualiser manuellement les bases et les modules logiciels.

Il est possible de contrôler le lancement des applications particulières installées sur votre ordinateur : le *contrôle de l'activité des applications* a été développé à cette fin. L'accès des applications aux *données personnelles* est contrôlé d'une manière spéciale. Il s'agit des fichiers, des répertoires et des clés du registre qui contiennent les paramètres de fonctionnement et les données importantes des applications les plus souvent utilisées ainsi que les fichiers de l'utilisateur (répertoire Mes Documents, les cookies, les données relatives à l'activité de l'utilisateur). Les applications dont vous n'êtes pas sûr peuvent être lancées dans un *environnement protégé* spécial.

Certaines tâches spécifiques qui requièrent une exécution épisodique sont réalisées à l'aide d'outils et d'Assistants d'optimisation (cf. section "Outils de protection complémentaire" à la page 179) : par exemple, la configuration du navigateur Microsoft Internet Explorer ou la suppression des traces d'activité de l'utilisateur dans le système.

## Composants de protection

Les composants suivants assurent la protection en temps réel de votre ordinateur.

Antivirus Fichiers

L'Antivirus Fichiers permet d'éviter l'infection du système de fichiers de l'ordinateur. Le composant est lancé au démarrage du système d'exploitation. Il se trouve en permanence dans la mémoire vive de l'ordinateur et il analyse tous les fichiers ouverts, enregistrés et exécutés sur l'ordinateur et sur tous les disques montés. Kaspersky Internet Security intercepte chaque requête adressée à un fichier et recherche la présence éventuelle de virus connus dans ce dernier. Il sera possible de continuer à utiliser le fichier uniquement si celui-ci est sain ou s'il a pu être réparé par l'application. Si le fichier ne peut être réparé pour une raison quelconque, il sera supprimé. Une copie du fichier sera conservée dans la sauvegarde ou placée en quarantaine.

Antivirus Courrier

L'Antivirus Courrier l'ensemble du courrier entrant et sortant de votre ordinateur. Le message sera délivré au destinataire uniquement s'il ne contient aucun objet dangereux.

Antivirus Internet

L'Antivirus Internet intercepte et bloque l'exécution des scripts dans les pages Web si ceux-ci constituent une menace. Tout le trafic HTTP est également soumis à un contrôle strict. De plus, le composant bloque l'accès aux sites Web dangereux.

Antivirus IM ("Chat")

L'Antivirus IM garantit la sécurité de l'utilisation des messageries instantanées. Le composant protège les informations envoyées vers votre ordinateur via les protocoles des clients de messagerie instantanée. L'Antivirus IM vous protège pendant l'utilisation de nombreux clients de messagerie instantanée.

Défense Proactive

La Défense Proactive permet d'identifier un nouveau programme malveillant avant qu'il n'ait eu le temps de provoquer des dégâts. Le composant repose sur la surveillance et l'analyse du comportement de toutes les applications installées sur l'ordinateur. En fonction des tâches qu'ils exécutent, Kaspersky Internet Security décide si ces applications constituent un danger potentiel. Ainsi, l'ordinateur est protégé non seulement contre les virus connus mais également contre les nouveaux virus qui n'ont pas encore été étudiés.

Anti-phishing

Composant intégré à l'Antivirus Internet, l'Anti-Spam et l'Antivirus IM qui permet de vérifier si une URL appartient à la liste des URL suspectes ou de phishing.

Contrôle des Applications

Le Contrôle des Applications enregistre les actions réalisées par les applications dans le système et réglemente l'activité des applications sur la base du groupe dans lequel le composant place cette application. Un ensemble de règles est défini pour chaque groupe d'applications. Ces règles définissent l'accès des applications à diverses ressources du système d'exploitation.

Pare-feu

Le Pare-feu vous protège pendant l'utilisation des réseaux locaux et d'Internet. Le composant filtre toute l'activité de réseau selon deux types de règles : *les règles pour les applications* et *les règles pour les paquets*.

Prévention des intrusions

*La Prévention des intrusions* est lancée au démarrage du système d'exploitation et surveille l'activité du trafic entrant caractéristique des attaques de réseau. Dès qu'il décèle une tentative d'attaque contre votre ordinateur, Kaspersky Internet Security bloque toute activité de réseau de l'ordinateur qui vous attaque.

Anti-Spam

L'Anti-Spam s'intègre au client de messagerie de votre ordinateur et recherche la présence éventuelle de messages non sollicités dans tout le courrier entrant. Tous les messages non sollicités sont identifiés par un objet particulier. Il est possible également de configurer l'Anti-Spam pour le traitement du courrier indésirable (suppression automatique, enregistrement dans un répertoire spécial, etc.). Le composant recherche également la présence éventuelle d'attaques de phishing dans les messages électroniques.

Surveillance du réseau

Ce composant a été développé pour consulter en temps réel les informations relatives à l'activité de réseau.

Anti-bannière

L'Anti-bannière bloque les messages publicitaires situés sur des bannières spéciales dans l'interface de diverses applications installées sur votre ordinateur ou dans des sites Web.

Contrôle Parental

Le Contrôle Parental a été développé pour protéger les enfants et les adolescents des menaces liées à l'utilisation d'Internet et de l'ordinateur.

Le Contrôle Parental permet d'instaurer des restrictions souples sur l'accès aux ressources Internet et aux applications pour divers utilisateurs en fonction de l'âge. Il propose aussi des rapports statistiques sur les actions des utilisateurs contrôlés.

Les composants de l'application protègent trois groupes d'objets :

- Les fichiers, les données personnelles, les noms d'utilisateur et les mots de passe, les informations relatives aux cartes bancaires, etc. La protection de ces objets est garantie par l'Antivirus Fichiers, le Contrôle des Applications et la Défense proactive.

- Les applications installées sur l'ordinateur et les objets du système d'exploitation. La protection de ces objets est garantie par l'Antivirus Courrier, l'Antivirus Internet, l'Antivirus IM, le Contrôle des Applications, la Prévention des intrusions, l'Anti-Spam et la Défense proactive.

- Utilisation du réseau : consultation de sites, utilisation de systèmes de paiement en ligne, protection du courrier contre les messages non sollicités et les virus, etc. La protection de ces objets est garantie par l'Antivirus Courrier, l'Antivirus Internet, l'Antivirus IM ("Chat"), le Pare-feu, la Prévention des intrusions, l'Anti-Spam, la Surveillance du réseau, l'Anti-bannière et le Contrôle Parental et l'Anti-Phishing.

La présentation évidente du groupement des composants selon les objets à protéger est visible dans la section **Protection** de la fenêtre principale de l'application (cf. section "Fenêtre principale de Kaspersky Internet Security" à la page 42).

# DISTRIBUTION

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

Si vous achetez l'application en boîte, vous trouverez :

- Une pochette scellée contenant le CD d'installation avec les fichiers du logiciel et la documentation au format PDF ;

- Une version imprimée de la documentation dans le document Guide éclair de l'utilisateur ou Guide de l'utilisateur (selon la région) ;

- Le contrat de licence (selon la région) ;

- Une carte d'activation, contenant le code d'activation (selon la région).

Lisez attentivement le contrat de licence (cf. section "Présentation du contrat de licence" à la page 37) !

Si vous n'acceptez pas les conditions du contrat de licence, vous pouvez renvoyer la boîte avec le produit au partenaire chez qui vous l'aviez acheté et obtenir un remboursement. Dans ce cas, la pochette contenant le CD d'installation (ou les disquettes) doit toujours être scellée.

L'ouverture de la pochette contenant le CD d'installation (ou les disquettes) constitue une approbation des dispositions du contrat de licence.

Avant d'ouvrir la pochette contenant le CD (ou les disquettes), lisez attentivement le contrat de licence.

Si vous achetez Kaspersky Internet Security dans la boutique en ligne, vous copiez le logiciel depuis le site Web de Kaspersky Lab. Outre le logiciel, la distribution reprend également le présent guide. Le code d'activation est envoyé par courrier électronique après le paiement.

# SERVICE POUR LES UTILISATEURS ENREGISTRES

Kaspersky Lab offre à ses clients légitimes toute une série de services qui permettent d'accroître l'efficacité de l'utilisation de l'application.

Au moment d'obtenir la licence, vous devenez un utilisateur enregistré et vous pouvez utiliser les services suivants pendant la durée de validité de la licence :

- Mise à jour toutes les heures des bases de l'application et offre des nouvelles versions de cette application ;
- Consultations liées aux questions d'installation, de configuration et d'exploitation de l'application, via téléphone ou Mon Espace Personnel.
- Notifications sur la diffusion de nouveaux logiciels de Kaspersky Lab ou sur l'émergence de nouveaux virus. Ce service est offert aux utilisateurs qui se sont abonnés au bulletin d'informations de Kaspersky Lab sur le site du service d'Assistance technique (http://support.kaspersky.com/fr/subscribe).

Les questions relatives au fonctionnement et à l'utilisation des systèmes d'exploitation, des applications d'éditeurs tiers ou aux différentes technologies ne seront pas traitées.

# CONFIGURATIONS LOGICIELLE ET MATERIELLE

Afin de garantir le fonctionnement normal de Kaspersky Internet Security, l'ordinateur doit répondre à la configuration minimum suivante.

Configuration générale :

- 480 Mo d'espace disponible sur le disque dur.
- CD/DVD-ROM (pour l'installation de Kaspersky Internet Security depuis un cédérom).
- Connexion à Internet (pour la mise à jour des bases et des modules de l'application).
- Microsoft Internet Explorer 6.0 ou suivant.
- Microsoft Windows Installer 2.0.

Exigences pour les systèmes d'exploitation Microsoft Windows XP Home Edition (Service Pack 2 ou suivant), Microsoft Windows XP Professional (Service Pack 2 ou suivant), Microsoft Windows XP Professional x64 Edition (Service Pack 2 ou suivant) :

- Processeur Intel Pentium 800 MHz 32 bits (x86)/64 bits (x64) ou supérieur (ou analogue compatible) ;
- 512 Mo de mémoire vive disponible.

Exigences pour les systèmes d'exploitation Microsoft Windows Vista Home Basic, Microsoft Windows Vista Home Premium, Microsoft Windows Vista Business, Microsoft Windows Vista Enterprise, Microsoft Windows Vista Ultimate, Microsoft Windows 7 Starter, Microsoft Windows 7 Home Basic, Microsoft Windows 7 Home Premium, Microsoft Windows 7 Professional, Microsoft Windows 7 Ultimate :

- Processeur Intel Pentium 1 GHz 32 bits (x86)/64 bits (x64) ou supérieur (ou analogue compatible) ;
- 1 Go de mémoire vive disponible (32 bits), 2 Go de mémoire vive disponible (64 bits).

En cas d'utilisation de Microsoft Windows XP (64-bit), l'utilisation de l'Environnement protégé est impossible. Sous les systèmes d'exploitation Microsoft Windows Vista (64-bit) et Microsoft Windows 7(64-bit), l'utilisation de l'Environnement protégé est limitée.

Exigences pour les netbooks :

- Processeur Intel Atom 1.33 MHz (Z520) ou analogue compatible.
- Carte vidéo Intel GMA950 avec une mémoire d'au moins 64 Mo (ou analogue compatible).

- Écran de 10,1 pouces minimum.
- Système d'exploitation Microsoft Windows XP Home Edition ou suivant.

# INSTALLATION DE L'APPLICATION

Cette rubrique contient les instructions qui vous aideront à installer l'application sur l'ordinateur et à effectuer sa configuration initiale. Cette rubrique aussi décrit comment supprimer l'application de l'ordinateur.

### DANS CETTE SECTION



## PROCEDURE D'INSTALLATION

L'installation de Kaspersky Internet Security s'opère en mode interactif à l'aide d'un Assistant d'installation.

L'Assistant se compose d'une série de fenêtres (étapes) entre lesquelles vous pouvez naviguer grâce aux boutons **Précédent** et **Suivant**. Pour quitter l'Assistant, cliquez sur le bouton **Terminer**. Pour interrompre l'Assistant à n'importe quelle étape, cliquez sur le bouton **Annuler**.

Si l'application est utilisée pour la protection de plus d'un ordinateur, elle sera installée de la même manière sur tous les ordinateurs. Notez que dans ce cas, la durée de validité de la licence commence à courir à partir de la première activation de l'application, conformément aux termes du contrat de licence. Au moment d'activer l'application pour la protection d'un deuxième ordinateur et des ordinateurs suivants, la durée de validité de la licence sera réduite du nombre de jour écoulés depuis la date de la première activation de l'application. Ainsi, la licence arrivera à échéance le même jour pour toutes les copies de l'application.

- *Pour installer Kaspersky Internet Security sur votre ordinateur,*

  exécutez le fichier d'installation (fichier avec extension *.exe) sur le CD de l'application.

La procédure d'installation de Kaspersky Internet Security depuis une version téléchargée via Internet est en tout point identique à la procédure d'installation depuis le CD.

**DANS CETTE SECTION**



# ETAPE 1. RECHERCHER D'UNE VERSION PLUS RECENTE DE L'APPLICATION

Avant l'installation, Kaspersky Internet Security vérifie la présence de l'application plus récente sur les serveurs de mises à jour de Kaspersky Lab.

Si les serveurs de Kaspersky Lab n'hébergent pas une version plus récente, l'Assistant d'installation de la version actuelle est lancé.

Si les serveurs de mises à jour hébergent une version plus récente, vous serez invité à la télécharger et à l'installer sur votre ordinateur. Si vous refusez d'installer la version plus récente, l'Assistant d'installation de la version actuelle sera lancé. Si vous décidez d'installer la nouvelle version, les fichiers de la distribution seront copiés sur l'ordinateur et l'Assistant d'installation de la nouvelle version sera lancé automatiquement. Pour connaître la suite de l'installation de la version plus récente, lisez la documentation de la version correspondante de l'application.

# ETAPE 2. VERIFICATION DE LA CONFIGURATION DU SYSTEME PAR RAPPORT A LA CONFIGURATION REQUISE

Avant d'installer l'application, le programme vérifie si le système d'exploitation et les paquets de mises à jour (Service Pack) installés correspondent à la configuration requise pour l'installation de Kaspersky Internet Security. (cf. rubrique "Configurations logicielle et matérielle" à la page 27). De plus, l'application vérifie la présence de la configuration requise ainsi que les privilèges pour l'installation du logiciel.

Si une des conditions n'est pas remplie, le message de circonstance apparaîtra. Dans ce cas, avant d'installer l'application de Kaspersky Lab, il est conseillé d'installer les paquets de mises à jour requis à l'aide du service Windows Update ainsi que les applications requises.

Cette étape correspond à la recherche d'applications de Kaspersky Lab dont l'utilisation conjointe avec Kaspersky Internet Security pourrait provoquer des conflits. Si de telles applications sont découvertes, vous pourrez les supprimer manuellement.

Si la liste des applications contient une version antérieure de Kaspersky Anti-Virus ou de Kaspersky Internet Security, toutes les données qui peuvent être utilisées par Kaspersky Internet Security 2011 (informations sur l'activation, paramètres de l'application, etc.) seront enregistrées et utilisées pendant l'installation.

## ETAPE 3. SELECTION DU TYPE D'INSTALLATION

Cette étape de l'installation permet de choisir le type d'installation de Kaspersky Internet Security qui vous convient le mieux :

- *Installation standard*. Si vous choisissez cette option (la case **Modifier les paramètres d'installation** n'est pas cochée), l'application sera complètement installée sur l'ordinateur, avec les paramètres recommandés par les experts de Kaspersky Lab.

- *Installation avec possibilité de modification des paramètres*. Dans ce cas (la case **Modifier les paramètres d'installation est installée**), vous pourrez indiquer le dossier dans lequel l'application doit être installée (cf. rubrique "Etape 7. Sélection du dossier d'installation" à la page 32), et si nécessaire, activer la protection du processus d'installation (cf. rubrique "Etape 8. Préparation de l'installation" à la page 32).

Afin de poursuivre l'installation, cliquez sur **Suivant**.

## ETAPE 4. LECTURE DU CONTRAT DE LICENCE

Au cours de cette étape, vous devez prendre connaissance du contrat de licence conclu entre vous et Kaspersky Lab.

Lisez attentivement le contrat et si vous en acceptez toutes les dispositions, cliquez sur **J'accepte**. L'installation de l'application se poursuivra.

Si vous ne souhaitez pas poursuivre l'application, cliquez sur **Annuler**.

## ETAPE 5. REGLEMENT D'UTILISATION DE KASPERSKY SECURITY NETWORK

Cette étape est une invitation à participer au programme Kaspersky Security Network. La participation au programme implique l'envoi à Kaspersky Lab, Ltd. d'informations sur les nouvelles menaces découvertes sur l'ordinateur, sur les applications exécutées et sur les applications signées téléchargées, ainsi que l'envoi d'un identifiant unique attribué à votre copie de Kaspersky Internet Security et d'informations relatives au système. Aucune donnée personnelle n'est transmise.

Lisez les dispositions relatives à l'utilisation de Kaspersky Security Network. Si vous êtes d'accord avec tous les points, cochez la case **J'accepte les conditions de participation à Kaspersky Security Network**.

Cliquez sur le bouton **Suivant**, si vous exécutez l'installation avec possibilité de modification des paramètres (cf. la rubrique Etape 3. Sélection du type d'installation" à la page 31). Pour l'installation standard, cliquez sur le bouton **Installer**. L'installation continuera.

## ETAPE 6. RECHERCHE D'APPLICATIONS INCOMPATIBLES

Au cours de cette étape, le programme d'installation recherche des applications incompatibles avec Kaspersky Internet Security.

Si ces applications n'existent pas, l'Assistant passe automatiquement à l'étape suivante.

Si des applications incompatibles sont détectées, une liste sera affichée sur l'écran et vous aurez la possibilité de les supprimer automatiquement ou manuellement. Au cours de la suppression des applications incompatibles, le redémarrage du système sera requis. Ensuite, l'installation de Kaspersky Internet Security se poursuivra automatiquement.

Afin de poursuivre l'installation, cliquez sur **Suivant**.

# ETAPE 7. SELECTION DU DOSSIER D'INSTALLATION

Cette étape de l'Assistant d'installation est proposée uniquement en cas d'installation avec possibilité de modification des paramètres (cf. rubrique Etape 3. Sélection du type d'installation" à la page 31). Cette étape est sautée pendant l'installation standard et l'application est installée dans le dossier par défaut.

Cette étape correspond à la sélection du dossier dans lequel Kaspersky Internet Security sera installé. Le chemin d'accès suivant est proposé par défaut :

- **<disque> \ Program Files \ Kaspersky Lab \ Kaspersky Internet Security 2011** pour les systèmes 32 bits ;
- **<disque> \ Program Files (x86) \ Kaspersky Lab \ Kaspersky Internet Security 2011** pour les systèmes 64 bits.

Pour installer Kaspersky Internet Security dans un autre dossier, saisissez le nouveau chemin d'accès dans le champ ou cliquez sur le bouton **Parcourir** et choisissez le dossier dans la fenêtre qui s'ouvre.

Le chemin d'accès au dossier d'installation doit compter moins de 200 caractères et ne peut pas contenir les caractères suivants ****, **/**, **?**, **:**, *****, **"**, **>**, **<** et **|**

Si vous souhaitez savoir si vous disposez d'assez de place sur le disque pour installer l'application, cliquez sur **Disque**. La fenêtre qui s'ouvre fournit les informations relatives à l'espace disque. Cliquez sur **OK** pour fermer la fenêtre.

Pour poursuivre l'installation, cliquez sur le bouton **Suivant** dans la fenêtre de l'Assistant.

# ETAPE 8. PREPARATION DE L'INSTALLATION

Cette étape de l'Assistant d'installation est proposée uniquement en cas d'installation avec possibilité de modification des paramètres (cf. rubrique Etape 3. Sélection du type d'installation" à la page 31). Lors de l'installation standard, cette étape est ignorée.

Dans la mesure où des applications malveillantes capables de gêner l'installation de Kaspersky Internet Security pourraient être présentes sur l'ordinateur, le processus d'installation doit être protégé.

Par défaut, la protection du processus d'installation est activée : la case **Protéger l'installation de l'application** est cochée dans la fenêtre de l'Assistant.

Il est conseillé de décocher cette case s'il est impossible d'exécuter l'installation de l'application (par exemple, lors de l'installation à distance via Windows Remote Desktop). La protection activée peut en être la cause.

Dans ce cas, interrompez l'installation et relancez l'installation de l'application dès le début, cochez la case **Modifier les paramètres d'installation** à l'étape Choix du type d'installation (cf. rubrique "Etape 3. Sélection du type d'installation" à la page 31), et, à l'étape Préparation de l'installation, décochez la case **Protéger l'installation de l'application**.

Afin de poursuivre l'installation, cliquez sur **Installer**.

Lors de l'installation de l'application sur un ordinateur fonctionnant sous le système d'exploitation Microsoft Windows XP, les connexions de réseau en cours seront interrompues. La majorité des connexions interrompues seront rétablies après un certain temps.

## ETAPE 9. INSTALLATION

L'installation de l'application dure un certain temps. Attendez jusque la fin.

Une fois l'installation terminée, l'Assistant passe automatiquement à l'étape suivante.

En cas d'erreurs d'installation qui pourraient être provoquées par la présence sur l'ordinateur de programmes malveillants empêchant l'installation de logiciels antivirus, l'Assistant d'installation proposera de télécharger un outil spécial pour éliminer l'infection : *l'utilitaire Kaspersky Virus Removal Tool*.

Si vous êtes d'accord avec l'installation de l'utilitaire, l'Assistant le téléchargera depuis les serveurs de Kaspersky Lab. Ensuite, l'installation de l'utilitaire sera lancée automatiquement. Si l'Assistant ne parvient pas à télécharger l'utilitaire, vous aurez la possibilité de le télécharger vous-même en cliquant sur le lien proposé.

Une fois que l'utilitaire aura terminé son travail, il faut le supprimer et lancer l'installation de Kaspersky Internet Security dès le début.

## ETAPE 10. ACTIVATION DE L'APPLICATION

L'*activation* est une procédure qui correspond à l'entrée en vigueur d'une licence. Cette licence donne le droit d'utiliser la version commerciale de l'application pendant la durée de validité de la licence.

Une connexion à Internet est indispensable pour activer l'application.

Vous pouvez choisir parmi les options suivantes pour activer Kaspersky Internet Security :

- **Activer la version commerciale**. Choisissez cette option et saisissez le code d'activation (cf. section "Présentation du code d'activation" à la page 38) si vous avez acheté la version commerciale de l'application.

  Si vous saisissez le code d'activation de Kaspersky Anti-Virus, la procédure de permutation sur Kaspersky Anti-Virus sera lancée à la fin de l'activation.

- **Activer la version d'évaluation**. Sélectionnez cette option si vous souhaitez installer une version d'évaluation du logiciel avant de décider d'acheter la version commerciale. Vous pouvez utiliser toutes les fonctionnalités de l'application pendant la période définie par la licence de la version d'évaluation. Après la date d'expiration de la licence, vous ne pourrez plus activer à nouveau la version d'évaluation.

- **Activer plus tard**. Si vous choisissez cette option, l'activation de Kaspersky Internet aura lieu plus tard. L'application sera installée et vous aurez accès à toutes les fonctions, sauf la mise à jour. Les bases antivirus et les modules de Kaspersky Internet Security pourront être actualisés une seule fois uniquement après l'installation. L'option **Activer plus tard** est accessible uniquement au premier lancement de l'Assistant d'activation, juste après l'installation de l'application.

Si Kaspersky Internet Security avait été installé puis supprimé avec l'enregistrement des données relatives à l'activation, alors cette étape est passée. Dans ce cas, l'Assistant obtient automatiquement les données relatives à la licence existante et passe à l'étape finale de l'activation (cf. la rubrique Etape 12. Fin de l'activation" à la page 34).

## ETAPE 11. ENREGISTREMENT DE L'UTILISATEUR

Cette étape est accessible uniquement lors de l'activation de la version commerciale de l'application. Lors de l'activation de la version d'évaluation, cette étape est passée.

Si vous souhaitez pouvoir demander l'aide du Service d'assistance technique de Kaspersky Lab, il faudra vous enregistrer. Les utilisateurs non enregistrés de l'application bénéficient d'une assistance minimum.

Si vous acceptez de vous enregistrer, saisissez les données requises dans les champs correspondants, puis cliquez sur le bouton **Suivant**.

## ETAPE 12. FIN DE L'ACTIVATION

L'Assistant vous signale la réussite de l'activation de Kaspersky Internet Security. Il propose également des informations sur la licence : type (commerciale, évaluation, etc.), fin de validité de la licence et nombre d'ordinateurs couverts par cette licence.

En cas d'activation de l'abonnement, les informations relatives à la durée de validité de la licence sont fournies en plus des informations sur l'état de l'abonnement (cf. section "Etats de l'abonnement" à la page 203).

Cliquez sur le bouton **Suivant** afin de poursuivre l'Assistant.

## ETAPE 13. ANALYSE DU SYSTEME

Cette étape correspond à la collecte d'informations sur les applications reprises dans Microsoft Windows. Ces applications figurent dans la liste des applications de confiance et elles ne sont soumises à aucune restriction sur les actions qu'elles peuvent réaliser dans le système.

Une fois l'analyse terminée, l'Assistant passe automatiquement à l'étape suivante.

## ETAPE 14. FIN DE L'ASSISTANT

La dernière fenêtre de l'Assistant vous signale la fin de l'installation de l'application. Pour commencer à utiliser Kaspersky Internet Security, assurez-vous que la case **Lancer Kaspersky Internet Security** est cochée puis cliquez sur le bouton **Terminer**.

Dans certains cas, le redémarrage du système d'exploitation peut être requis. Si la case **Lancer Kaspersky Internet Security** est cochée, l'application sera lancée automatiquement après le redémarrage.

Si, avant la fin de l'Assistant, vous avez décoché la case, l'application doit être lancée manuellement (cf. rubrique "Lancement et arrêt manuels de l'application" à la page 48).

# PREMIERE UTILISATION

Après l'installation et la configuration, l'application est prête à l'emploi. Pour garantir le niveau de protection adéquat de l'ordinateur, exécutez les opérations suivantes directement après l'installation et la configuration de l'application :

- Mise à jour les bases de l'application (cf. rubrique "Procédure de mise à jour des bases de l'application" à la page 56).
- Rechercher la présence éventuelle de virus (cf. rubrique "Procédure d'exécution d'une analyse complète de l'ordinateur" à la page 59), et de vulnérabilités (cf. rubrique "Procédure de recherche de vulnérabilités sur l'ordinateur" à la page 59) sur l'ordinateur.

- Vérifier l'état de la protection de l'ordinateur (à la page 49) et, le cas échéant, éliminer les problèmes de protection (cf. rubrique "Diagnostic et suppression des problèmes dans la protection de l'ordinateur" à la page 49).

# SUPPRESSION DE L'APPLICATION

Suite à la suppression de Kaspersky Internet Security, l'ordinateur et vos données personnelles ne seront plus protégés !

La suppression de Kaspersky Internet Security s'effectue à l'aide de l'Assistant d'installation.

*Pour lancer l'Assistant, procédez comme suit :*

1. Dans le menu **Démarrer**, sélectionnez le point **Applications** → **Kaspersky Internet Security 2011** → **Restauration ou suppression**.

2. Dans la fenêtre qui s'ouvre, cliquez sur **Supprimer**.

## DANS CETTE SECTION



# ETAPE 1. ENREGISTREMENT DE DONNEES POUR UNE REUTILISATION

A cette étape vous pouvez indiquer les données de l'application que vous voulez enregistrer pour l'utilisation suivante lors de la réinstallation de l'application (par exemple, sa version plus récente).

Par défaut, l'application est supprimée entièrement de l'ordinateur.

*Pour enregistrer les données en vue de leur réutilisation, procédez comme suit :*

1. Sélectionnez l'option **Enregistrer les objets de l'application**.

2. Cochez les cases en regard des données à enregistrer :

   - **Informations sur l'activation** : données permettant de ne pas activer ultérieurement l'application à installer, mais d'utiliser automatiquement la licence actuelle, à condition qu'elle soit toujours valable au moment de l'installation.

   - **Base Anti-Spam** : bases contenant les modèles des messages non sollicités reçus et enregistrés durant le travail.

   - **Objets de la sauvegarde ou de la quarantaine** : fichiers analysés par l'application et placés dans la sauvegarde ou en quarantaine.

   - **Paramètres** de **fonctionnement de l'application** : valeurs des paramètres de fonctionnement de l'application. Ces paramètres sont définis au cours de la configuration de l'application.

   - **Données iSwift et iChecker** : fichiers contenant les informations sur les objets déjà analysés sur les virus.

   - **Données du dossier virtuel de l'environnement protégé** : fichiers enregistrés dans un dossier spécial lors du fonctionnement dans l'Environnement protégé. Ce dossier est aussi disponible dans l'environnement normal.

## ETAPE 2. CONFIRMATION DE LA SUPPRESSION DU PROGRAMME

Dans la mesure où la suppression de l'application met en danger la protection de l'ordinateur et de vos données personnelles, vous devez confirmer la suppression de l'application. Pour ce faire, cliquez sur le bouton **Supprimer**.

Vous pouvez à tout moment annuler cette action, au cours de celle-ci, en cliquant sur le bouton **Annuler**.

## ETAPE 3. SUPPRESSION DE L'APPLICATION. FIN DE LA SUPPRESSION

Cette étape de l'Assistant correspond à la suppression de l'application de l'ordinateur. Attendez la fin du processus de suppression.

La suppression peut requérir le redémarrage du système d'exploitation. Si vous décidez de reporter le redémarrage, la fin de la procédure de suppression sera reportée jusqu'au moment où le système d'exploitation sera redémarré ou quand l'ordinateur sera allumé et éteint.

# GESTIONNAIRE DE LICENCES

Cette rubrique contient les informations sur les notions générales utilisées dans le contexte de l'octroi de licences de l'application. Dans cette rubrique, vous apprendrez également comment prolonger automatiquement la durée de validité de la licence et où trouver les informations sur la licence actuelle.

### DANS CETTE SECTION



## 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 Internet Security et Kaspersky Lab, Ltd. Ce contrat figure dans chaque application de Kaspersky Lab. Il reprend des informations détaillées sur les droits et les restrictions d'utilisation de Kaspersky Internet Security

Conformément au contrat de licence, en achetant et en installant l'application de Kaspersky Lab, vous obtenez le droit illimité de posséder une copie.

## PRESENTATION DE LA LICENCE

*La licence* représente le droit d'utiliser Kaspersky Internet Security et les services complémentaires associés offerts par Kaspersky Lab ou ses partenaires.

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

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

- Assistance technique ;
- Mise à jour des bases et des modules de l'application.

Les services offerts dépendent du type de licence.

Les types suivants de licences sont prévus :

- *Evaluation* : licence gratuite à durée de validité réduite (par exemple, 30 jours) qui permet de découvrir Kaspersky Internet Security.

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

  La licence d'évaluation est proposée avec la version d'évaluation de l'application. La licence d'évaluation vous permet de contacter le service d'assistance technique uniquement pour les questions en rapport avec l'activation de l'application ou l'achat d'une licence commerciale. Une fois que la validité de la licence

d'évaluation est écoulée, Kaspersky Internet Security arrête de remplir toutes ces fonctions. Pour continuer à utiliser l'application, il faut l'activer (cf. section "Procédure d'activation de l'application" à la page 54).

- *La licence commerciale* est une licence payante avec une durée de validité limitée (par exemple, un an) octroyée à l'achat de Kaspersky Internet Security. Une licence peut être appliquée à plusieurs ordinateurs.

  Pendant la durée de validité de la licence commerciale, toutes les fonctionnalités de l'application et les services complémentaires sont accessibles.

  À l'issue de la période de validité de la licence commerciale, Kaspersky Internet Security continue à remplir toutes ses fonctions, à l'exception de la mise à jour des bases antivirus. Vous pouvez continuer à lancer des analyses de l'ordinateur ou utiliser les composants de la protection, mais uniquement avec les bases qui étaient d'actualité à l'expiration de la licence. Deux semaines avant l'expiration de la licence, l'application enverra une notification et vous aurez la possibilité de prolonger la durée de validité de la licence (cf. section "Procédure d'achat ou de renouvellement de la licence" à la page 55).

- *La licence commerciale avec abonnement à la mise à jour* ou *la licence commerciale avec abonnement à la mise à jour et à la protection* est une licence payante qui propose une administration souple : il est possible de suspendre et de reprendre l'abonnement, de le prolonger en mode automatique ou de le supprimer. La licence avec abonnement est distribuée via les prestataires de service. L'administration de l'abonnement s'opère via l'espace personnel de l'utilisateur sur le site du prestataire de services.

  L'abonnement peut être à durée déterminée (par exemple, un an) ou indéterminée. L'abonnement à durée déterminée devra être reconduit manuellement à l'échéance. L'abonnement à durée indéterminée est prolongé automatiquement si le paiement du prestataire a été réalisé à temps.

  Si la durée de l'abonnement est déterminée, vous bénéficierez d'une période de grâce à l'échéance de la validité pour le renouveler. Au cours de cette période, le fonctionnement de l'application sera préservé.

  Si l'abonnement n'a pas été reconduite, à l'issue de la période de grâce Kaspersky Internet Security ne réalisera plus la mise à jour des bases (pour les licences avec abonnement à la mise jour) et arrêtera également d'assurer la protection de l'ordinateur ou de lancer une tâche d'analyse (pour les licences avec abonnement à la mise à jour et à la protection).

  Si vous utilisez un abonnement, vous ne pourrez pas utiliser un autre code d'activation pour prolonger la durée de validité de la licence. Cela sera possible uniquement à l'échéance de l'abonnement.

  Si au moment d'activer l'abonnement vous aviez déjà activé la licence à durée déterminée, elle sera remplacée par la licence avec abonnement. Pour arrêter l'abonnement, il faut contacter le prestataire de services où vous avez acheté Kaspersky Internet Security.

  En fonction du fournisseur de l'abonnement, la sélection d'actions possibles avec l'abonnement (cf. section "Etats de l'abonnement" à la page 203) peut varier. De plus, il se peut que la période de grâce au cours de laquelle le prolongement de l'abonnement est possible ne soit pas offerte.

# PRESENTATION DU CODE D'ACTIVATION

*Le code d'activation* est un code que vous recevez après l'achat de la licence commerciale de Kaspersky Internet 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.

Si vous avez acheté l'application en ligne, vous recevrez le code d'activation par courrier électronique. Si vous avez acheté l'application en magasin, le code d'activation est imprimé sur la pochette contenant le cédérom d'installation ou sous le film de protection collé à l'intérieur de la boîte contenant le disque d'installation.

# CONSULTATION DES INFORMATIONS SUR LA LICENCE

*Pour consulter les informations sur la licence en cours, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.

2. Cliquez sur le lien **Licence** dans la partie inférieure de la fenêtre pour ouvrir la fenêtre **Gestionnaire de licences**.

   Cette fenêtre permet de lancer la procédure d'activation de l'application (cf. section "Procédure d'activation de l'application" à la page 54), d'achat d'une nouvelle licence ou de renouvellement de la durée de validité de la licence en cours (cf. section "Procédure d'achat ou de renouvellement de la licence" à la page 55).

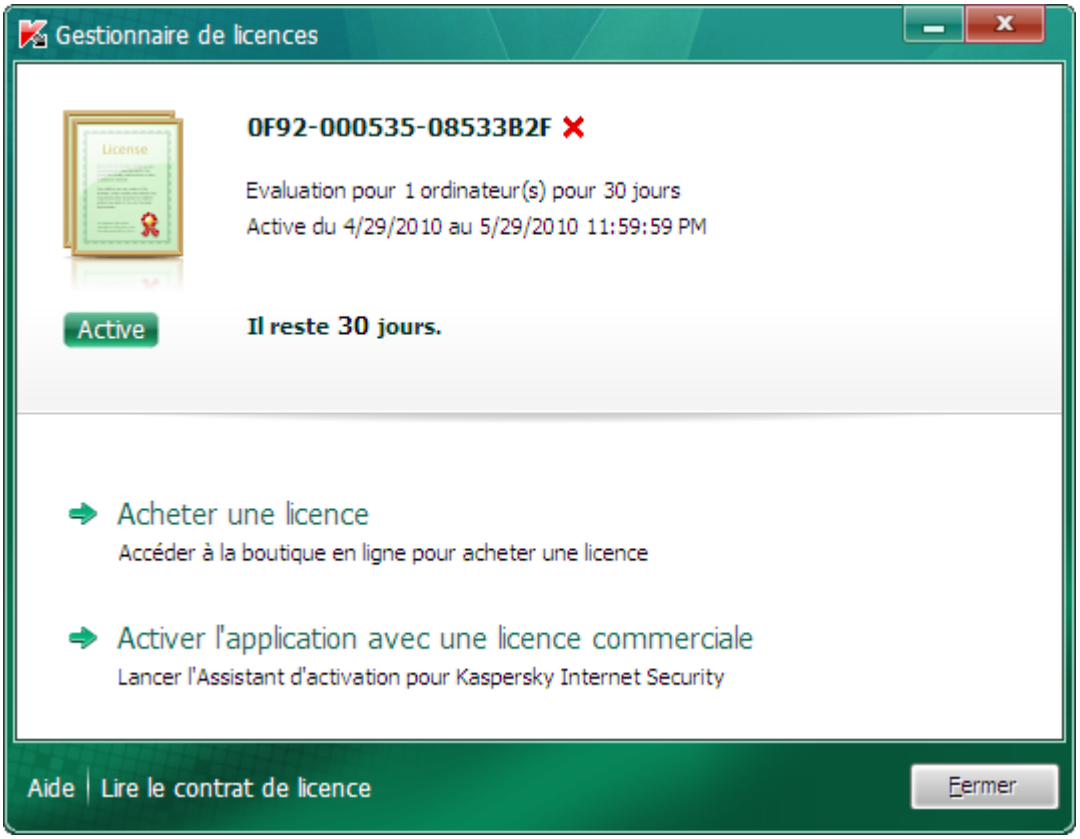



*Illustration 1. Fenêtre Gestionnaire de licences*

# INTERFACE DE L'APPLICATION

L'interface de Kaspersky Internet Security est simple et conviviale. Cette rubrique aborde en détail les éléments principaux de l'interface.

Kaspersky Internet Security possède des plug-ins pour Microsoft Office Outlook, Microsoft Outlook Express, The Bat!, Thunderbird, Mozilla Firefox, Microsoft Internet Explorer et Microsoft Windows Explorer. Les plug-ins élargissent les possibilités des programmes cités et permettent de configurer, depuis leur interface, les paramètres des composants de l'application.

### DANS CETTE SECTION



# ICONE DANS LA ZONE DE NOTIFICATION

L'icône de l'application apparaît dans la zone de notification de la barre des tâches de Microsoft Windows directement après son installation.

Dans le système d'exploitation Microsoft Windows 7, l'icône de l'application est dissimulée par défaut. Pour utiliser l'application, vous pouvez l'afficher (cf. la documentation du système d'exploitation).

L'icône remplit les fonctions fondamentales suivantes :

- Elle indique le fonctionnement de l'application ;
- Elle permet d'accéder au menu contextuel, à la fenêtre principale de l'application et à la fenêtre de consultation des nouvelles.

### Indication du fonctionnement de l'application

L'icône indique le fonctionnement de l'application. Elle représente l'état de la protection et montre également plusieurs actions fondamentales exécutées par l'application à l'heure actuelle :

 – analyse d'un message en cours ;

 – analyse du trafic Web en cours ;

 – mise à jour des bases et des modules des applications en cours ;

 – redémarrage de l'ordinateur requis pour appliquer les mises à jour ;

 – échec du fonctionnement d'un composant quelconque de l'application.

L'animation de l'icône est activée par défaut : par exemple, lors de l'analyse du message, l'icône miniature d'un message pulse sur le fond de l'icône de l'application, et lors de la mise à jour des bases de l'application, l'icône du globe tourne. Vous pouvez désactiver l'animation (cf. section "Eléments actifs de l'interface" à la page 190).

Si l'animation est désactivée, l'icône peut prendre un des aspects suivants :

 (icône de couleur) : tous les composants de la protection ou certains d'entre eux fonctionnent ;

 (icône noire et blanche) : tous les composants de la protection sont désactivés.

### Accès au menu contextuel et aux fenêtres de l'application.

L'icône permet d'ouvrir le menu contextuel (à la page 41) et la fenêtre principale de l'application (cf. rubrique "Fenêtre principale de Kaspersky Internet Security" à la page 42).

- *Pour ouvrir le menu contextuel,*

  placez le curseur sur l'icône, puis cliquez avec le bouton droit de la souris.

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

  placez le curseur sur l'icône, puis cliquez avec le bouton gauche de la souris.

L'icône  apparaît dans la barre des tâches de Microsoft Windows lorsque des infos sont émises par Kaspersky Lab. La fenêtre Kiosque d'informations (cf. rubrique "Kiosque d'informations" à la page 190) s'ouvre d'un double-clique sur cette icône.

# MENU CONTEXTUEL

Le menu contextuel permet d'exécuter toutes les tâches principales liées à la protection.

Le menu de Kaspersky Internet Security contient les points suivants :

- **Outils** : ouvre un sous-menu contenant les options suivantes :
  - **Contrôle des Applications** : ouvre la fenêtre **Surveillance des Applications** ;
  - **Surveillance du réseau** : ouvre la fenêtre **Surveillance du réseau** ;
  - **Clavier virtuel** : affiche le clavier virtuel.
- **Exécution des applications en mode protégé** : lance l'environnement protégé pour l'exécution des applications qui, d'après vous peuvent être dangereuses. Si l'Environnement Protégé est déjà lancé, l'utilisateur passe dans cet environnement.

  Pendant l'utilisation de l'Environnement Protégé, cette option du menu devient **Dans l'environnement principal** et permet de revenir dans l'environnement principal du système d'exploitation.
- **Kaspersky Internet Security** : ouvre la fenêtre principale de l'application.
- **Suspension de la protection/Lancement de la protection** : suspend temporairement/active le composant de la protection en temps réel. Cette option du menu n'a aucune influence sur la mise à jour de l'application, ni sur l'exécution de la recherche de virus.
- **Activer Contrôle Parental/Désactiver Contrôle Parental** : active/désactive le Contrôle Parental pour le compte utilisateur en cours.

- **Configuration** : ouvre la fenêtre de configuration de l'application.
- **A propos du programme** : ouvre la fenêtre contenant les informations relatives à l'application.
- **Infos** : ouvre la fenêtre du kiosque d'informations (cf. section "Kiosque d'informations" à la page 190). Cette option est visible uniquement lorsqu'il y a des informations non lues.
- **Quitter** : arrêt du fonctionnement de Kaspersky Internet Security (si vous choisissez cette option, l'application sera déchargée de la mémoire vive de l'ordinateur).

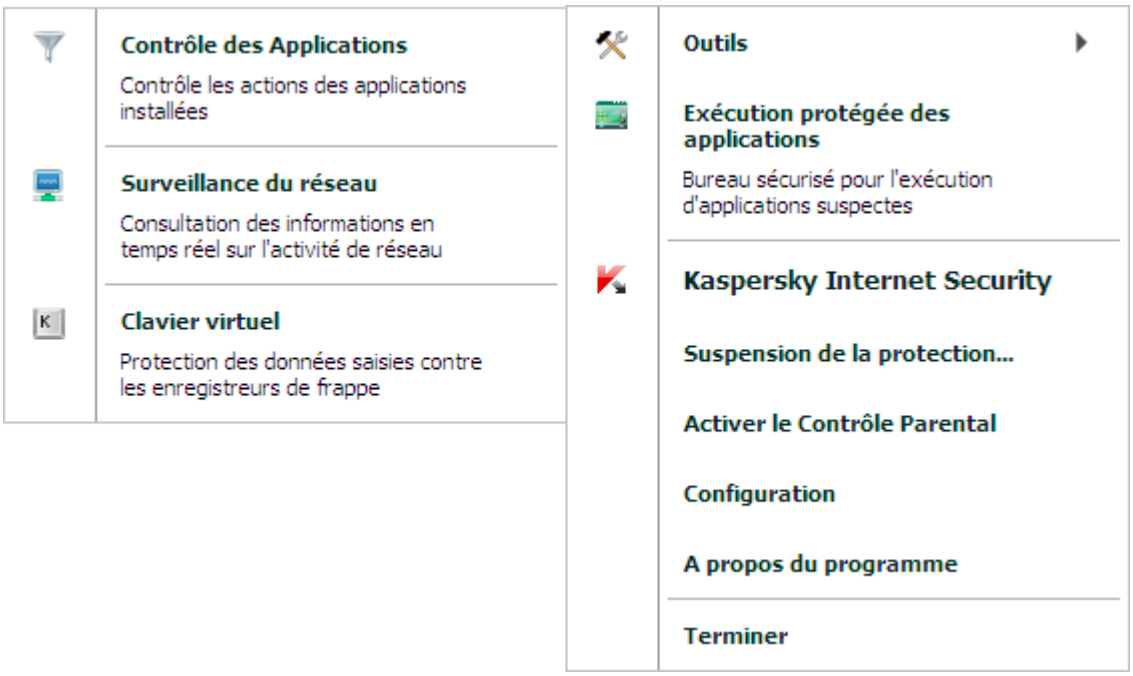



*Illustration 2. Menu contextuel*

Si une tâche quelconque de recherche de virus ou de mise à jour est lancée quand vous ouvrez le menu contextuel, son nom apparaît dans le menu contextuel accompagné de la progression en pour cent. Après avoir sélectionné une tâche, vous pouvez passer à la fenêtre principale présentant le rapport avec les résultats détaillés de l'exécution.

*Pour ouvrir le menu contextuel,*

placez le curseur sur l'icône de l'application dans la zone de notification de la barre des tâches, puis cliquez avec le bouton droit de la souris.

Dans le système d'exploitation Microsoft Windows 7, l'icône de l'application est dissimulée par défaut. Pour utiliser l'application, vous pouvez l'afficher (cf. la documentation du système d'exploitation).

# FENETRE PRINCIPALE DE KASPERSKY INTERNET SECURITY

La fenêtre principale de l'application reprend les éléments de l'interface qui permettent d'accéder à l'ensemble des fonctions principales de l'application.

La fenêtre principale est scindée en trois parties :

- La partie supérieure reprend l'indicateur de l'état de la protection qui indique l'état actuel de la protection de votre ordinateur.

*Illustration 3. Etat actuel de la protection de l'ordinateur*

Il existe trois états possibles pour la protection. Chacun d'entre eux est associé à une couleur. Le vert indique que la protection de l'ordinateur est assurée au niveau requis. Le jaune et le rouge signalent la présence de menaces de divers types pour la sécurité. Les menaces sont non seulement les applications malveillantes, mais également les bases de l'application dépassées, certains composants désactivés, les paramètres minimes de fonctionnement de l'application, etc.

Il faut remédier aux menaces pour la sécurité au fur et à mesure qu'elles se présentent (cf. rubrique "Diagnostic et suppression des problèmes dans la protection de l'ordinateur" à la page 49).

- La partie gauche de la fenêtre permet d'accéder rapidement aux fonctions principales de l'application : activation et désactivation des composants de la protection, exécution des tâches d'analyse, mise à jour des bases et des modules de l'application, etc.


*Illustration 4. Partie gauche de la fenêtre principale*

- La partie droite de la fenêtre contient des informations relatives à la fonction de l'application choisie dans la partie gauche. Vous pouvez aussi configurer les paramètres de la fonction, utiliser des outils pour exécuter les recherches de virus et la récupération des mises à jour, etc.

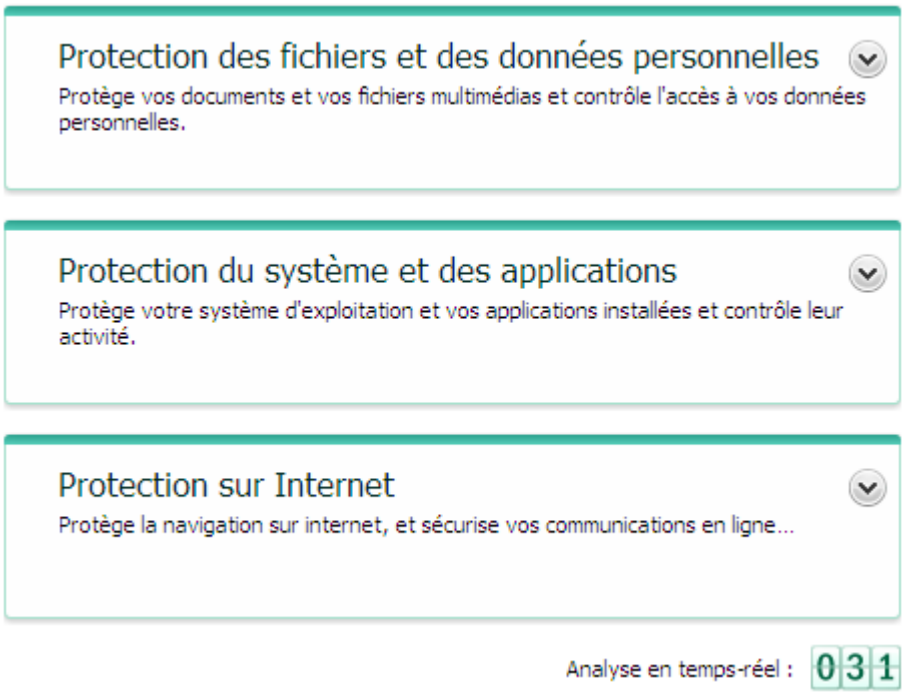



*Illustration 5. Partie droite de la fenêtre principale*

Vous pouvez également cliquer sur les boutons et les liens suivants :

- **Configuration** : ouvre la fenêtre de configuration des paramètres de l'application.
- **Quarantaine** : passe à la manipulation des objets placés en quarantaine.
- **Rapports** : ouvre le rapport sur le fonctionnement de l'application, présenté sous la forme d'un diagramme.
- **Infos** : affiche les dernières nouvelles dans la fenêtre du kiosque d'informations (cf. rubrique "Kiosque d'informations" à la page 190). Le lien apparaît après que l'application a reçu les premières informations.
- **Aide** : ouvre le système d'aide de l'application.
- **Mon Espace Personnel** : ouvre l'espace personnel de l'utilisateur sur le site web du service d'assistance technique (cf. rubrique "Mon Espace Personnel" à la page 198).
- **Assistance technique** : ouvre la fenêtre contenant les informations relatives au système et les liens vers les sources d'informations de Kaspersky Lab (site du service d'assistance technique, forum).
- **Licence** : passe à l'activation de Kaspersky Internet Security et au renouvellement de la licence.

Vous pouvez modifier l'aspect de Kaspersky Internet Security à l'aide de skins (cf. section "Apparence de l'application" à la page 189).

*Pour ouvrir la fenêtre principale de l'application, réalisez une des opérations suivantes :*

- placez le curseur sur l'icône de l'application dans la zone de notification de la barre des tâches, puis cliquez avec le bouton gauche de la souris.

Dans le système d'exploitation Microsoft Windows 7, l'icône de l'application est dissimulée par défaut. Pour utiliser l'application, vous pouvez l'afficher (cf. la documentation du système d'exploitation).

- Choisissez l'option **Kaspersky Internet Security** dans le menu contextuel (cf. rubrique "Menu contextuel" à la page 41) ;

- Cliquez sur l'icône de Kaspersky Internet Security, située au centre de Kaspersky Gadget (uniquement pour les systèmes d'exploitation Microsoft Windows Vista et Microsoft Windows 7).

# FENETRE DES NOTIFICATIONS

Lorsqu'un événement survient durant l'utilisation de Kaspersky Internet Security, des notifications apparaissent à l'écran sous la forme de messages contextuels au-dessus de l'icône de l'application dans la barre des tâches de Microsoft Windows.

En fonction du degré d'importance de l'événement (au niveau de la sécurité de l'ordinateur), les notifications peuvent être de divers type :

- Critiques : signalent des événements d'une importance capitale du point de vue de la sécurité de l'ordinateur (par exemple : découverte d'un objet malveillant ou d'une activité dangereuse dans le système). Quand un tel message apparaît, il faut impérativement décider de la suite des événements. La fenêtre de ce genre de notification est rouge.

- Importantes : signalent des événements potentiellement importants du point de vue de la sécurité de l'ordinateur (par exemple : découverte d'un objet potentiellement infecté ou d'une activité suspecte dans le système). Quand un tel message apparaît, il faut décider du danger que représente l'objet ou le processus découvert et décider de la suite des événements. La fenêtre de ce genre de notification est orange.

- Informatives : signalent des événements qui n'ont pas une importance capitale. La fenêtre de ce genre de notification est verte.

# FENETRE DE CONFIGURATION DES PARAMETRES DE L'APPLICATION

La fenêtre de configuration des paramètres de Kaspersky Internet Security permet de configurer les paramètres de fonctionnement de l'application dans son ensemble, de composants distincts de la protection, de l'analyse et de la mise à jour et d'exécuter d'autres tâches de configuration étendue (cf. rubrique Configuration étendue de l'application à la page 73).

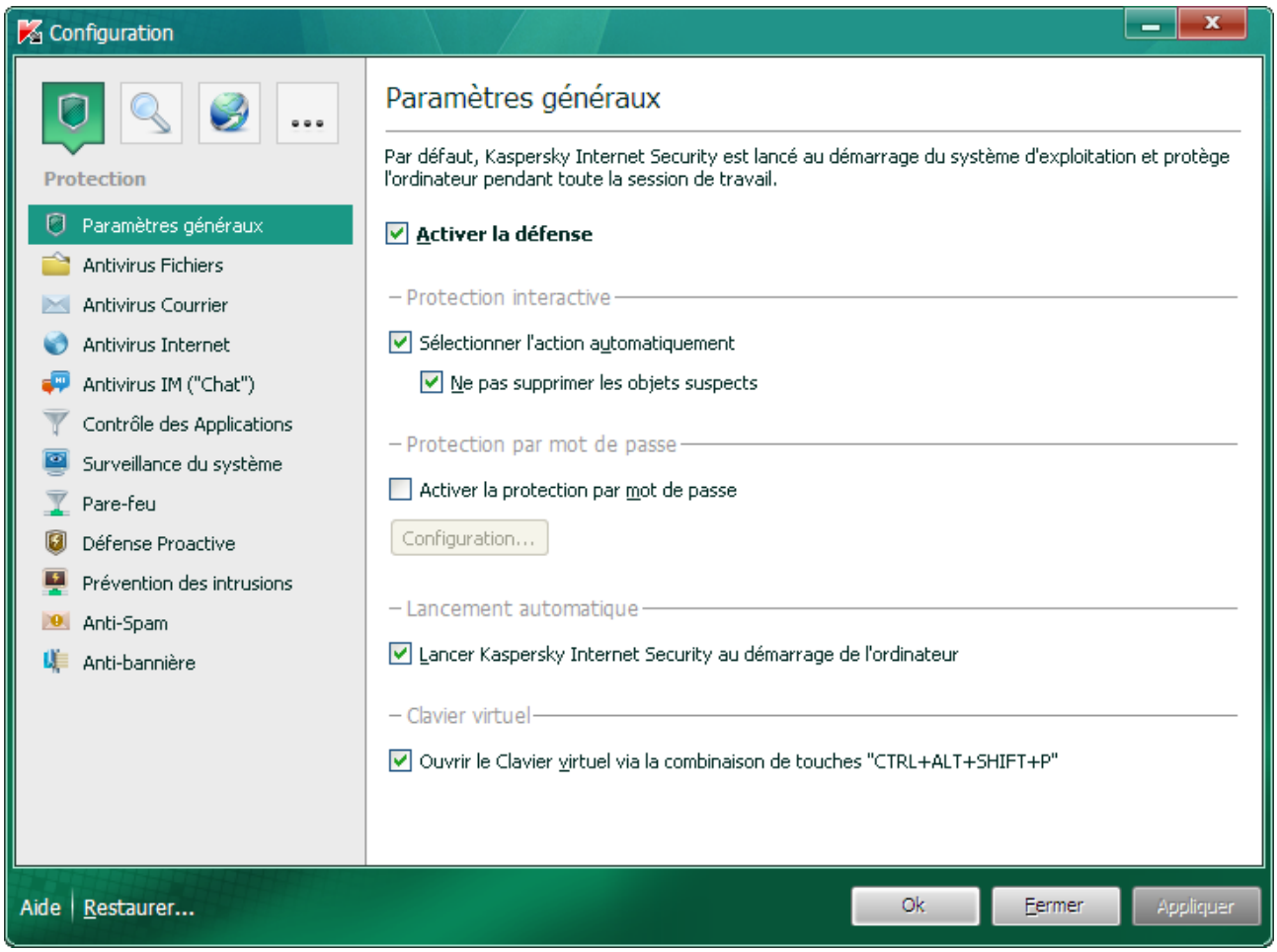



*Illustration 6. Fenêtre de configuration des paramètres de l'application*

La fenêtre de configuration contient deux parties :

- La partie gauche de la fenêtre permet de sélectionner le composant de l'application, la tâche ou tout autre élément qu'il faut configurer ;
- La partie droite de la fenêtre contient les éléments d'administration à l'aide desquels il est possible de configurer le fonctionnement des éléments choisis dans la partie gauche de la fenêtre.

Les composants, les tâches et autres éléments dans la partie gauche sont regroupés en rubrique :

– **Protection** ;

– **Analyse de l'ordinateur** ;

– **Mise à jour** ;

– **Paramètres avancés**.

*Pour ouvrir la fenêtre principale de configuration de l'application, réalisez une des opérations suivantes :*

- Passez au lien **Configuration** dans la partie supérieure de la fenêtre principale de l'application (cf. rubrique "Fenêtre principale de Kaspersky Internet Security" à la page 42) ;
- Choisissez l'option **Configuration** dans le menu contextuel (cf. rubrique "Menu contextuel" à la page 41) ;
- Cliquez sur le bouton avec l'icône **Configuration** dans l'interface de Kaspersky Gadget (uniquement pour les systèmes d'exploitation Microsoft Windows Vista et Microsoft Windows 7). Il faut associer la fonction d'ouverture de la fenêtre de configuration à ce bouton (cf. rubrique "Utilisation de Kaspersky Gadget" à la page 71).

*Pour sélectionner la rubrique requise dans la fenêtre de configuration,*

cliquez sur l'icône de la rubrique qui vous intéresse dans la partie supérieure gauche de la fenêtre (cf. illustration ci-dessus).

# KASPERSKY GADGET

Si vous utilisez Kaspersky Internet Security sur un ordinateur fonctionnant sous le système d'exploitation Microsoft Windows Vista ou Microsoft Windows 7, vous pouvez utiliser Kaspersky Gadget.

Le gadget permet d'accéder rapidement aux fonctions principales de l'application : indication de l'état de la protection de l'ordinateur, analyse des objets, consultation des rapports sur le fonctionnement de l'application, etc.

Le gadget apparaît automatiquement sur le Bureau après l'installation de Kaspersky Internet Security sur un ordinateur fonctionnant sous Microsoft Windows 7. Après l'installation de l'application sur un ordinateur tournant sous Microsoft Windows Vista, le gadget devra être ajouté manuellement au Volet Windows de Microsoft Windows (cf. la documentation du système d'exploitation).

*Illustration 7. Kaspersky Gadget*

# LANCEMENT ET ARRET DE L'APPLICATION

Une fois l'installation terminée, Kaspersky Internet Security est lancé automatiquement. Par la suite, le lancement automatique de l'application au démarrage du système d'exploitation aura lieu par défaut.

### DANS CETTE SECTION



## ACTIVATION ET DESACTIVATION DU LANCEMENT AUTOMATIQUE

Dans ce cas-ci, le lancement automatique de l'application signifie le lancement de Kaspersky Internet Security sans aucune intervention de votre part, directement après le démarrage du système d'exploitation. Ce mode de lancement est activé par défaut.

- *Pour activer ou désactiver le lancement automatique de l'application, procédez comme suit :*

  1. Ouvrez la fenêtre de configuration de l'application.
  2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez la sous-section **Paramètres généraux**.
  3. Pour désactiver le lancement automatique de l'application, dans le groupe **Lancement automatique** de la partie droite de la fenêtre, décochez la case **Lancer Kaspersky Internet Security au démarrage de l'ordinateur**. Pour activer le lancement automatique de l'application, cochez cette case.

## LANCEMENT ET ARRET MANUELS DE L'APPLICATION

Kaspersky Lab déconseille d'arrêter Kaspersky Internet Security car, dans ce cas, l'ordinateur et les données personnelles qu'il contient seront menacés. Si une telle mesure s'impose vraiment, il est conseillé de suspendre la protection pour une période déterminée sans quitter l'application.

Il faut lancer Kaspersky Internet Security manuellement uniquement si vous avez désactivé le lancement automatique de l'application (cf. rubrique "Activation et désactivation du lancement automatique" à la page 48).

- *Pour lancer l'application manuellement,*

  dans le menu **Démarrer** dans le menu et choisissez l'option **Applications** → **Kaspersky Internet Security 2011** → **Kaspersky Internet Security 2011**.

- *Pour quitter l'application,*

  cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel de l'icône de l'application situé dans la zone de notification de la barre des tâches, puis choisissez l'option **Quitter**.

Dans le système d'exploitation Microsoft Windows 7, l'icône de l'application est dissimulée par défaut. Pour utiliser l'application, vous pouvez l'afficher (cf. la documentation du système d'exploitation).

# 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. Cette rubrique explique aussi comment activer ou désactiver la suspension temporaire de la protection pendant l'utilisation de Kaspersky Internet Security.

### DANS CETTE SECTION



## DIAGNOSTIC ET SUPPRESSION DES PROBLEMES DANS LA PROTECTION DE L'ORDINATEUR

L'indicateur d'état de la protection, situé dans la partie supérieure de la fenêtre principale de l'application (cf. rubrique "Fenêtre principale de Kaspersky Internet Security" à la page 42), signale les problèmes qui pourraient survenir dans la protection de l'ordinateur. La couleur de l'indicateur change en fonction de l'état de la protection de l'ordinateur : le vert indique que l'ordinateur est protégé, le jaune signale un problème dans la protection et le rouge indique une menace sérieuse pour la sécurité de l'ordinateur. Il est conseillé d'éliminer immédiatement les problèmes et les menaces sur la sécurité.

*Illustration 8. Etat actuel de la protection de l'ordinateur*

En cliquant sur l'icône de l'indicateur dans la fenêtre principale, vous pouvez ouvrir la fenêtre **Etat de la protection** (cf. ill. ci-après) qui affiche des informations détaillées sur l'état de la protection de l'ordinateur et qui propose diverses solutions pour supprimer les problèmes et les menaces.

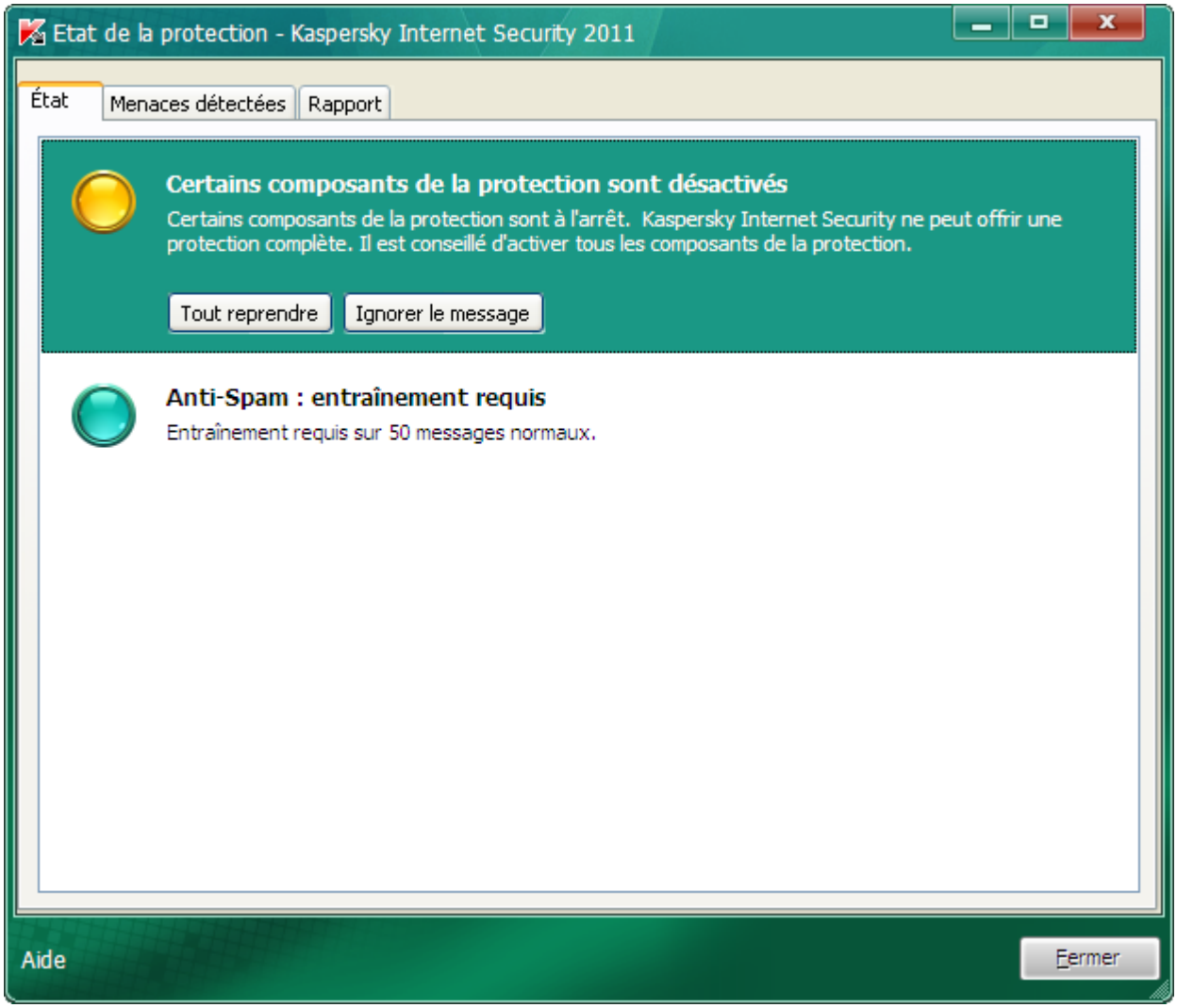



*Illustration 9. Résolution des problèmes de sécurité*

L'onglet **Etat** de la fenêtre **Etat de la protection** reprend la liste des problèmes, y compris les éléments qui provoquent un écart par rapport au fonctionnement optimal de l'application (par exemple, des bases dépassées). Les actions suivantes sont proposées pour supprimer les menaces.

- Résolution immédiate. Les boutons correspondant permettent d'accéder à la résolution directe du problème. Il s'agit de l'action recommandée.

- Reporter la suppression. Si la suppression immédiate du problème est impossible pour une raison quelconque, vous pouvez la reporter et y revenir plus tard. Pour ce faire, cliquez sur le bouton **Ignorer le message**.

  Sachez toutefois que cette possibilité ne concerne pas les problèmes graves. Il s'agit par exemple de la présence d'objets malveillants non réparés, de l'échec d'un ou de plusieurs composants ou de la corruption de fichiers de l'application.

Pour que les messages dissimulés soient à nouveau affichés dans la liste générale, cochez la case **Afficher les messages ignorés** visible dans la partie inférieure de l'onglet quand des messages masqués existent.

L'onglet **Menaces détectées** permet de consulter la liste des objets malveillants ou potentiellement malveillants découverts et de sélectionner l'action à exécuter sur ceux-ci (par exemple, les placer en quarantaine). Pour sélectionner

les actions, cliquez sur les éléments d'administration situés au-dessus de la liste ou utilisez le menu contextuel des entrées de la liste.

L'onglet **Rapport** permet de prendre connaissance des rapports sur le fonctionnement de l'application (cf. rubrique "Emplacement du rapport sur le fonctionnement de l'application" à la page 69).

# ACTIVATION ET DESACTIVATION DE LA PROTECTION

Kaspersky Internet Security est lancé par défaut au démarrage du système d'exploitation et protège votre ordinateur pendant la session. Tous les composants de la protection sont activés.

Vous pouvez désactiver la protection en temps réel offerte par Kaspersky Internet Security complètement ou partiellement.

Les experts de Kaspersky Lab déconseillent vivement désactiver la protection car cela pourrait entraîner l'infection de l'ordinateur et la perte de données. Si cela est absolument nécessaire, il est conseillé de suspendre la protection pendant la durée requise (cf. rubrique "Suspension et lancement de la protection" à la page 52).

Cette action entraînera l'arrêt de tous les composants.

Les éléments suivants en témoignent :

- L'icône de l'application dans la zone de notification de la barre des tâches est gris (cf. rubrique "Icône dans la zone de notification" à la page 40) ;
- Couleur rouge de l'indicateur de sécurité dans la partie supérieure de la fenêtre principale de l'application.

Notez que dans ce cas, la protection est envisagée dans le contexte des composants du logiciel. La désactivation du fonctionnement des composants de la protection n'a pas d'influence sur la recherche de virus et la mise à jour de Kaspersky Internet Security.

Il est possible d'activer ou de désactiver complètement la protection depuis la fenêtre de configuration de l'application (cf. rubrique "Fenêtre de configuration des paramètres de l'application" à la page 46). Il est possible d'activer ou de désactiver des composants de l'application depuis la fenêtre de configuration ou depuis la fenêtre principale de l'application (cf. rubrique "Fenêtre principale de Kaspersky Internet Security" à la page 42).

*Pour désactiver ou activer complètement la protection, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez la sous-section **Paramètres généraux**.
3. Décochez la case **Activer la protection** s'il faut désactiver la protection. Cochez cette case s'il faut activer la protection.

*Pour activer ou désactiver un composant de la protection depuis la fenêtre de configuration, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la rubrique **Protection**, sélectionnez le composant qu'il faut activer ou désactiver.
3. Dans la partie droite de la fenêtre, décochez la case **Activer <nom du composant>** s'il faut désactiver le composant. Cochez cette case s'il faut activer le composant.

*Pour activer ou désactiver un composant de la protection depuis la fenêtre principale, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et choisissez la rubrique **Protection**.

2. Dans la partie droite de la fenêtre, cliquez avec le bouton gauche de la souris pour déployer le groupe auquel appartient le composant activé ou désactivé.

3. Ouvrez le menu de sélection des actions en cliquant sur le bouton portant le nom du composant. Pour activer le composant, sélectionnez l'option **Activer <nom du composant>** dans le menu ou l'option **Désactiver <nom du composant>** s'il faut le désactiver.

   Quand un composant est activé, l'icône à côté de son nom devient vert. Elle est grise lorsqu'il est désactivé.

# SUSPENSION ET LANCEMENT DE LA PROTECTION

La suspension de la protection signifie la désactivation de tous ses composants pour un certain temps.

Suite à la désactivation temporaire, le fonctionnement de tous les composants de la protection est suspendu.

Les éléments suivants en témoignent :

- L'icône de l'application dans la zone de notification de la barre des tâches est grise (cf. rubrique "Icône dans la zone de notification" à la page 40) ;

- Couleur rouge de l'indicateur de sécurité dans la partie supérieure de la fenêtre principale de l'application.

Notez que dans ce cas, la protection est envisagée dans le contexte des composants du logiciel. La désactivation du fonctionnement des composants de la protection n'a pas d'influence sur la recherche de virus et la mise à jour de Kaspersky Internet Security.

Si des connexions de réseau étaient ouvertes au moment de la suspension de la protection, un message sur l'interruption de celles-ci sera affiché.

Si vous travaillez sur un ordinateur fonctionnant sous Microsoft Windows Vista ou Microsoft Windows 7, vous pouvez suspendre la protection à l'aide du Kaspersky Gadget. Pour ce faire, Kaspersky Gadget doit être configuré de telle manière qu'un de ses boutons est associé à la fonction d'ouverture de la fenêtre des rapports (cf. rubrique "Utilisation de Kaspersky Gadget" à la page 71).

*Pour suspendre la protection de l'ordinateur, procédez comme suit :*

1. Ouvrez la fenêtre **Suspension de la protection** d'une des manières suivantes :

   - Choisissez l'option **Suspension de la protection** dans le menu contextuel de l'icône de l'application (cf. rubrique "Menu contextuel" à la page 41) ;

   - Cliquez sur le bouton avec l'icône **Suspension de la protection** dans l'interface de Kaspersky Gadget (uniquement pour les systèmes d'exploitation Microsoft Windows Vista et Microsoft Windows 7).

2. Dans la fenêtre **Suspension de la protection** sélectionnez la durée à l'issue de laquelle la protection sera à nouveau activée :

   - **Suspendre à l'heure indiquée** : la protection sera activée à l'issue de l'intervalle défini dans le champ en dessous.

   - **Suspendre jusqu'au redémarrage** : la protection sera activée après le redémarrage de l'application ou du système d'exploitation (si le lancement automatique de l'application est activé (cf. rubrique "Activation et désactivation du lancement automatique" à la page 48)).

   - **Reprendre manuellement** : la protection sera activée uniquement lorsque vous déciderez de la rétablir (cf. ci-après).

*Pour reprendre la protection de l'ordinateur,*

Choisissez l'option **Lancement de la protection** dans le menu contextuel de l'icône de l'application (cf. rubrique "Menu contextuel" à la page 41).

Vous pouvez rétablir la protection de l'ordinateur de cette façon non seulement lorsque l'option **Reprendre manuellement** a été choisie pour la suspension, mais également en cas de sélection des options **Suspendre à l'heure indiquée** ou **Suspendre jusqu'au redémarrage**.

# RESOLUTION DES PROBLEMES TYPES

Cette rubrique contient des instructions sur les principales tâches de l'application réalisées le plus souvent par l'utilisateur.

### DANS CETTE SECTION



# PROCEDURE D'ACTIVATION DE L'APPLICATION

L'*activation* est une procédure qui correspond à l'entrée en vigueur d'une licence. Cette licence donne le droit d'utiliser la version commerciale de l'application pendant la durée de validité de la licence.

Si vous n'avez pas activé l'application pendant l'installation, vous pouvez le faire plus tard. Les notifications de Kaspersky Internet Security dans la zone de notifications de la barre des tâches vous rappelleront qu'il faut activer l'application.

*Pour démarrer l'Assistant d'activation de Kaspersky Internet Security, exécutez une des actions suivantes :*

- Cliquez sur le lien **Veuillez activer l'application** dans la fenêtre de notification de Kaspersky Internet Security dans la zone de notifications de la barre des tâches.

- Cliquez sur le lien **Licence** situé dans la partie inférieure de la fenêtre principale de l'application. Dans la fenêtre **Gestionnaire de licences** qui s'ouvre, cliquez sur le bouton **Activer l'application avec une nouvelle licence**.

Examinons en détails les étapes de l'Assistant.

### Etape 1. Sélection du type de licence et saisie du code d'activation

Assurez-vous que l'option **Activer la version commerciale** a bien été sélectionnée dans la fenêtre de l'Assistant d'activation, saisissez le code d'activation (cf. section "Présentation du code d'activation" à la page 38) dans le champ correspondant, puis cliquez sur le bouton **Suivant**.

### Etape 2. Demande d'activation

Lors de la première étape, l'Assistant envoie une demande d'activation de la version commerciale de l'application au serveur d'activation. Si la requête réussit, l'Assistant passe automatiquement à l'étape suivante.

### Etape 3. Saisie des données d'enregistrement

L'enregistrement de l'utilisateur est nécessaire pour qu'il puisse s'adresser ultérieurement au Support technique. Les utilisateurs non enregistrés bénéficient d'une assistance minimum.

Saisissez vos données pour l'enregistrement, puis cliquez sur le bouton **Suivant**.

### Etape 4. Activation

Lors de cette étape, l'Assistant contacte le serveur d'activation pour terminer l'activation de l'application et l'enregistrement de l'utilisateur, après quoi il passe automatiquement à la fenêtre suivante.

### Etape 5. Fin de l'Assistant

Cette fenêtre de l'Assistant reprend les informations sur les résultats de l'activation : type de licence utilisée et date de fin de validité de la licence.

Cliquez sur le bouton **Terminer** pour quitter l'Assistant.

# PROCEDURE D'ACHAT OU DE RENOUVELLEMENT DE LA LICENCE

Si vous avez installé Kaspersky Internet 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. Au moment d'acheter ou de renouveler une licence, vous recevez le code requis pour activer l'application (cf. rubrique "Procédure d'activation de l'application" à la page 54).

*Pour acheter une licence, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.

2. Cliquez sur le bouton **Acheter une licence** situé dans la partie inférieure de la fenêtre.

   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, puis cliquez sur le lien **Licence** situé dans la partie inférieure de la fenêtre.

   La fenêtre **Gestionnaire de licences** s'ouvre.

2. Cliquez sur le bouton **Renouveler la durée de validité de la licence**.

   La page du centre de mise à jour des licences où vous pourrez renouveler votre licence s'ouvre.

# QUE FAIRE EN CAS D'AFFICHAGE DE NOTIFICATIONS

Les notifications de l'application qui apparaissent dans la zone de notification de la barre des tâches signalent les événements survenus pendant l'utilisation de l'application et qui requièrent votre attention. En fonction de la gravité de l'événement, les notifications peuvent appartenir aux catégories suivantes :

- Critiques : signalent des événements d'une importance capitale du point de vue de la sécurité de l'ordinateur (par exemple : découverte d'un objet malveillant ou d'une activité dangereuse dans le système). Quand un tel message apparaît, il faut impérativement décider de la suite des événements. La fenêtre de ce genre de notification est rouge.

- Importantes : signalent des événements potentiellement importants du point de vue de la sécurité de l'ordinateur (par exemple : découverte d'un objet potentiellement infecté ou d'une activité suspecte dans le système). Quand un tel message apparaît, il faut décider du danger que représente l'objet ou le processus découvert et décider de la suite des événements. La fenêtre de ce genre de notification est orange.

- Informatives : signalent des événements qui n'ont pas une importance capitale. La fenêtre de ce genre de notification est verte.

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.

# PROCEDURE DE MISE A JOUR DES BASES DE L'APPLICATION

Kaspersky Internet Security vérifie automatiquement la présence des mises à jour sur les serveurs de mises à jour de Kaspersky Lab. Si le serveur héberge les mises à jour les plus récentes, Kaspersky Internet Security les télécharge et les installe en arrière plan. Vous pouvez lancer la mise à jour de Kaspersky Internet Security à tout moment.

Le téléchargement des mises à jour depuis les serveurs de Kaspersky Lab requiert une connexion Internet.

*Pour lancer la mise à jour de Kaspersky Internet Security depuis la fenêtre principale de l'application, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et dans la partie gauche de la fenêtre, sélectionnez la rubrique **Mise à jour**.

2. Dans la partie droite de la fenêtre, cliquez sur le bouton **Exécuter la mise à jour**.

   Les informations relatives à la progression de la mise à jour apparaîtront dans la fenêtre principale de l'application, dans la rubrique **Mise à jour**, ainsi que dans le menu contextuel de l'icône de l'application.

# PROCEDURE D'ANALYSE DES SECTEURS IMPORTANTS DE L'ORDINATEUR

L'analyse des secteurs importants désigne l'analyse des objets chargés au démarrage du système d'exploitation, l'analyse de la mémoire système, l'analyse des secteurs d'amorçage du disque, ainsi que l'analyse des objets ajoutés par l'utilisateur (cf. rubrique "Composition de la liste des objets à analyser" à la page 78).

Vous pouvez lancer une analyse des zones importantes d'une des méthodes suivantes :

- via un raccourci créé (cf. page 82) au préalable ;
- depuis la fenêtre principale de l'application (cf. section "Fenêtre principale de Kaspersky Internet Security" à la page 42).

*Pour lancer l'analyse via un raccourci, procédez comme suit :*

1. Ouvrez l'Assistant de Microsoft Windows et accédez au dossier où vous avez créé le raccourci.
2. Double-cliquez sur le raccourci pour lancer l'analyse.

   La progression de la tâche sera illustrée dans la fenêtre principale de Kaspersky Internet Security dans la rubrique **Analyse**, dans la fenêtre **Analyse des secteurs importants** ouverte d'un clic dans le groupe **L'analyse des secteurs importants est en cours** dans la rubrique **Analyse** de la fenêtre principale pendant l'analyse ainsi que dans le menu contextuel de l'icône de l'application.

*Pour lancer l'analyse depuis la fenêtre principale de l'application, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et dans la partie gauche de la fenêtre, sélectionnez la rubrique **Analyse**.
2. Dans la partie droite de la fenêtre principale, cliquez sur le groupe **Lancer l'analyse rapide**.

   La progression de la tâche sera illustrée dans la fenêtre principale de Kaspersky Internet Security dans la rubrique **Analyse**, dans la fenêtre **Analyse des secteurs importants** ouverte d'un clic dans le groupe **L'analyse des secteurs importants est en cours** dans la rubrique **Analyse** de la fenêtre principale pendant l'analyse ainsi que dans le menu contextuel de l'icône de l'application.

# PROCEDURE D'ANALYSE D'UN OBJET DISTINCT (FICHIER, DOSSIER, DISQUE)

Pour analyser un objet distinct, utilisez une des méthodes suivantes :

- Via le menu contextuel de l'objet ;
- Depuis la fenêtre principale de l'application (cf. section "Fenêtre principale de Kaspersky Internet Security" à la page 42) ;
- Via le gadget Kaspersky Internet Security (uniquement pour les systèmes d'exploitation Microsoft Windows Vista et Microsoft Windows 7).

*Pour lancer la recherche d'éventuels virus depuis le menu contextuel de l'objet, procédez comme suit :*

1. Ouvrez la fenêtre de l'Assistant de Microsoft Windows et accédez au dossier contenant l'objet à analyser.
2. Ouvrez le menu contextuel de l'objet en cliquant avec le bouton droit de la souris (cf. ill. ci-après) et choisissez l'option **Rechercher d'éventuels virus**.

La progression et le résultat d'exécution de la tâche sont illustrés dans la fenêtre **Recherche de virus** ouverte.


*Illustration 10. Menu contextuel de l'objet dans Microsoft Windows*

- *Pour lancer la recherche d'éventuels virus dans un objet depuis la fenêtre principale de l'application, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et dans la partie gauche de la fenêtre, sélectionnez la rubrique **Analyse**.

2. Désignez l'objet à analyser d'une des méthodes suivantes :

   - Cliquez sur le lien **sélectionnez** situé dans la partie droite de la fenêtre pour ouvrir la fenêtre **Analyse des Objets**, puis cochez les cases en regard des dossiers et des disques à analyser. Si les objets à analyser ne figurent pas dans la liste, cliquez sur le lien **Ajouter** de la fenêtre **Sélection de l'objet à analyser**, puis sélectionnez les objets à analyser.

   - Faites glisser l'objet à analyser dans la zone de la fenêtre principale prévue à cet effet (cf. ill. ci-dessous).

   Le processus d'exécution de la tâche apparaîtra dans la fenêtre **Recherche de virus** qui s'ouvre.



*Illustration 11. Zone de la fenêtre sur laquelle il faut déposer l'objet à analyser*

- *Pour rechercher la présence éventuelle de virus à l'aide du gadget,*

  faites glisser l'objet sur le gadget.

  Le processus d'exécution de la tâche apparaîtra dans la fenêtre **Recherche de virus** qui s'ouvre.

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

Vous pouvez lancer l'analyse complète de l'ordinateur d'une des méthodes suivantes :

- via un raccourci créé (cf. page 82) au préalable ;
- depuis la fenêtre principale de l'application (cf. section "Fenêtre principale de Kaspersky Internet Security" à la page 42).

*Pour lancer l'analyse complète via un raccourci, procédez comme suit :*

1. Ouvrez l'Assistant de Microsoft Windows et accédez au dossier où vous avez créé le raccourci.
2. Double-cliquez sur le raccourci pour lancer l'analyse.

   La progression de la tâche sera illustrée dans la fenêtre principale de Kaspersky Internet Security dans la rubrique **Analyse**, dans la fenêtre **Analyse complète** ouverte d'un clic dans le groupe **L'analyse complète est en cours** dans la rubrique **Analyse** de la fenêtre principale pendant l'analyse ainsi que dans le menu contextuel de l'icône de l'application.

*Pour lancer l'analyse complète depuis la fenêtre principale de l'application, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et dans la partie gauche de la fenêtre, sélectionnez la rubrique **Analyse**.
2. Dans la partie droite de la fenêtre, cliquez sur le bouton **Lancer l'analyse complète**.

   La progression de la tâche sera illustrée dans la fenêtre principale de Kaspersky Internet Security dans la rubrique **Analyse**, dans la fenêtre **Analyse complète** ouverte d'un clic dans le groupe **L'analyse complète est en cours** dans la rubrique **Analyse** de la fenêtre principale pendant l'analyse ainsi que dans le menu contextuel de l'icône de l'application.

# PROCEDURE DE RECHERCHE DE VULNERABILITES SUR L'ORDINATEUR

Une *vulnérabilité* est un endroit non protégé dans le code que les individus malintentionnés peuvent utiliser à leur fin, par exemple copier les données utilisées par l'application au code non protégé. La recherche de vulnérabilités potentielles sur votre ordinateur permet d'identifier ces "points faibles" dans la protection de votre ordinateur. Il est conseillé de supprimer les vulnérabilités découvertes.

Vous pouvez lancer la recherche de vulnérabilités d'une des manières suivantes :

- Depuis la fenêtre principale de l'application (cf. section "Fenêtre principale de Kaspersky Internet Security" à la page 42) ;
- Via un raccourci créé au préalable.

*Pour lancer une tâche à l'aide d'un raccourci, procédez comme suit :*

1. Ouvrez l'Assistant de Microsoft Windows et accédez au dossier où vous avez créé le raccourci.
2. Double-cliquez sur le raccourci pour lancer la tâche de recherche de vulnérabilités.

   L'exécution de la tâche est illustrée dans la fenêtre principale de l'application.

*Pour lancer la tâche depuis la fenêtre de l'application, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et dans la partie gauche de la fenêtre, sélectionnez la rubrique **Outils**.

2. Dans la partie droite de la fenêtre, cliquez sur le bouton **Recherche de vulnérabilités dans le système**.

3. Dans la fenêtre **Recherche de Vulnérabilités** qui s'ouvre, cliquez sur le bouton **Lancer la recherche de vulnérabilités** situé dans la partie supérieure de la fenêtre.

   Le processus d'exécution de la tâche s'affiche dans le champ **Fin**. Pour suspendre l'exécution de la tâche, cliquez sur le bouton **La recherche de vulnérabilités est en cours** dans la partie supérieure de la fenêtre.

# PROCEDURE DE PROTECTION DES DONNEES PERSONNELLES CONTRE LE VOL

Kaspersky Internet Security permet de protéger les données personnelles suivantes contre le vol :

- Mots de passe, noms d'utilisateur et autres données d'enregistrement ;
- Numéros de compte et de cartes de crédit.

Kaspersky Internet Security reprend des composants et des outils qui permettent de protéger vos données personnelles contre le vol par des individus malintentionnés via des méthodes telles que le phishing et l'interception des données saisies au clavier.

L'Anti-Phishing, inclus dans l'Antivirus Internet, l'Antivirus Courrier et l'Antivirus IM, garantit la protection contre le phishing.

Pour vous protéger contre l'interception des données saisies au clavier, utilisez le *Clavier virtuel*.

## DANS CETTE SECTION



# PROTECTION CONTRE LE PHISHING

Le *phishing* (ou hameçonnage) est un type d'escroquerie sur Internet qui vise à "extraire" le numéro de carte de crédit, les codes d'identification personnelle et d'autres données privées de l'utilisateur dans le but de lui voler de l'argent.

Le phishing est lié à l'émergence des services bancaires en ligne. Les individus malintentionnés reproduisent une copie fidèle du site web de la banque prise pour cible puis envoient aux clients de celle-ci un message qui a tous les attributs d'un message authentique en provenance de la banque. Ces messages invitent le client à confirmer ou à modifier ses données d'accès au site web de la banque à la suite d'une panne ou d'un changement de système d'opérations bancaires en ligne qui a entraîné la perte de toutes les données. L'utilisateur clique sur le lien qui renvoie vers le site Web créé par les malfaiteurs et y saisit ses données personnelles qui seront transmises aux individus malintentionnés.

L'Anti-Phishing, inclus dans l'Antivirus Internet, l'Antivirus Courrier et l'Antivirus IM, garantit la protection contre le phishing. Activez ces composants afin de garantir la protection la plus efficace contre le phishing.

*Pour activer les composants qui assure la protection contre les attaques de phishing, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et dans la partie gauche de la fenêtre, sélectionnez la rubrique **Protection**.

2. Dans la partie droite de la fenêtre, cliquez sur le bouton gauche de la souris et ouvrez le groupe **Contrôle de l'utilisation du réseau**.

3. Ouvrez le menu de sélection de l'action pour le composant en cliquant sur le bouton **Anti-Phishing** et sélectionnez l'option **Activer Anti-Phishing** dans le menu.

   Cette action entraîne l'activation de l'Anti-Phishing et des composants qui l'utilisent.

## CLAVIER VIRTUEL

Au cours de l'utilisation de l'ordinateur, il arrive souvent qu'il faille saisir des données personnelles ou un nom d'utilisateur et un mot de passe. Ceci se produit par exemple lors de l'ouverture d'une session sur un site web, lors de l'achat dans une boutique en ligne ou en cas d'utilisation d'un service de transactions bancaires en ligne.

Le risque existe que ces données soient interceptées à l'aide d'outils d'interception ou d'enregistreurs de frappes.

Le clavier virtuel permet d'éviter l'interception des données saisies à l'aide du clavier traditionnel.

Le clavier virtuel ne peut protéger vos données si le site web nécessitant la saisie de ces données a été compromis car dans ce cas, les données tombent directement entre les mains des individus malintentionnés.

De nombreux logiciels espions peuvent réaliser des captures d'écran qui sont transmises automatiquement à l'individu malintentionné pour qu'il l'analyse et qu'il puisse récupérer les données personnelles de l'utilisateur. Le clavier virtuel protège les données personnelles saisies contre l'interception par capture d'écran.

Le clavier virtuel protège contre l'interception des données personnelles uniquement avec les navigateurs Microsoft Internet Explorer et Mozilla Firefox.

Avant d'utiliser le clavier virtuel, prenez connaissance des particularités de son utilisation :

- Avant de saisir les données à l'aide du clavier virtuel, assurez-vous que le curseur de la souris se trouve dans le champ requis.
- Il faut appuyer sur les touches du clavier à l'aide de la souris.
- À la différence du clavier ordinaire, le clavier virtuel ne vous permet pas d'appuyer sur deux touches en même temps. Par conséquent, si vous souhaitez utiliser une combinaison de touches (par exemple, **ALT+F4**), il faut d'abord appuyer sur la première touche (par exemple **ALT**), puis sur la deuxième (par exemple **F4**), puis à nouveau sur la première. La deuxième pression sur la première touche équivaut au relâchement des deux touches sur le clavier.
- Sur le clavier virtuel, vous pouvez changer la langue de saisie à l'aide de la combinaison de touches **CTRL+SHIFT** (dans ce cas, il faut appuyer sur la touche **SHIFT** avec le bouton droit de la souris) ou **CTRL+LEFT ALT** (cliquez sur la touche **LEFT ALT** avec le bouton droit de la souris), en fonction des paramètres définis.

Plusieurs méthodes s'offrent à vous pour ouvrir le clavier virtuel :

- Depuis le menu contextuel de l'icône de l'application ;
- Au départ de la fenêtre principale de l'application ;
- Depuis la fenêtre du navigateur Microsoft Internet Explorer ou Mozilla Firefox ;
- À l'aide d'une combinaison de touches.

*Pour ouvrir le clavier virtuel depuis le menu contextuel de l'icône de l'application,*

Choisissez l'option **Outils** → **Clavier virtuel** dans le menu contextuel de l'icône de l'application.

*Pour ouvrir le clavier virtuel depuis la fenêtre principale de l'application, procédez comme suit :*

1. Ouvrez la Ouvrez la fenêtre principale de l'application et dans la partie gauche de la fenêtre, sélectionnez la rubrique **Exécution en Environnement Protégé**.

2. Dans la partie droite de la fenêtre, cliquez sur le groupe **Clavier virtuel**.

*Pour ouvrir le clavier virtuel depuis la fenêtre du navigateur,*

Cliquez sur le bouton  **Clavier virtuel** dans la barre d'outils de Microsoft Internet Explorer ou Mozilla Firefox

*Pour ouvrir le clavier virtuel à l'aide du clavier physique,*

utilisez la combinaison de touches **CTRL+ALT+SHIFT+P**.

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

Si vous pensez que l'objet est infecté par un virus, analysez-le d'abord à l'aide de Kaspersky Internet Security (cf. rubrique "Procédure d'analyse d'un objet distinct (fichier, dossier, disque)" à la page 57).

Si l'application, suite à l'analyse, signale que l'objet est sain, mais que vous pensez que ce n'est pas le cas, vous pouvez agir de la manière suivante :

- Placer l'objet 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 Internet Security puisse identifier la menace et la supprimer.

- Envoyer l'objet au *Laboratoire d'étude des virus*. Les experts du laboratoire d'étude des virus étudieront l'objet pour voir s'il est vraiment infecté par un virus et ajouteront sur le champ la description du nouveau virus aux bases qui seront chargées par l'application lors de la mise à jour (cf. rubrique "Procédure de mise à jour des bases de l'application" à la page 56).

Un objet peut être placé en quarantaine de deux manières :

- Via le lien **Placer en quarantaine** de la fenêtre **Etat de la protection** ;

- Via le menu contextuel de l'objet.

*Pour placer un objet en quarantaine depuis la fenêtre Etat de la protection, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.

2. Cliquez sur le lien **Quarantaine** situé dans la partie supérieure de la fenêtre principale pour ouvrir la fenêtre **Etat de la protection** à l'onglet **Menaces détectées**.

3. Cliquez sur le lien **Placer en quarantaine** situé au-dessus de la liste des menaces.

4. Dans la fenêtre qui s'ouvre, choisissez l'objet qu'il faut placer en quarantaine.

*Pour placer un objet en quarantaine à l'aide du menu contextuel, procédez comme suit :*

1. Ouvrez la fenêtre de l'Assistant de Microsoft Windows et accédez au dossier contenant l'objet à mettre en quarantaine.

2. Cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel de l'objet, puis choisissez l'option **Copier dans la quarantaine**.

*Pour envoyer l'objet au laboratoire d'étude des virus, procédez comme suit :*

1. Ouvrez la page d'envoi de requêtes au Laboratoire d'étude des virus (http://support.kaspersky.ru/virlab/helpdesk.html?LANG=fr).

2. Suivez les instructions affichées sur la page pour envoyer votre demande.

# QUE FAIRE AVEC UN GRAND NOMBRE DE MESSAGES NON SOLLICITES

Si vous recevez un volume important de courrier indésirable (spam), activez le composant Anti-Spam et définissez le niveau de protection recommandé, puis entraînez le composant à l'aide de l'*Assistant d'apprentissage*. Pour assurer une identification efficace du courrier indésirable, il est indispensable de réaliser l'entraînement sur un minimum de 50 exemplaires de courrier normal et de 50 exemplaires de courrier indésirable.

*Pour activer l'Anti-Spam et définir le niveau de protection recommandé, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.

2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Anti-Spam**.

3. Dans la partie droite de la fenêtre, cochez la case **Activer l'Anti-Spam**.

4. Dans le groupe **Niveau de protection**, le niveau de protection par défaut doit être **Recommandé**.

   Si le niveau est **Bas** ou **Autre**, cliquez sur le bouton **Par défaut**. Le niveau de protection prendra automatiquement la valeur **Recommandé**.

*Pour entraîner l'Anti-Spam à l'aide de l'Assistant d'apprentissage, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.

2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Anti-Spam**.

3. Dans la partie droite de la fenêtre, dans le groupe **Entraînement d'Anti-Spam**, cliquez sur le bouton **Entraîner**.

   La fenêtre de l'Assistant d'apprentissage s'ouvre.

Examinons en détails les étapes de l'Assistant.

### Etape 1. Début de l'utilisation de l'Assistant

Cliquez sur le bouton **Suivant** pour commencer l'apprentissage.

### Etape 2. Sélection des répertoires contenant le courrier normal

Cette étape permet de sélectionner les répertoires contenant le courrier normal. Il faut sélectionner uniquement les répertoires dont vous êtes certain du contenu.

Seuls les dossiers des comptes Microsoft Office Outlook et Microsoft Outlook Express (Windows Mail) sont proposés pour la sélection.

### Etape 3. Sélection des répertoires contenant le courrier indésirable

Cette étape permet de sélectionner le dossier qui contient le courrier indésirable. Si votre client de messagerie ne possède pas ce répertoire, passez cette étape.

Seuls les dossiers des comptes Microsoft Office Outlook et Microsoft Outlook Express (Windows Mail) sont proposés pour la sélection.

### Etape 4. Entraînement d'Anti-Spam

Cette étape correspond à l'entraînement automatique de l'Anti-Spam sur la base des répertoires choisis au cours des étapes précédentes. Les messages de ces dossiers viennent s'ajouter à la base de l'Anti-Spam. Les expéditeurs de courrier normal sont ajoutés automatiquement à la liste des expéditeurs autorisés.

### Etape 5. Enregistrement des résultats de l'entraînement

Cette étape de l'Assistant d'apprentissage consiste à enregistrer les résultats de l'entraînement d'une des manières suivantes :

- Ajouter les résultats de l'apprentissage à la base existante de l'Anti-Spam (choisissez l'option **Ajouter les résultats de l'apprentissage à la base existante de l'Anti-Spam**) ;
- Remplacer la base actuelle par la base nouvelle obtenue suite à l'apprentissage (choisissez l'option **Créer une nouvelle base de connaissances de l'Anti-Spam**).

Cliquez sur le bouton **Terminer** pour quitter l'Assistant.

# QUE FAIRE SI VOUS PENSEZ QUE VOTRE ORDINATEUR EST INFECTE

Si vous pensez que votre ordinateur est infecté, utilisez l'*Assistant de restauration du système* qui supprimera les traces de la présence d'objets malveillants dans le système. Les experts de Kaspersky Lab conseillent également de lancer l'Assistant après la réparation de l'ordinateur afin de confirmer que toutes les menaces et les dégâts ont été supprimés.

L'Assistant vérifie si le système a été modifié d'une manière ou d'une autre : blocage de l'accès à l'environnement de réseau, modification des extensions de fichiers de format connu, blocage du panneau d'administration, etc. Les causes de ces dégâts sont multiples. Il peut s'agir de l'activité de programmes malveillants, d'une mauvaise configuration du système, de pannes du système ou de l'utilisation d'applications d'optimisation du système qui ne fonctionnent pas correctement.

Après l'étude, l'Assistant analyse les informations recueillies afin d'identifier les dégâts dans le système qui requièrent une intervention immédiate. La liste des actions à exécuter pour supprimer l'infection est générée sur la base des résultats de l'analyse. L'Assistant regroupe les actions en catégorie selon la gravité des problèmes identifiés.

L'Assistant se compose d'une série de fenêtres (étapes) entre lesquelles vous pouvez naviguer grâce aux boutons **Précédent** et **Suivant**. Pour quitter l'Assistant, cliquez sur le bouton **Terminer**. Pour interrompre l'Assistant à n'importe quelle étape, cliquez sur le bouton **Annuler**.

*Pour lancer l'Assistant de restauration du système, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et dans la partie gauche de la fenêtre, sélectionnez la rubrique **Outils**.
2. Dans la partie droite de la fenêtre, cliquez sur le bouton **Restauration du système**.

Examinons en détails les étapes de l'Assistant.

### Etape 1. Lancement de la restauration du système

Assurez-vous que l'option **Rechercher les problèmes liés à l'activité d'un programme malveillant** a été sélectionnée dans la fenêtre de l'Assistant, puis cliquez sur le bouton **Suivant**.

### Etape 2. Recherche des problèmes

L'Assistant recherche les problèmes et les dégâts potentiels qu'il faut supprimer. Une fois la recherche terminée, l'Assistant passe automatiquement à l'étape suivante.

### Etape 3. Sélection d'actions pour la résolution des problèmes

Tous les problèmes identifiés à l'étape précédente sont regroupés en fonction du danger qu'ils présentent. Pour chaque groupe de corruptions, les experts de Kaspersky Lab proposent un ensemble d'actions dont l'exécution contribuera à l'élimination des problèmes. Trois groupes d'actions ont été désignés :

- Les *actions vivement recommandées* permettent de supprimer les corruptions qui constituent un problème sérieux. Il est conseillé d'exécuter toutes les actions de ce groupe.
- Les *actions recommandées* visent à supprimer les corruptions qui peuvent présenter un danger potentiel. L'exécution des actions de ce groupe est également recommandée.
- Les *actions complémentaires* sont prévues pour supprimer les corruptions du système qui ne présentent actuellement aucun danger mais qui à l'avenir pourraient menacer la sécurité de l'ordinateur.

Pour voir les actions reprises dans le groupe, cliquez sur le signe **+** situé à gauche du nom du groupe.

Pour que l'Assistant réalise une action, cochez la case à gauche du nom de l'action. Toutes les actions recommandées et vivement recommandées sont exécutées par défaut. Si vous ne souhaitez pas exécuter une action quelconque, désélectionnez la case en regard de celle-ci.

Il est vivement déconseillé de décocher les cases sélectionnées par défaut car vous pourriez mettre en danger la sécurité de l'ordinateur.

Une fois que vous aurez sélectionné les actions pour l'Assistant, cliquez sur **Suivant**.

### Etape 4. Suppression des problèmes

L'Assistant exécute les actions sélectionnées à l'étape précédente. La suppression des problèmes peut durer un certain temps. Une fois la suppression des problèmes terminée, l'Assistant passe automatiquement à l'étape suivante.

### Etape 5. Fin de l'Assistant

Cliquez sur le bouton **Terminer** pour quitter l'Assistant.

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

Kaspersky Lab déconseille la restauration d'objets supprimés ou réparés car ils peuvent constituer une menace pour votre ordinateur.

Si la restauration d'un objet supprimé ou réparé s'impose, utilisez sa copie de sauvegarde créée par l'application lors de l'analyse de l'objet.

*Pour restaurer un objet supprimé ou réparé par l'application, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.

2. Cliquez sur le lien **Quarantaine** situé dans la partie supérieure de la fenêtre principale pour ouvrir la fenêtre **Etat de la protection** à l'onglet **Menaces détectées**.

3. Choisissez d'afficher les objets neutralisés en cliquant sur le lien **Neutralisées** situé au-dessus de la liste des menaces.

   La liste des objets modifiés et réparés apparaît sous l'onglet **Menaces détectées**. Les objets sont regroupés par état. Pour afficher la liste des objets figurant dans un groupe, cliquez sur le bouton **+** situé à gauche du titre du groupe.

4. Cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel de l'objet qu'il faut restaurer et choisissez l'option **Restaurer**.

# PROCEDURE DE CREATION DU DISQUE DE DEPANNAGE ET UTILISATION DE CELUI-CI

Il est conseillé de créer le disque de dépannage après l'installation et la configuration de Kaspersky Internet Security et après avoir utilisé ce dernier pour analyser l'ordinateur et confirmé qu'il n'était pas infecté. À l'avenir, vous pourrez utiliser le disque de dépannage pour analyser et réparer l'ordinateur infecté dont la réparation par n'importe quel autre moyen est impossible (par exemple, à l'aide d'un logiciel antivirus).

### DANS CETTE SECTION



## CREATION D'UN DISQUE DE DEPANNAGE

La création du disque de dépannage consiste à générer une image du disque (fichier .iso) avec les bases antivirus actuelles ainsi que les fichiers de configuration.

L'image du disque de départ, qui sert à la création du fichier, peut être téléchargée du serveur de Kaspersky Lab ou copiée depuis une source locale.

Le disque de dépannage est créé à l'aide de l'*Assistant de création de disque de dépannage*. Le fichier de l'image rescuecd.iso créé par l'Assistant est enregistré sur le disque dur de l'ordinateur.

- Sous Microsoft Windows XP dans le dossier : Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP11\Data\Rdisk\ ;

- Sous Microsoft Windows Vista et Microsoft Windows 7 dans le dossier : ProgramData\Kaspersky Lab\AVP11\Data\Rdisk\.

L'Assistant se compose d'une série de fenêtres (étapes) entre lesquelles vous pouvez naviguer grâce aux boutons **Précédent** et **Suivant**. Pour quitter l'Assistant, cliquez sur le bouton **Terminer**. Pour interrompre l'Assistant à n'importe quelle étape, cliquez sur le bouton **Annuler**.

*Afin de lancer l'Assistant de création de disque de dépannage, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et dans la partie gauche de la fenêtre, sélectionnez la rubrique **Outils**.

2. Dans la partie droite de la fenêtre, cliquez sur le bouton **Disque de dépannage**.

Examinons en détails les étapes de l'Assistant.

### Etape 1. Recherche d'une image de disque existante

Si l'Assistant découvre un fichier d'image de disque de dépannage dans le dossier prévu à cet effet (cf. ci-dessus), vous pouvez, en cochant la case **Utiliser l'image existante**, utiliser ce fichier en guise d'image de disque source et passer directement à l'étape **Mise à jour de l'image du disque** (cf. ci-dessous). Décochez cette case si vous ne souhaitez pas utiliser l'image de disque trouvée. L'Assistant passera à la fenêtre **Sélection de la source de l'image du disque**.

Si l'Assistant n'a pas trouvé d'image de disque, cette étape est ignorée et l'Assistant passe à la fenêtre **Sélection de la source de l'image du disque**.

### Etape 2. Sélection de la source de l'image du disque

Si dans la fenêtre précédente de l'Assistant vous avez coché la case **Utiliser l'image existante**, alors cette étape n'est pas présentée.

Cette étape vous oblige à sélectionner une source du fichier de l'image parmi les options proposées :

- Sélectionnez l'option **Copier l'image sur le disque local ou de réseau** si vous possédez déjà une image du disque de dépannage ou si cette image a déjà été préparée et qu'elle se trouve sur l'ordinateur ou sur une ressource du réseau local.

- Sélectionnez l'option **Télécharger l'image depuis les serveurs de Kaspersky Lab** si vous n'avez pas une copie du fichier d'image afin de le télécharger depuis le serveur de Kaspersky Lab (le fichier pèse environ 175 Mo).

### Etape 3. Copie (téléchargement) de l'image du disque

Si dans la fenêtre précédente de l'Assistant vous avez coché la case **Utiliser l'image existante**, alors cette étape n'est pas présentée.

Si à l'étape précédente vous avez sélectionné l'option de copie de l'image de la source locale (Copier **l'image sur le disque local ou de réseau**), alors il faudra indiquer au cours de cette étape le chemin d'accès à celle-ci. Pour ce faire, cliquez sur le bouton **Parcourir**. Après avoir indiqué le chemin d'accès au fichier, cliquez sur **Suivant**. La progression de la copie de l'image de disque est illustrée dans la fenêtre de l'Assistant.

Si vous aviez choisi l'option **Télécharger l'image depuis les serveurs de Kaspersky Lab**, alors la progression du téléchargement s'affichera directement.

Une fois que la copie ou le téléchargement de l'image de disque sera terminé, l'Assistant passera automatiquement à l'étape suivante.

### Etape 4. Mise à jour de l'image du disque

La procédure d'actualisation du fichier d'image prévoit :

- La mise à jour des bases antivirus ;

- La mise à jour des fichiers de configuration.

Les fichiers de configuration déterminent la possibilité de charger l'ordinateur depuis un CD/DVD enregistré avec le disque de dépannage créé à l'aide de l'Assistant.

Lors de la mise à jour des bases antivirus, les bases obtenues suite à la mise à jour la plus récente de Kaspersky Internet Security sont utilisées. Si les bases sont dépassées, il est conseillé de réaliser une mise à jour et de lancer à nouveau l'Assistant de création de disque de dépannage.

Pour lancer la mise à jour du fichier, cliquez sur **Suivant**. La fenêtre de l'Assistant illustrera la progression de la mise à jour.

### Etape 5. Enregistrement de l'image sur un support

Cette fenêtre vous informe de la réussite de la création du disque de dépannage et propose de copier l'image sur un support.

Désignez le support pour la copie de l'image de disque :

- Choisissez l'option **Ecrire sur un disque laser** si vous souhaitez enregistrer l'image sur un CD/DVD.

  Vous devrez désigner le CD/DVD sur lequel il faut enregistrer l'image avant de lancer la copie de celle-ci. L'enregistrement peut durer un certain temps. Veuillez attendre jusque la fin.

- Choisissez l'option **Ecrire sur un périphérique USB** si vous voulez enregistrer l'image sur un disque amovible.

  Kaspersky Lab déconseille d'enregistrer l'image de disque sur un périphérique qui n'est pas prévu exclusivement pour le stockage de données, comme un téléphone intelligent, un téléphone mobile, un ordinateur de poche ou un lecteur MP3. L'enregistrement de l'image de disque sur de tels appareils pourrait nuire au fonctionnement ultérieur de ceux-ci.

  Vous devrez indiquer le disque amovible sur lequel l'image sera enregistrée avant de lancer l'enregistrement de celle-ci. L'enregistrement peut durer un certain temps. Veuillez attendre jusque la fin.

- Sélectionnez l'option **Ne pas enregistrer** pour ne pas enregistrer l'image de disque créée sur un support.

  Dans ce cas, le dossier contenant l'image de disque créée s'ouvrira.

### Etape 6. Fin de l'Assistant

Pour quitter l'Assistant, cliquez sur **Terminer**. Le disque créé pourra être utilisé ultérieurement pour le lancement de l'ordinateur (cf. page 68).

## DEMARRAGE DE L'ORDINATEUR A L'AIDE DU DISQUE DE DEPANNAGE

S'il est impossible de charger le système d'exploitation suite à une attaque de virus, utilisez le disque de dépannage.

Le chargement du système d'exploitation requiert le CD/DVD ou le disque amovible contenant le fichier d'image de disque (.iso) de dépannage (cf. rubrique "Création d'un disque de dépannage" à la page 66).

Le lancement de l'ordinateur depuis un disque amovible n'est pas toujours possible. C'est le cas par exemple si l'ordinateur appartient à des anciennes générations. Avant d'éteindre l'ordinateur en vue de le redémarrer depuis un disque amovible, vérifiez si cette option est prise en charge par l'ordinateur.

*Pour démarrer l'ordinateur depuis le disque de dépannage, procédez comme suit :*

1. Dans les paramètres BIOS, activez le chargement depuis un CD/DVD ou depuis un disque amovible (pour obtenir de plus amples informations, consultez la documentation de la carte mère de votre ordinateur).
2. Introduisez le CD/DVD dans le lecteur de l'ordinateur infecté ou connectez le disque amovible contenant l'image de disque de dépannage.
3. Redémarrez l'ordinateur.

Pour en savoir plus sur l'utilisation du disque de dépannage, consultez le guide de l'utilisateur de Kaspersky Rescue Disk.

# EMPLACEMENT DU RAPPORT SUR LE FONCTIONNEMENT DE L'APPLICATION

Kaspersky Internet Security crée un rapport sur le fonctionnement de chacun de ses composants. Ce rapport permet de voir le nombre d'objets malveillants détectés et neutralisés (par exemple, virus ou chevaux de Troie) pendant l'utilisation de l'application au cours d'une période déterminée, le nombre de fois que l'application a été mise à jour au cours de la même période, la quantité de messages non sollicités découverte, etc.

Si vous travaillez sur un ordinateur fonctionnant sous Microsoft Windows Vista ou Microsoft Windows 7, vous pouvez ouvrir les rapports à l'aide du Kaspersky Gadget. Pour ce faire, Kaspersky Gadget doit être configuré de telle manière qu'un de ses boutons soit associé à la fonction d'ouverture de la fenêtre des rapports (cf. rubrique "Utilisation de Kaspersky Gadget" à la page 71).

*Pour consulter le rapport sur le fonctionnement du composant, procédez comme suit :*

1. Ouvrez la fenêtre **Etat de la protection**, sous l'onglet **Rapport** selon un des moyens suivants :

   - Cliquez sur le lien **Rapports** dans la partie supérieure de la fenêtre principale de l'application ;
   - Cliquez sur le bouton avec l'icône **Rapports** dans l'interface de Kaspersky Gadget (uniquement pour les systèmes d'exploitation Microsoft Windows Vista et Microsoft Windows 7).

   L'onglet **Rapport** affiche les rapports sur l'utilisation de l'application sous la forme de diagrammes.

2. Pour consulter un rapport détaillé (par exemple un rapport sur chacun des composants de l'application), cliquez sur le bouton **Rapport détaillé** situé dans la partie inférieure de l'onglet **Rapport**.

   La fenêtre **Rapport détaillé** s'ouvre. Elle présente les données sous forme d'un tableau. Pour faciliter la lecture du tableau, il est possible de regrouper les entrées du tableau selon différents critères.

# PROCEDURE DE RESTAURATION DES PARAMETRES STANDARDS D'UTILISATION DE L'APPLICATION

Vous pouvez revenir à tout moment aux paramètres de fonctionnement de Kaspersky Internet Security recommandés par Kaspersky Lab et considérés comme optimum. La restauration des paramètres s'opère à l'aide de l'*Assistant de configuration de l'application*.

À l'issue de l'utilisation de l'Assistant, le niveau de protection **Recommandé** sera sélectionné pour tous les composants de la protection. Lors de la restauration des paramètres, vous aurez également la possibilité de définir les paramètres qu'il faut ou non maintenir en parallèle à la restauration du niveau de protection recommandé et les composants concernés.

*Pour restaurer les paramètres de protection, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Lancez l'Assistant de configuration de l'application d'une des manières suivantes :

   - Cliquez sur le lien **Restaurer** dans la partie inférieure de la fenêtre ;
   - Dans la partie gauche de la fenêtre, choisissez la rubrique **Paramètres avancés**, sous-rubrique **Administration des paramètres**, puis cliquez sur le bouton **Restaurer** dans le groupe **Restauration des paramètres standard**.

Examinons en détails les étapes de l'Assistant.

### Etape 1. Début de l'utilisation de l'Assistant

Cliquez sur le bouton **Suivant** afin de poursuivre l'Assistant.

### Etape 2. Sélection des paramètres à conserver

Cette fenêtre de l'Assistant reprend les composants de Kaspersky Internet Security dont les paramètres ont été modifiés par l'utilisateur ou assimilés par Kaspersky Internet Security durant l'entraînement des composants Pare-feu et Anti-Spam. Si des paramètres uniques ont été définis pour un composant quelconque, ils figureront également dans la fenêtre.

Parmi les paramètres uniques, il y a les listes blanche et noire des expressions et des adresses utilisées par Anti-Spam, la liste des adresses Internet et des numéros d'accès de confiance, les règles d'exclusion pour les composants de l'application, les règles de filtrage des paquets et les règles des applications du Pare-feu.

Ces listes sont composées pendant l'utilisation de Kaspersky Internet Security et tiennent compte des tâches individuelles et des exigences de sécurité. La composition de telles listes prend en général beaucoup de temps et pour cette raison, il est recommandé de les conserver en cas de rétablissement des paramètres du programme à leur valeur d'origine.

Cochez la case en regard des paramètres à enregistrer, puis cliquez sur le bouton **Suivant**.

### Etape 3. Analyse du système

Cette étape correspond à la collecte d'informations sur les applications reprises dans Microsoft Windows. Ces applications figurent dans la liste des applications de confiance et elles ne sont soumises à aucune restriction sur les actions qu'elles peuvent réaliser dans le système.

Une fois l'analyse terminée, l'Assistant passe automatiquement à l'étape suivante.

### Etape 4. Fin de la restauration

Pour quitter l'Assistant, cliquez sur **Terminer**.

# PROCEDURE DE TRANSFERT DES PARAMETRES DE L'APPLICATION DANS UNE VERSION DE KASPERSKY INTERNET SECURITY INSTALLEE SUR UN AUTRE ORDINATEUR

Après avoir configuré l'application, vous pouvez appliquer ses paramètres de fonctionnement à une version de Kaspersky Internet Security installée sur un autre ordinateur. L'application sur les deux ordinateurs sera configurée de la même manière. Cela est utile si vous avez installé Kaspersky Internet Security sur votre ordinateur chez vous et au bureau.

Les paramètres de fonctionnement de l'application sont enregistrés dans un fichier de configuration spécial que vous pouvez transférer d'un ordinateur à l'autre. Voici la marche est à suivre :

1. Réalisez une *exportation* : enregistrez les paramètres de fonctionnement de l'application dans un fichier de configuration.

2. Transférez le fichier créé sur un autre ordinateur (par exemple, envoyez-le par courrier électronique ou via une clé USB).

3. Réalisez une *importation* : appliquez les paramètres du fichier de configuration au programme installé sur l'autre ordinateur.

*Pour exporter les paramètres actuels de fonctionnement de Kaspersky Internet Security, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, sélectionnez la rubrique **Administration des paramètres**.
3. Dans le groupe **Restauration des paramètres standard**, cliquez sur le bouton **Exporter**.
4. Saisissez le nom du fichier de configuration dans la fenêtre qui s'ouvre et précisez l'emplacement de la sauvegarde.

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

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, sélectionnez la rubrique **Administration des paramètres**.
3. Dans le groupe **Restauration des paramètres standard**, cliquez sur le bouton **Télécharger**.
4. Dans la fenêtre qui s'ouvre, sélectionnez le fichier à utiliser pour importer les paramètres de Kaspersky Internet Security.

# UTILISATION DE KASPERSKY GADGET

Si vous utilisez Kaspersky Internet Security sur un ordinateur fonctionnant sous le système d'exploitation Microsoft Windows Vista ou Microsoft Windows 7, vous pouvez utiliser Kaspersky Gadget.

Le gadget apparaît automatiquement sur le Bureau après l'installation de Kaspersky Internet Security sur un ordinateur fonctionnant sous Microsoft Windows 7. Après l'installation de l'application sur un ordinateur tournant sous Microsoft Windows Vista, le gadget devra être ajouté manuellement au Volet Windows de Microsoft Windows (cf. la documentation du système d'exploitation).

L'indicateur de couleur du gadget signale l'état de la protection de votre ordinateur de la même manière que l'indicateur de l'état de la protection situé dans la fenêtre principale de l'application (cf. rubrique "Fenêtre principale de Kaspersky Internet Security" à la page 42). La couleur verte indique que l'ordinateur est protégé, la couleur jaune signale un problème dans la protection, la couleur rouge indique une menace sérieuse pour la sécurité de l'ordinateur. La couleur grise de l'indicateur indique que le fonctionnement de l'application a été arrêté.

L'aspect extérieur du gadget permet également de juger du chargement des mises à jour : au cours de la mise à jour des bases et des modules de l'application, une icône du globe en rotation apparaît au milieu du gadget.

À l'aide du gadget, vous pouvez exécuter les tâches principales suivantes :

- Lancer l'application, si son fonctionnement est arrêté ;
- Ouvrir le menu principal de l'application ;
- Rechercher la présence éventuelle de virus dans des objets en particuliers ;
- Ouvrir la fenêtre de consultation des nouvelles.

*Pour lancer l'application à l'aide du gadget,*

cliquez sur l'icône **Activer** située au milieu du gadget.

*Pour ouvrir la fenêtre principale de l'application à l'aide du gadget,*

cliquez sur l'icône Kaspersky Internet Security située au milieu du gadget.

*Pour rechercher la présence éventuelle de virus à l'aide du gadget,*

faites glisser l'objet sur le gadget.

Le processus d'exécution de la tâche apparaîtra dans la fenêtre **Recherche de virus** qui s'ouvre.

*Pour ouvrir la fenêtre de consultation des nouvelles à l'aide du gadget,*

cliquez sur l'icône  affichée au centre du Gadget lors de l'apparition des infos.

### Configuration du gadget

Vous pouvez configurer le gadget de telle manière que vous puissiez exécuter les actions suivantes à l'aide de ses boutons :

- modifier les paramètres de fonctionnement de l'application ;
- consulter les rapports de l'application ;
- utiliser le mode de lancement des applications dans l'Environnement protégé ;
- passer au Bureau protégé (uniquement pour les systèmes d'exploitation de 32 bits) ;
- consulter les rapports du Contrôle Parental ;
- consulter les informations sur l'activité de réseau (Surveillance du réseau) ;
- suspendre la protection.

De plus, vous pouvez modifier l'apparence du gadget en choisissant un autre skin.

*Pour configurer le gadget, procédez comme suit :*

1. Ouvrez la fenêtre de configuration du gadget en cliquant sur l'icône  qui apparaît dans le coin supérieur droit du gadget lorsque le curseur est placé sur celui-ci.
2. Des listes déroulantes **Icône de gauche** et **Icône de droite**, sélectionnez les actions qui doivent être exécutées lorsque vous cliquez sur le bouton gauche ou droit du gadget.
3. Sélectionnez le skin du gadget en cliquant sur les boutons  .
4. Cliquez sur le bouton **OK** afin d'enregistrer les modifications introduites.

# CONFIGURATION ETENDUE DE L'APPLICATION

Cette rubrique 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.

*Pour réaliser la configuration étendue de l'application, ouvrez la fenêtre de configuration d'une des méthodes suivantes :*

- Cliquez sur le lien **Configuration** situé dans la partie supérieure de la fenêtre principale de l'application ;
- Sélectionnez le point **Configuration** dans le menu contextuel de l'icône de l'application.

### DANS CETTE SECTION



# SELECTION DU MODE DE PROTECTION

Kaspersky Internet Security fonctionne par défaut dans le *mode automatiquement de la protection*. Dans ce mode, lors de l'apparition des événements dangereux, l'application applique automatiquement l'action recommandée par les experts de Kaspersky Lab. Vous pouvez installer un *mode de protection interactif*, pour que Kaspersky Internet Security vous informe sur tous les événements dangereux et suspects dans le système et offre la possibilité de prendre indépendamment la décision sur l'action proposée par l'application à appliquer.

*Pour sélectionner le mode de protection, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez la sous-section **Paramètres généraux**.
3. Dans le groupe **Protection interactive**, décochez ou cochez les cases selon le mode de protection que vous avez sélectionné :
   - Pour installer le mode de protection interactif, décochez la case **Sélectionner l'action automatiquement** ;
   - Pour installer le mode de protection automatique, cochez la case **Sélectionner l'action automatiquement**.

     Si vous ne souhaitez pas que Kaspersky Internet Security supprime les objets suspects en mode automatique, cochez la case **Ne pas supprimer les objets suspects**.

# ANALYSE DE L'ORDINATEUR

La recherche de virus et de vulnérabilités sur l'ordinateur est une des principales tâches qui garantira la protection de l'ordinateur. Il est indispensable de rechercher la présence éventuelle de virus à intervalle régulier afin d'éviter la propagation de programmes malveillants qui n'auraient pas été découverts par les composants de la protection, par exemple en raison d'un niveau de protection trop faible ou pour toute autre raison.

La recherche de vulnérabilités consiste à poser un diagnostic sur la sécurité du système d'exploitation et à identifier dans les applications les particularités qui pourraient être exploitées par des individus malintentionnés désireux de diffuser des objets malveillants ou d'accéder aux données personnelles.

Les rubriques suivantes contiennent des informations détaillées sur les particularités et les paramètres des tâches d'analyse ainsi que sur les niveaux de protection, les méthodes et les technologies d'analyse.

### DANS CETTE SECTION



# RECHERCHE DE VIRUS

Kaspersky Internet Security propose les tâches suivantes pour la recherche de virus :

- **Analyse des Objets**. Analyse des objets sélectionnés par l'utilisateur. Il est possible d'analyser n'importe quel objet du système de fichiers de l'ordinateur de la liste suivante : mémoire système, objets exécutés au démarrage du système, sauvegarde du système, bases de messagerie, disques durs, disques amovibles et disques de réseau.
- **Analyse complète**. Analyse minutieuse de tout le système. Les objets suivants sont analysés par défaut : mémoire système, objets exécutés au démarrage du système, sauvegarde, bases de messagerie, disques durs, disques de réseau et disques amovibles.
- **Analyse rapide**. Recherche de la présence éventuelle de virus dans les objets chargés lors du démarrage du système d'exploitation.

Les tâches d'analyse complète et d'analyse des secteurs importants sont des tâches spécifiques. Pour ces tâches, il est déconseillé de modifier la liste des objets à analyser.

Chaque tâche d'analyse est exécutée dans une zone définie et peut être lancée selon un horaire défini. De plus, chaque tâche d'analyse se distingue par un niveau de protection (ensemble de paramètres qui exercent une influence sur la minutie de l'analyse). Le mode de recherche des menaces à l'aide des signatures des bases de l'application est toujours activé par défaut. De plus, il est possible d'impliquer diverses méthodes et technologies (cf. page 79) d'analyse.

Après le lancement de la tâche d'analyse, la progression de cette dernière est présentée dans la rubrique **Analyse** de la fenêtre principale de Kaspersky Internet Security dans le champ sous le nom de la tâche exécutée.

Dès que Kaspersky Internet Security identifie une menace, il attribue un des états suivants à l'objet détecté :

- Etat de l'un des programmes malveillants (exemple, *virus*, *cheval de Troie*).
- *Probablement infecté* (suspect) lorsqu'il est impossible d'affirmer avec certitude si l'objet est infecté ou non. Le fichier contient peut-être une séquence de code propre aux virus ou la modification d'un code de virus connu.

Ensuite, l'application affiche une notification sur la menace détectée et exécute l'action définie. Vous pouvez modifier l'action exécutée après la découverte d'une menace.

Si vous travaillez en mode automatique (cf. section "Sélection du mode de protection" à la page 74), Kaspersky Internet Security appliquera automatiquement l'action recommandée par les experts de Kaspersky Lab en cas de découverte d'objets dangereux. Pour les objets malveillants, il s'agit de l'action **Réparer. Supprimer, si la réparation est impossible**, pour les objets suspects : **Mettre en quarantaine**.

Avant de réparer ou de supprimer un objet, Kaspersky Internet Security crée une copie de sauvegarde au cas où la restauration de l'objet serait requise par la suite ou si la possibilité de le réparer se présentait. Les objets suspects (potentiellement infectés) sont placés en quarantaine. Vous pouvez activer l'analyse automatique des fichiers en quarantaine après chaque mise à jour.

Les informations relatives aux résultats de l'analyse et à tous les événements survenus pendant l'exécution des tâches sont consignées dans le rapport de Kaspersky Internet Security.

## DANS CETTE SECTION

## MODIFICATION ET RESTAURATION DU NIVEAU DE PROTECTION

En fonction de vos besoins actuels, vous pouvez choisir un des niveaux prédéfinis de la protection ou configurer vous-même les paramètres.

Une fois que vous aurez configuré les paramètres d'exécution de la tâche de l'analyse, sachez que vous pourrez toujours revenir aux paramètres recommandés. Il s'agit des paramètres optimum recommandés par les experts de Kaspersky Lab et regroupés au sein du niveau de protection **Recommandé**.

*Afin de modifier le niveau de protection du courrier, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, sélectionnez dans la rubrique **Analyse de l'ordinateur** la tâche requise (**Analyse complète**, **Analyse rapide** ou **Analyse des objets**).
3. Pour la tâche sélectionnée, dans le groupe **Niveau de protection**, sélectionnez le niveau de protection requis ou cliquez sur le bouton **Configuration** afin de définir manuellement les paramètres d'analyse.

En cas de configuration manuelle, le nom du niveau de protection devient **Autre**.

*Pour restaurer les paramètres d'analyse recommandés, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, sélectionnez dans la rubrique **Analyse de l'ordinateur** la tâche requise (**Analyse complète**, **Analyse rapide** ou **Analyse des objets**).
3. Pour la tâche sélectionnée dans le groupe **Niveau de protection** cliquez sur le bouton **Par défaut**.

## PROGRAMMATION DE L'EXECUTION DE L'ANALYSE

Il est possible d'exécuter les tâches automatiquement en les programmant, à savoir en définissant la fréquence d'exécution de la tâche, l'heure d'exécution (le cas échéant), ainsi que des paramètres complémentaires.

Si l'exécution est impossible pour une raison quelconque (par exemple, l'ordinateur était éteint à ce moment), vous pouvez configurer le lancement automatique de la tâche ignorée dès que cela est possible. De plus, il est possible de programmer l'arrêt automatique de l'analyse quand l'économiseur d'écran se désactive ou quand l'ordinateur est déverrouillé. Cette possibilité permet de reporter le lancement de la tâche jusqu'à ce que l'utilisateur termine son travail sur l'ordinateur. Ainsi, la tâche d'analyse n'occupera pas les ressources de l'ordinateur pendant son exécution.

Le mode spécial d'analyse pendant le temps mort (cf. rubrique "Lancement des tâches pendant les temps morts de l'ordinateur" à la page 174) permet de lancer l'analyse de la mémoire système, du système et des objets de démarrage lorsque l'ordinateur n'est pas utilisé.

*Pour programmer l'exécution de la tâche d'analyse, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, sélectionnez dans la rubrique **Analyse de l'ordinateur** la tâche requise (**Analyse complète**, **Analyse rapide**, **Analyse des objets** ou **Recherche de vulnérabilités**).
3. Pour la tâche sélectionnée dans le groupe **Mode d'exécution**, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Mode d'exécution**, groupe **Programmation**, sélectionnez le mode d'exécution.

*Pour activer l'exécution automatique d'une tâche d'analyse qui n'aurait pas été exécutée, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, sélectionnez dans la rubrique **Analyse de l'ordinateur** la tâche requise (**Analyse complète**, **Analyse rapide**, **Analyse des objets** ou **Recherche de vulnérabilités**).
3. Pour la tâche sélectionnée dans le groupe **Mode d'exécution**, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Mode d'exécution**, groupe **Programmation**, cochez la case **Lancer les tâches non exécutées**.

*Pour lancer l'analyse une fois que l'utilisateur aura terminé son travail, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, sélectionnez dans la rubrique **Analyse de l'ordinateur** la tâche requise (**Analyse complète**, **Analyse rapide**, **Analyse des objets** ou **Recherche de vulnérabilités**).
3. Pour la tâche sélectionnée dans le groupe **Mode d'exécution**, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Mode d'exécution**, dans le groupe **Programmation**, cochez la case **Suspendre l'analyse selon la programmation si l'écran de veille est inactif et l'ordinateur est débloqué**.

## COMPOSITION DE LA LISTE DES OBJETS A ANALYSER

Une liste d'objets à analyser est associée par défaut à chaque tâche de recherche d'éventuels virus. Ces objets peuvent être des objets du système de fichiers de l'ordinateur (par exemple, les disques logiques, les **bases de messagerie**) ainsi que des objets d'autres types (par exemple, des disques de réseau). Vous pouvez introduire des modifications dans cette liste.

Si la zone d'analyse est vide ou si aucun des objets qu'elle contient n'a été coché, il ne sera pas possible de lancer la tâche d'analyse.

*Pour composer la liste des objets à analyser, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie gauche de la fenêtre, sélectionnez la section **Analyse**.
3. Dans la partie droite de la fenêtre, cliquez sur le lien **sélectionnez** afin d'ouvrir la liste des objets à analyser.
4. Dans la fenêtre **Analyse des objets** qui s'ouvre, cliquez sur le lien **Ajouter** pour ouvrir la fenêtre d'ajout d'objets.
5. Dans la fenêtre **Sélection de l'objet à analyser** qui s'ouvre, sélectionnez l'objet et cliquez sur le bouton **Ajouter**. Une fois que vous aurez ajouté tous les objets requis, cliquez sur le bouton **OK**. Pour exclure un objet quelconque de la liste, désélectionnez la case située en regard de celui-ci.

   Vous pouvez également transférer directement les fichiers à analyser dans un secteur spécial de la rubrique **Analyse**.

*Pour composer la liste des objets pour les analyses complète ou rapide, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Analyse de l'ordinateur**, sélectionnez la tâche **Analyse Complète** ou **Analyse rapide**.
3. Pour la tâche sélectionnée, dans le groupe **Objets à analyser**, cliquez sur le bouton **Configuration**.

4. Dans la fenêtre **<Nom de l'analyse>: les objets à analyser**, composez la liste à l'aide des liens **Ajouter**, **Modifier** ou **Supprimer**. Pour exclure un objet quelconque de la liste, désélectionnez la case située en regard de celui-ci.

Les objets ajoutés à la liste par défaut ne peuvent être modifiés ou supprimés.

## SELECTION DE LA METHODE D'ANALYSE

La recherche d'éventuels virus sur l'ordinateur s'opère toujours selon l'*analyse sur la base des signatures* au cours de laquelle Kaspersky Internet Security compare l'objet trouvé aux signatures des bases.

Pour renforcer l'efficacité de la recherche, vous pouvez activer des méthodes d'analyse complémentaires : *analyse heuristique* (analyse de l'activité de l'objet dans le système) et *recherche d'outils de dissimulation d'activité* (utilitaires qui permettent de dissimuler les programmes malveillants dans le système d'exploitation).

*Pour utiliser les méthodes d'analyse requises, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, sélectionnez dans la rubrique **Analyse de l'ordinateur** la tâche requise (**Analyse complète**, **Analyse rapide** ou **Analyse des objets**).
3. Pour la tâche sélectionnée dans le groupe **Niveau de protection** cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Avancé**, dans le groupe **Méthodes d'analyse**, définissez les paramètres requis.

## SELECTION DE LA TECHNOLOGIE D'ANALYSE

Outre le choix des méthodes d'analyse, vous pouvez faire intervenir des technologies spéciales qui permettent d'optimiser la vitesse de la recherche de virus en excluant les fichiers qui n'ont pas été modifiés depuis la dernière analyse.

*Pour activer les technologies d'analyse des objets, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, sélectionnez dans la rubrique **Analyse de l'ordinateur** la tâche requise (**Analyse complète**, **Analyse rapide** ou **Analyse des objets**).
3. Pour la tâche sélectionnée dans le groupe **Niveau de protection** cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Avancé**, dans le bloc **Technologies d'analyse**, définissez les paramètres requis.

## MODIFICATION DE L'ACTION A EXECUTER APRES LA DECOUVERTE D'UNE MENACE

En cas de découverte d'objets infectés ou potentiellement infectés, l'application exécute l'action définie.

*Pour modifier l'action à exécuter sur les objets découverts, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, sélectionnez dans la rubrique **Analyse de l'ordinateur** la tâche requise (**Analyse complète**, **Analyse rapide** ou **Analyse des objets**).

3. Dans la partie droite de la fenêtre, dans le groupe **Action en cas de découverte d'une menace**, sélectionnez l'option requise.

## LANCEMENT DE L'ANALYSE SOUS LES PRIVILEGES D'UN AUTRE UTILISATEUR

La mise à jour est lancée par défaut sous le compte que vous avez utilisé pour ouvrir votre session dans le système. Toutefois, il peut s'avérer parfois nécessaire d'exécuter une tâche sous les privilèges d'un autre utilisateur. Vous pouvez désigner le compte utilisateur sous les privilèges duquel chaque tâche d'analyse sera exécutée.

*Pour lancer l'analyse sous les privilèges d'un autre utilisateur, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, sélectionnez dans la rubrique **Analyse de l'ordinateur** la tâche requise (**Analyse complète**, **Analyse rapide**, **Analyse des objets** ou **Recherche de vulnérabilités**).
3. Pour la tâche sélectionnée dans le groupe **Mode d'exécution**, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Mode d'exécution**, dans le groupe **Utilisateur** cochez la case ☑ **Lancer la tâche avec les privilèges de l'utilisateur**. Saisissez le nom de l'utilisateur et le mot de passe dans les champs en bas.

## MODIFICATION DU TYPE D'OBJETS A ANALYSER

La définition du type d'objet à analyser est la fonction qui vous permet d'indiquer le format et la taille des fichiers qui seront analysés lors de l'exécution de la tâche d'analyse sélectionnée.

Lors de la sélection du type de fichiers, rappelez-vous des éléments suivants :

- La probabilité d'insertion d'un code malveillant dans les fichiers de certains formats (par exemple txt) et son activation ultérieure est relativement faible. Mais il existe également des formats de fichier qui contiennent ou qui pourraient contenir un code exécutable (par exemple, exe, dll, doc). Le risque d'intrusion et d'activation d'un code malveillant dans ces fichiers est assez élevé.
- Un individu mal intentionné peut envoyer un virus sur votre ordinateur dans un fichier exécutable renommé en fichier txt. Si vous avez sélectionné l'analyse des fichiers selon l'extension, ce fichier sera ignoré lors de l'analyse. Si vous avez choisi l'analyse des fichiers selon le format, alors l'Antivirus Fichiers analysera l'en-tête du fichier, quelle que soit l'extension, et identifiera le fichier comme étant au format exe. Le fichier sera alors soumis à une analyse antivirus minutieuse.

*Afin de modifier les types de fichiers à analyser, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, sélectionnez dans la rubrique **Analyse de l'ordinateur** la tâche requise (**Analyse complète**, **Analyse rapide** ou **Analyse des objets**).
3. Pour la tâche sélectionnée dans le groupe **Niveau de protection** cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Zone d'action** dans le groupe **Types de fichiers**, sélectionnez le paramètre requis.

## ANALYSE DES FICHIERS COMPOSES

L'insertion de virus dans des fichiers composés (archives, bases de données, etc.) est une pratique très répandue. Pour identifier les virus dissimulés de cette façon, il faut décompacter le fichier composé, ce qui peut entraîner un ralentissement significatif de l'analyse.

Pour chaque type de fichier composé, vous pouvez décider d'analyser tous les fichiers ou uniquement les nouveaux. Pour réaliser la sélection, cliquez sur le lien situé à côté du nom de l'objet. Il change de valeur lorsque vous appuyez sur

le bouton gauche de la souris. Si le mode d'analyse uniquement des nouveaux fichiers ou des fichiers modifiés (cf. page 81) est sélectionné, les liens pour la sélection de l'analyse de tous les fichiers ou des nouveaux fichiers uniquement seront inaccessibles.

Vous pouvez également définir la taille maximale du fichier composé à analyser. Les fichiers composés dont la taille dépasse la valeur définie ne seront pas analysés.

Lors de l'extraction d'archives, les fichiers de grande taille seront soumis à l'analyse antivirus même si la case **Ne pas décompacter les fichiers composés de grande taille** est cochée.

*Pour modifier la liste des fichiers composés à analyser, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, sélectionnez dans la rubrique **Analyse de l'ordinateur** la tâche requise (**Analyse complète**, **Analyse rapide** ou **Analyse des objets**).
3. Pour la tâche sélectionnée dans le groupe **Niveau de protection** cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Zone d'action** dans le groupe **Analyse des fichiers composés**, sélectionnez les types de fichiers composés à analyser.

*Pour définir la taille maximale des fichiers composés qui seront analysés, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, sélectionnez dans la rubrique **Analyse de l'ordinateur** la tâche requise (**Analyse complète**, **Analyse rapide** ou **Analyse des objets**).
3. Pour la tâche sélectionnée dans le groupe **Niveau de protection** cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, cliquez sur **Avancé** dans le groupe **Analyse des fichiers composés** de l'onglet **Zone d'action**.
5. Dans la fenêtre **Fichiers composés** qui s'ouvre, cochez la case **Ne pas décompacter les fichiers composés de grande taille** et définissez la taille maximale des fichiers à analyser.

## OPTIMISATION DE L'ANALYSE

Vous pouvez réduire la durée d'analyse et accélérer le fonctionnement de Kaspersky Internet Security. Pour ce faire, il faut analyser uniquement les nouveaux fichiers et ceux qui ont été modifiés depuis la dernière analyse. Ce mode d'analyse s'applique aussi bien aux fichiers simples qu'aux fichiers composés.

Il est également possible de limiter la durée de l'analyse d'un fichier. A l'issue du temps défini, le fichier sera exclu de l'analyse en cours.

*Afin d'analyser uniquement les nouveaux fichiers et les fichiers modifiés, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, sélectionnez dans la rubrique **Analyse de l'ordinateur** la tâche requise (**Analyse complète**, **Analyse rapide** ou **Analyse des objets**).
3. Pour la tâche sélectionnée dans le groupe **Niveau de protection** cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Zone d'action** dans le groupe **Optimisation de l'analyse**, cochez la case **Analyser uniquement les nouveaux fichiers et les fichiers modifiés**.

*Pour limiter la durée de l'analyse, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.

2. Dans la partie gauche de la fenêtre, sélectionnez dans la rubrique **Analyse de l'ordinateur** la tâche requise (**Analyse complète**, **Analyse rapide** ou **Analyse des objets**).

3. Pour la tâche sélectionnée dans le groupe **Niveau de protection** cliquez sur le bouton **Configuration**.

4. Dans la fenêtre qui s'ouvre, sous l'onglet **Zone d'action** dans le groupe **Optimisation de l'analyse**, cochez la case **Ignorer les fichiers si l'analyse dure plus de** et définissez la durée d'analyse d'un fichier.

## ANALYSE DES DISQUES AMOVIBLES A LA CONNEXION

Ces derniers temps, les objets malveillants qui exploitent les vulnérabilités du système d'exploitation pour se diffuser via les réseaux locaux et les disques amovibles sont fort répandus. Kaspersky Internet Security prend en charge la recherche de virus sur les disques amovibles lorsque ceux-ci sont connectés à l'ordinateur.

*Pour configurer l'analyse des disques amovibles lors de leur connexion à l'ordinateur, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.

2. Dans la partie gauche de la fenêtre, dans la section **Analyse de l'ordinateur**, sélectionnez la section **Paramètres généraux**.

3. Dans le groupe **Analyse des disques amovibles à la connexion**, sélectionnez l'action et, le cas échéant, définissez la taille maximale du disque à analyser dans le champ inférieur.

## CREATION D'UN RACCOURCI POUR LE LANCEMENT D'UNE TACHE

L'application prend en charge la création de raccourcis pour accélérer le lancement des analyses complètes et rapides ou de la recherche de vulnérabilités. Il est ainsi possible de lancer la tâche d'analyse requise sans devoir ouvrir la fenêtre principale de l'application ou le menu contextuel.

*Pour créer un raccourci pour le lancement de l'analyse, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.

2. Dans la partie gauche de la fenêtre, dans la section **Analyse de l'ordinateur**, sélectionnez la section **Paramètres généraux**.

3. Dans la partie droite de la fenêtre, dans le groupe **Lancement rapide des tâches**, cliquez sur le lien **Créer un raccourci** situé à côté du nom de la tâche envisagée (**Analyse rapide** ou **Analyse complète** ou **Recherche de Vulnérabilités**).

4. Dans la fenêtre qui s'ouvre, saisissez le chemin d'accès pour l'enregistrement du raccourci ainsi que le nom de celui-ci. Par défaut, le raccourci prend le nom de la tâche et est créé dans le répertoire *Poste de travail* de l'utilisateur actuel de l'ordinateur.

# RECHERCHE DE VULNERABILITES

Les vulnérabilités dans le système d'exploitation peuvent être le résultat d'erreurs de programmation ou de planification, de mots de passe faibles, de l'action de programmes malveillants, etc. La recherche de vulnérabilités consiste à étudier le système, à rechercher des anomalies et des corruptions dans les paramètres du système d'exploitation et du navigateur, à rechercher des services vulnérables et d'autres mesures de sécurité.

Le diagnostic peut durer un certain temps. Une fois qu'un problème a été identifié, il est analysé pour déterminer le danger qu'il représente.

Une fois que la tâche de recherche des vulnérabilités (cf. page 59) a été lancée, vous pouvez suivre sa progression dans le champ **Fin** de la fenêtre **Recherche de Vulnérabilités**. Les vulnérabilités identifiées dans le système et dans les applications à la suite de l'analyse figurent dans cette même fenêtre sous les onglets **Vulnérabilités du système** et **Applications vulnérables**.

Les informations sur les résultats de la recherche de menaces sont consignées dans le rapport de Kaspersky Internet Security.

Tout comme pour les tâches de recherche de virus, il est possible de programmer l'exécution de recherche de vulnérabilités, de composer la liste des objets à analyser (cf. page 78), de sélectionner le compte utilisateur (cf. rubrique "Lancement de l'analyse sous les privilèges d'un autre utilisateur" à la page 80) et de créer un raccourci pour l'exécution rapide de la tâche. Par défaut, les applications installées sont choisies en guise d'objets à analyser.

# MISE A JOUR

La mise à jour des bases et des modules logiciels de Kaspersky Internet Security préserve l'actualité de la protection de votre ordinateur. Chaque jour, de nouveaux virus, chevaux de Troie et autres programmes malveillants apparaissent dans le monde. Les bases de Kaspersky Internet Security contiennent les données relatives aux menaces et les méthodes de neutralisation. C'est la raison pour laquelle la mise à jour régulière de l'application est indispensable pour garantir la protection de l'ordinateur et la découverte des nouvelles menaces à temps.

La mise à jour régulière requiert une licence d'utilisation de l'application valide. En l'absence d'une telle licence, vous ne pourrez réaliser la mise à jour qu'une seule fois.

Lors de la mise à jour de l'application, les objets suivants sont téléchargés et installés sur votre ordinateur :

- Bases de Kaspersky Internet Security.

  La protection des données est garantie par l'utilisation de bases de données qui contiennent les signatures des menaces et des attaques de réseau ainsi que les méthodes de lutte contre celles-ci. Elles sont utilisées par les composants de la protection pour rechercher les objets dangereux sur votre ordinateur et les neutraliser. Ces bases sont enrichies régulièrement avec les définitions des nouvelles menaces et les moyens de lutter contre celles-ci. Pour cette raison, il est vivement recommandé de les actualiser régulièrement.

  En plus des bases de Kaspersky Internet Security, la mise à jour concerne également les pilotes de réseau qui assurent l'interception du trafic de réseau par les composants de la protection.

- Modules logiciels.

  Outre les bases de Kaspersky Internet Security, il est possible d'actualiser les modules logiciels. Les paquets de mise à jour permettent de supprimer les vulnérabilités de Kaspersky Internet Security, ajoutent de nouvelles fonctionnalités ou améliorent les fonctionnalités existantes.

Les serveurs spéciaux de mise à jour de Kaspersky Lab sont la principale source de mise à jour pour Kaspersky Internet Security. Pendant la mise à jour de Kaspersky Internet Security, vous pouvez copier les mises à jour des bases et des modules récupérés sur les serveurs de Kaspersky Lab dans un répertoire local, puis octroyer l'accès à ce répertoire aux autres ordinateurs du réseau. Vous économiserez ainsi du trafic Internet.

Vous pouvez également configurer les paramètres de lancement automatique de la mise à jour.

Pour que le téléchargement des mises à jour depuis les serveurs réussisse, l'ordinateur doit être connecté à Internet. Les paramètres de connexion à Internet sont définis automatiquement par défaut. Si vous utilisez un serveur proxy, il faudra peut-être configurer les paramètres de connexion à celui-ci.

Au cours du processus (cf. page 133) de mise à jour, les modules logiciels et les bases installés sur votre ordinateur sont comparés à ceux présents sur la source des mises à jour. Si les bases et les modules actuels diffèrent de la version à jour, la partie manquante des mises à jour sera installée sur l'ordinateur.

Si les bases sont fortement dépassées, la taille du paquet de mise à jour peut être considérable, ce qui augmentera le trafic Internet (de quelques dizaines de Mo).

Avant d'actualiser les bases, Kaspersky Internet Security crée une copie de sauvegarde au cas où vous souhaiteriez utiliser à nouveau les bases de la version antérieure.

Les informations relatives à l'état actuel des bases de Kaspersky Internet Security sont affichées dans la rubrique **Mise à jour** de la fenêtre principale de l'application.

Les informations relatives aux résultats de la mise à jour et à tous les événements survenus pendant l'exécution des tâches sont consignées dans le rapport de Kaspersky Internet Security.

### DANS CETTE SECTION



## SELECTION DE LA SOURCE DE MISES A JOUR

*La source des mises à jour* est une ressource qui contient les mises à jour des bases et des modules de Kaspersky Internet Security. En guise de source des mises à jour, vous pouvez désigner un serveur HTTP ou FTP, un répertoire local ou un répertoire de réseau.

Les serveurs de mise à jour de Kaspersky Lab, qui hébergent les mises à jour des bases et des modules pour tous les produits de Kaspersky Lab, sont la principale source de mises à jour.

Si vous ne pouvez pas accéder aux serveurs de mises à jour de Kaspersky Lab (par exemple, votre accès à Internet est limité), vous pouvez contacter notre siège social (http://www.kaspersky.com/fr/contacts) afin d'obtenir les adresses des partenaires de Kaspersky Lab qui pourront vous transmettre les mises à jour sur disque amovible.

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

Par défaut, la liste des sources de mises à jour contient uniquement les serveurs de mise à jour de Kaspersky Lab. Si plusieurs ressources ont été sélectionnées en guise de sources de mise à jour, Kaspersky Internet Security les consultera dans l'ordre de la liste et réalisera la mise à jour au départ de la première source disponible.

Si en guise de source de mises à jour vous avez sélectionné une ressource située hors de l'intranet, vous devrez être connecté à Internet pour télécharger la mise à jour.

*Pour sélectionner la source de mises à jour, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, choisissez dans la rubrique **Mise à jour** le composant **Paramètres de la mise à jour**.
3. Dans le groupe **Source des mises à jour**, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Source**, ouvrez la fenêtre de sélection en cliquant sur le lien **Ajouter**.

5. Dans la fenêtre **Source des mises à jour** qui s'ouvre, sélectionnez le dossier contenant les mises à jour ou saisissez l'adresse du serveur sur lequel il faut récupérer les mises à jour dans le champ **Source**.

## SELECTION DE LA REGION DU SERVEUR DE MISES A JOUR

Si vous utilisez les serveurs de Kaspersky Lab en guise de source de mises à jour, vous pouvez sélectionner le serveur en fonction de la situation géographique qui vous convient le mieux. Les serveurs de Kaspersky Lab sont répartis dans plusieurs pays.

En utilisant le serveur de mise à jour de Kaspersky Lab le plus proche, vous réduirez la durée nécessaire à la récupération des mises à jour. Par défaut, la sélection s'opère sur la base des informations géographiques reprises dans la base de registres système. Vous pouvez choisir la région manuellement.

*Pour choisir la région du serveur, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, choisissez dans la rubrique **Mise à jour** le composant **Paramètres de la mise à jour**.
3. Dans le groupe **Source des mises à jour**, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre sous l'onglet **Source**, dans le groupe **Paramètres régionaux**, choisissez l'option **Choisir dans la liste** et, dans la liste déroulante, sélectionnez le pays le plus proche de votre situation géographique actuelle.

## MISE A JOUR DEPUIS UN REPERTOIRE LOCAL

Afin d'économiser le trafic Internet, il est possible de configurer la mise à jour de Kaspersky Internet Security sur les ordinateurs du réseau depuis un répertoire local. Dans ce cas, un des ordinateurs du réseau récupère les mises à jour depuis les serveurs de Kaspersky Lab ou depuis une autre ressource en ligne contenant la version la plus récente des mises à jour. Les mises à jour récupérées sont copiées dans un dossier partagé. Les autres ordinateurs de réseau accèdent à ce dossier pour récupérer les mises à jour de Kaspersky Internet Security.

*Pour activer le mode de copie des mises à jour, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, choisissez dans la rubrique **Mise à jour** le composant **Paramètres de la mise à jour**.
3. Dans le groupe **Avancé**, cochez la case **Copier la mise à jour des bases dans le dossier** et dans le champ en dessous, saisissez le chemin d'accès au dossier partagé où seront stockées les mises à jour récupérées. Vous pouvez également choisir le dossier en cliquant sur le bouton **Parcourir**.

*Pour que la mise à jour pour cet ordinateur soit réalisée au départ du dossier partagé indiqué, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, choisissez dans la rubrique **Mise à jour** le composant **Paramètres de la mise à jour**.
3. Dans le groupe **Source des mises à jour**, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Source**, ouvrez la fenêtre de sélection en cliquant sur le lien **Ajouter**.
5. Dans la fenêtre **Source des mises à jour** qui s'ouvre, sélectionnez le répertoire ou saisissez son chemin d'accès complet dans le champ **Source**.

6. Sous l'onglet **Source**, désélectionnez la case ☑ **Serveurs de mise à jour de Kaspersky Lab**.

## PROGRAMMATION DE L'EXECUTION DE LA MISE A JOUR

Il est possible d'exécuter les tâches de mise à jour automatiquement en les programmant, à savoir en définissant la fréquence d'exécution de la tâche, l'heure d'exécution (le cas échéant), ainsi que des paramètres complémentaires.

Si l'exécution de la tâche est impossible pour une raison quelconque (par exemple, l'ordinateur était éteint à ce moment), vous pouvez configurer le lancement automatique de la tâche ignorée dès que cela est possible.

Vous pouvez également reporter le lancement automatique des tâches après le démarrage de l'application. Dans ce cas, toutes les tâches programmées seront lancées uniquement une fois que le délai défini après le démarrage de Kaspersky Internet Security sera écoulé.

Le mode spécial d'analyse pendant le temps mort (cf. rubrique "Lancement des tâches pendant les temps morts de l'ordinateur" à la page 174) permet de lancer la mise à jour automatique lorsque l'ordinateur n'est pas utilisé.

*Pour programmer l'exécution de la tâche de mise à jour, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, choisissez dans la rubrique **Mise à jour** le composant **Paramètres de la mise à jour**.
3. Dans le groupe **Mode d'exécution**, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Mode d'exécution**, groupe **Programmation**, sélectionnez le mode d'exécution.

*Pour activer l'exécution automatique d'une tâche d'analyse qui n'aurait pas été exécutée, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, choisissez dans la rubrique **Mise à jour** le composant **Paramètres de la mise à jour**.
3. Dans le groupe **Mode d'exécution**, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Mode d'exécution**, groupe **Programmation**, cochez la case ☑ **Lancer les tâches non exécutées**.

*Pour reporter l'exécution des tâches après le démarrage de l'application, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, choisissez dans la rubrique **Mise à jour** le composant **Paramètres de la mise à jour**.
3. Dans le groupe **Mode d'exécution**, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Mode d'exécution**, dans le groupe **Programmation**, cochez la case ☑ **Intervalle entre le lancement et le démarrage de l'application** et indiquez le temps qui doit s'écouler avant l'exécution des tâches.

## ANNULATION DE LA DERNIERE MISE A JOUR

Après la première mise à jour des bases et des modules de Kaspersky Internet Security, vous aurez la possibilité de revenir à l'état antérieur à la mise à jour.

Chaque fois que vous lancez la mise à jour, Kaspersky Internet Security crée une copie de sauvegarde de la version actuelle des bases et des modules de l'application utilisés avant de les actualiser. Ceci permet de revenir, le cas échéant, à l'utilisation des bases antérieures. La possibilité de revenir à l'état antérieur de la mise à jour est utile, par exemple, si la nouvelle version des bases contient une signature incorrecte qui fait que Kaspersky Internet Security bloque une application sans danger.

Si les bases sont endommagées, Kaspersky Internet 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, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie gauche de la fenêtre sélectionnez la section **Mise à jour**.
3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Restaurer les mises à jour précédentes**.

## ANALYSE DE LA QUARANTAINE APRES LA MISE A JOUR

Si l'analyse de l'objet n'a pas permis de définir exactement la nature des programmes malveillants qui l'ont infecté, il est placé en quarantaine. Il se peut que les bases puissent identifier catégoriquement la menace après la prochaine mise à jour et la supprimer. Vous pouvez activer l'analyse automatique des objets en quarantaine après chaque mise à jour.

Nous vous conseillons d'examiner fréquemment les objets en quarantaine. Leur statut peut changer après l'analyse. Certains objets pourront être restaurés dans leur emplacement d'origine et être à nouveau utilisés.

*Pour activer l'analyse des objets en quarantaine après la mise à jour, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, choisissez dans la rubrique **Mise à jour** le composant **Paramètres de la mise à jour**.
3. Dans le groupe **Avancé**, cochez la case **Analyser les fichiers en quarantaine après une mise à jour**.

## UTILISATION DU SERVEUR PROXY

Si l'accès à Internet s'opère via un serveur proxy, il faut configurer ses paramètres pour réussir la mise à jour de Kaspersky Internet Security.

*Pour configurer les paramètres du serveur proxy, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, choisissez dans la rubrique Mise à jour le composant **Paramètres de la mise à jour**.
3. Dans le groupe **Source des mises à jour**, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Source**, cliquez sur le lien **Serveur proxy**.
5. Dans la fenêtre **Paramètres du serveur proxy** qui s'ouvre, configurez les paramètres du serveur proxy.

## LANCEMENT DE LA MISE A JOUR AVEC LES PRIVILEGES D'UN AUTRE UTILISATEUR

La mise à jour est lancée par défaut sous le compte que vous avez utilisé pour ouvrir votre session dans le système. Il arrive parfois que la mise à jour de Kaspersky Internet Security se déroule depuis une source à laquelle vous n'avez pas accès (par exemple, le répertoire de réseau contenant des mises à jour) ou pour laquelle vous ne jouissez pas des privilèges d'utilisateur autorisé du serveur proxy. Vous pouvez lancer la mise à jour de Kaspersky Internet Security au nom d'un utilisateur possédant ces privilèges.

*Pour lancer la mise à jour sous les privilèges d'un autre utilisateur, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, choisissez dans la rubrique **Mise à jour** le composant **Paramètres de la mise à jour**.
3. Dans le groupe **Mode d'exécution**, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Mode d'exécution**, dans le groupe **Utilisateur** cochez la case ☑ **Lancer la tâche avec les privilèges de l'utilisateur**. Saisissez le nom de l'utilisateur et le mot de passe dans les champs en bas.

# ANTIVIRUS FICHIERS

L'Antivirus Fichiers permet d'éviter l'infection du système de fichiers de l'ordinateur. Le composant est lancé au démarrage du système d'exploitation. Il se trouve en permanence dans la mémoire vive de l'ordinateur et il analyse tous les fichiers ouverts, enregistrés et exécutés sur l'ordinateur et sur tous les disques montés.

Vous pouvez désigner une zone à protéger et sélectionner le niveau de la protection (ensemble de paramètres ayant une influence sur la minutie de l'analyse).

Lorsque l'utilisateur ou une application sollicite le fichier protégé, l'Antivirus Fichiers recherche les données relatives à celui-ci dans les bases iChecker et iSwift et, sur la base des données obtenues, décide d'analyser ou non le fichier.

Le mode de recherche des menaces à l'aide des signatures des bases de l'application est toujours activé par défaut. De plus, il est possible d'utiliser également l'analyse heuristique (cf. page 92) et diverses technologies d'analyse (cf. page 92).

Dès que Kaspersky Internet Security identifie une menace, il attribue un des états suivants à l'objet détecté :

- Etat de l'un des programmes malveillants (exemple, *virus*, *cheval de Troie*).
- *Probablement infecté* (suspect) lorsqu'il est impossible d'affirmer avec certitude si l'objet est infecté ou non. Le fichier contient peut-être une séquence de code propre aux virus ou la modification d'un code de virus connu.

Ensuite, l'application affiche une notification sur la menace détectée et exécute l'action définie. Vous pouvez modifier l'action exécutée après la découverte d'une menace.

Si vous travaillez en mode automatique (cf. section "Sélection du mode de protection" à la page 74), Kaspersky Internet Security appliquera automatiquement l'action recommandée par les experts de Kaspersky Lab en cas de découverte d'objets dangereux. Pour les objets malveillants, il s'agit de l'action **Réparer. Supprimer, si la réparation est impossible**, pour les objets suspects : **Mettre en quarantaine**.

Avant de réparer ou de supprimer un objet, Kaspersky Internet Security crée une copie de sauvegarde au cas où la restauration de l'objet serait requise par la suite ou si la possibilité de le réparer se présentait. Les objets suspects (potentiellement infectés) sont placés en quarantaine. Vous pouvez activer l'analyse automatique des fichiers en quarantaine après chaque mise à jour.

**DANS CETTE SECTION**



# ACTIVATION ET DESACTIVATION DE L'ANTIVIRUS FICHIERS

Par défaut, l'Antivirus Fichiers est activé et fonctionne en mode optimal. Vous pouvez désactiver l'Antivirus Fichiers le cas échéant.

*Pour désactiver l'utilisation de l'Antivirus Fichiers, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Antivirus Fichiers**.
3. Dans la partie droite de la fenêtre, désélectionnez la case **Activer l'Antivirus Fichiers**.

# ARRET AUTOMATIQUE DE L'ANTIVIRUS FICHIERS

Lors de l'exécution de tâches qui requièrent des ressources importantes du système d'exploitation, il est possible de suspendre le fonctionnement de l'Antivirus Fichiers. Pour réduire la charge et garantir un accès rapide aux objets, vous pouvez configurer l'arrêt automatique du composant à l'heure indiquée ou en cas d'utilisation d'une application en particulier.

Suspendre l'Antivirus Fichiers en cas de conflit avec certaines applications est une mesure extrême ! Si des conflits se manifestent pendant l'utilisation du composant, contactez le Service d'assistance technique de Kaspersky Lab (http://support.kaspersky.com/fr). Les experts vous aideront à garantir le fonctionnement de Kaspersky Internet Security avec d'autres applications sur votre ordinateur.

*Pour suspendre le fonctionnement du composant à une heure définie, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Antivirus Fichiers**.
3. Dans la partie droite de la fenêtre, dans le groupe **Niveau de protection**, cliquez sur **Configuration**.

4. Dans la fenêtre qui s'ouvre, sous l'onglet **Avancé**, dans le groupe **Suspension de la tâche**, cochez la case ☑ **Selon la programmation**, puis cliquez sur **Programmation**.

5. Dans la fenêtre **Suspension de la tâche**, indiquez la durée (au format hh:mm) pendant laquelle la protection sera suspendue (champs **Pause à partir de** et **Reprendre à**).

*Pour suspendre le fonctionnement du composant lors du lancement de certaines applications, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.

2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Antivirus Fichiers**.

3. Dans la partie droite de la fenêtre, dans le groupe **Niveau de protection**, cliquez sur **Configuration**.

4. Dans la fenêtre qui s'ouvre, sous l'onglet **Avancé**, dans le groupe **Suspension de la tâche**, cochez la case ☑ **Au lancement des applications** puis cliquez sur **Liste**.

5. Dans la fenêtre **Applications**, composez la liste des applications pendant l'utilisation desquelles le composant sera suspendu.

# CONSTITUTION DE LA ZONE DE PROTECTION

La zone de protection fait référence à l'emplacement des objets et aux types de fichiers à analyser. Kaspersky Internet Security analyse par défaut uniquement les fichiers qui pourraient être infectés et qui sont exécutés sur tous les disques durs, les disques amovibles et les disques de réseau.

Vous pouvez élargir ou restreindre la zone de protection en ajoutant ou en supprimant des objets ou en modifiant le type de fichiers à analyser. Par exemple, vous pouvez décider d'analyser uniquement les fichiers exe exécutés depuis des disques de réseau.

Lors de la sélection du type de fichiers, rappelez-vous des éléments suivants :

- La probabilité d'insertion d'un code malveillant dans les fichiers de certains formats (par exemple txt) et son activation ultérieure est relativement faible. Mais il existe également des formats de fichier qui contiennent ou qui pourraient contenir un code exécutable (par exemple, exe, dll, doc). Le risque d'intrusion et d'activation d'un code malveillant dans ces fichiers est assez élevé.

- Un individu mal intentionné peut envoyer un virus sur votre ordinateur dans un fichier exécutable renommé en fichier txt. Si vous avez sélectionné l'analyse des fichiers selon l'extension, ce fichier sera ignoré lors de l'analyse. Si vous avez choisi l'analyse des fichiers selon le format, alors l'Antivirus Fichiers analysera l'en-tête du fichier, quelle que soit l'extension, et identifiera le fichier comme étant au format exe. Le fichier sera alors soumis à une analyse antivirus minutieuse.

*Afin de modifier la liste des objets à analyser, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.

2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Antivirus Fichiers**.

3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Configuration**.

4. Dans la fenêtre qui s'ouvre, dans le groupe **Zone de protection** de l'onglet **Général**, ouvrez la fenêtre de sélection des objets en cliquant sur le lien **Ajouter**.

5. Dans la fenêtre **Sélection de l'objet à analyser**, sélectionnez l'objet et cliquez sur le bouton **Ajouter**.

6. Après avoir ajouté tous les fichiers requis, cliquez sur **OK** dans la fenêtre **Sélection de l'objet à analyser**.

7. Pour exclure un objet de la liste, désélectionnez la case située en regard de celui-ci.

*Afin de modifier les types de fichiers à analyser, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Antivirus Fichiers**.
3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Général** dans le bloc **Type de fichiers**, sélectionnez le paramètre requis.

## MODIFICATION ET RESTAURATION DU NIVEAU DE PROTECTION

En fonction des besoins actuels, vous pourrez choisir un des niveaux de protection prédéfinis pour les fichiers ou la mémoire ou configurer vous-même les paramètres de fonctionnement de l'Antivirus Fichiers.

Sachez que si vous configurez les paramètres de fonctionnement de l'Antivirus Fichiers, vous pourrez toujours revenir aux paramètres recommandés. Il s'agit des paramètres optimum recommandés par les experts de Kaspersky Lab et regroupés au sein du niveau de protection **Recommandé**.

*Pour modifier le niveau de protection défini des fichiers et de la mémoire, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Antivirus Fichiers**.
3. Dans le groupe **Niveau de protection** de la partie droite de la fenêtre, sélectionnez le niveau de protection requis ou cliquez sur le bouton **Configuration** afin de définir manuellement les paramètres d'analyse.

   En cas de configuration manuelle, le nom du niveau de protection devient **Autre**.

*Pour restaurer les paramètres de protection par défaut, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Antivirus Fichiers**.
3. Dans la partie droite de la fenêtre, dans le groupe **Niveau de protection**, cliquez sur **Par défaut**.

## SELECTION DU MODE D'ANALYSE

Le mode d'analyse désigne la condition de déclenchement de l'Antivirus Fichiers. Kaspersky Internet Security utilise par défaut le mode intelligent dans lequel la décision d'analyser un objet est prise sur la base des opérations exécutées avec celui-ci. Par exemple, dans le cas d'un fichier Microsoft Office, Kaspersky Internet Security analyse le fichier à la première ouverture et à la dernière fermeture. Toutes les opérations intermédiaires sur le fichier sont exclues de l'analyse.

Vous pouvez modifier le mode d'analyse des objets. La sélection du mode dépend du type de fichiers que vous manipulez le plus souvent.

*Afin de modifier le mode d'analyse des objets, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Antivirus Fichiers**.
3. Dans la partie droite de la fenêtre, dans le groupe **Niveau de protection**, cliquez sur **Configuration**.

4. Dans la fenêtre qui s'ouvre, sous l'onglet **Avancé** dans le groupe **Mode d'analyse**, sélectionnez le mode requis.

## UTILISATION DE L'ANALYSE HEURISTIQUE

L'Antivirus Fichiers utilise toujours l'*analyse sur la base des signatures* au cours de laquelle Kaspersky Internet Security compare l'objet trouvé aux signatures des bases.

Pour augmenter l'efficacité de la protection, vous pouvez utiliser *l'analyse heuristique* (analyse de l'activité de l'objet dans le système). Cette analyse permet d'identifier de nouveaux objets malveillants dont les définitions n'ont pas encore été ajoutées aux bases.

- *Pour activer l'utilisation de l'analyse heuristique, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Antivirus Fichiers**.
3. Dans la partie droite de la fenêtre, dans le groupe **Niveau de protection**, cliquez sur **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Performance** dans le groupe **Méthode d'analyse**, cochez la case **Analyse heuristique** et définissez le niveau de détail de l'analyse.

## SELECTION DE LA TECHNOLOGIE D'ANALYSE

En plus de l'analyse heuristique, vous pouvez faire intervenir des technologies spéciales qui permettent d'optimiser la vitesse de la recherche de virus en excluant les fichiers qui n'ont pas été modifiés depuis la dernière analyse.

- *Pour activer les technologies d'analyse des objets, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Antivirus Fichiers**.
3. Dans la partie droite de la fenêtre, dans le groupe **Niveau de protection**, cliquez sur **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Avancé**, dans le groupe **Technologies d'analyse**, définissez les paramètres requis.

## MODIFICATION DE L'ACTION A REALISER SUR LES OBJETS IDENTIFIES

En cas de découverte d'objets infectés ou potentiellement infectés, l'application exécute l'action définie.

- *Pour modifier l'action à exécuter sur les objets découverts, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Antivirus Fichiers**.
3. Dans la partie droite de la fenêtre, dans le groupe **Action en cas de découverte d'une menace**, sélectionnez l'option requise.

# ANALYSE DES FICHIERS COMPOSES

L'insertion de virus dans des fichiers composés (archives, bases de données, etc.) est une pratique très répandue. Pour identifier les virus dissimulés de cette façon, il faut décompacter le fichier composé, ce qui peut entraîner un ralentissement significatif de l'analyse.

Pour chaque type de fichier composé, vous pouvez décider d'analyser tous les fichiers ou uniquement les nouveaux. Pour réaliser la sélection, cliquez sur le lien situé à côté du nom de l'objet. Il change de valeur lorsque vous appuyez sur le bouton gauche de la souris. Si le mode d'analyse uniquement des nouveaux fichiers ou des fichiers modifiés (cf. page 94) est sélectionné, les liens pour la sélection de l'analyse de tous les fichiers ou des nouveaux fichiers uniquement seront inaccessibles.

Kaspersky Internet Security analyse par défaut uniquement les objets OLE joints.

Lors de l'analyse de fichiers composés de grande taille, le décompactage préalable peut prendre un certain temps. Il est possible de réduire la durée en activant le décompactage en arrière plan des fichiers composés dont la taille dépasse la limite définie. Si un objet malveillant est découvert pendant l'utilisation de ces fichiers, Kaspersky Internet Security vous le signale.

Vous pouvez également définir la taille maximale du fichier composé à analyser. Les fichiers composés dont la taille dépasse la valeur définie ne seront pas analysés.

Lors de l'extraction d'archives, les fichiers de grande taille seront soumis à l'analyse antivirus même si la case ☑ **Ne pas décompacter les fichiers composés de grande taille** est cochée.

- *Pour modifier la liste des fichiers composés à analyser, procédez comme suit :*

  1. Ouvrez la fenêtre de configuration de l'application.
  2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Antivirus Fichiers**.
  3. Dans la partie droite de la fenêtre, dans le groupe **Niveau de protection**, cliquez sur **Configuration**.
  4. Dans la fenêtre qui s'ouvre, dans le groupe **Analyse des fichiers composés** de l'onglet **Performance**, sélectionnez les types de fichiers composés à analyser.

- *Pour définir la taille maximale des fichiers composés qui seront analysés, procédez comme suit :*

  1. Ouvrez la fenêtre de configuration de l'application.
  2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Antivirus Fichiers**.
  3. Dans la partie droite de la fenêtre, dans le groupe **Niveau de protection**, cliquez sur **Configuration**.
  4. Dans la fenêtre qui s'ouvre, cliquez sur **Avancé** dans le groupe **Analyse des fichiers composés** de l'onglet **Performance**.
  5. Dans la fenêtre **Fichiers composés**, cochez la case ☑ **Ne pas décompacter les fichiers composés de grande taille** et définissez la taille maximale des fichiers à analyser.

- *Pour décompacter les fichiers composés de grande taille en arrière plan, procédez comme suit :*

  1. Ouvrez la fenêtre de configuration de l'application.
  2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Antivirus Fichiers**.
  3. Dans la partie droite de la fenêtre, dans le groupe **Niveau de protection**, cliquez sur **Configuration**.
  4. Dans la fenêtre qui s'ouvre, cliquez sur **Avancé** dans le groupe **Analyse des fichiers composés** de l'onglet **Performance**.

5. Dans la fenêtre **Fichiers composés**, cochez la case **Décompacter les fichiers composés en arrière-plan** et définissez la taille minimale du fichier dans le champ en dessous.

## OPTIMISATION DE L'ANALYSE

Vous pouvez réduire la durée d'analyse et accélérer le fonctionnement de Kaspersky Internet Security. Pour ce faire, il faut analyser uniquement les nouveaux fichiers et ceux qui ont été modifiés depuis la dernière analyse. Ce mode d'analyse s'applique aussi bien aux fichiers simples qu'aux fichiers composés.

*Afin d'analyser uniquement les nouveaux fichiers et les fichiers modifiés, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Antivirus Fichiers**.
3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Performance**, dans le groupe **Optimisation de l'analyse**, cochez la case **Analyser uniquement les nouveaux fichiers et les fichiers modifiés**.

# ANTIVIRUS COURRIER

L'Antivirus Courrier analyse le courrier entrant et sortant à la recherche d'objets dangereux. Il est lancé au démarrage du système d'exploitation, se trouve en permanence dans la mémoire vive de l'ordinateur et analyse tous les messages envoyés et reçus via les protocoles POP3, SMTP, IMAP, MAPI1 et NNTP ainsi que les messages envoyés via des connexions sécurisées (SSL) via les protocoles POP3 et IMAP.

L'icône de Kaspersky Internet Security dans la zone de notification de la barre des tâches indique le fonctionnement du composant. Cette icône prend cette apparence chaque fois qu'un message est analysé.

Vous pouvez désigner les types de messages qu'il faut analyser et sélectionner le niveau de protection (cf. page 96) (ensemble de paramètres exerçant une influence sur la minutie de l'analyse).

Chaque message, reçu ou envoyé par l'utilisateur, est intercepté et décomposé entre ses différentes parties : en-tête du message, corps, pièce jointe. Le corps et la pièce jointe du message (y compris les objets OLE) sont soumis à la recherche de menaces.

Le mode de recherche des menaces à l'aide des signatures des bases de l'application est toujours activé par défaut. Il est également possible d'utiliser l'analyse heuristique. De plus, vous pouvez activer le filtrage des pièces jointes (cf. page 97) qui permet de renommer automatiquement ou de supprimer les fichiers du type défini.

Dès que Kaspersky Internet Security identifie une menace, il attribue un des états suivants à l'objet détecté :

- Etat de l'un des programmes malveillants (exemple, *virus*, *cheval de Troie*).
- *Probablement infecté* (suspect) lorsqu'il est impossible d'affirmer avec certitude si l'objet est infecté ou non. Le fichier contient peut-être une séquence de code propre aux virus ou la modification d'un code de virus connu.

Ensuite, l'application bloque le message, affiche une notification sur la menace détectée et exécute l'action définie. Vous pouvez modifier l'action exécutée après la découverte d'une menace (cf. rubrique "Modification de l'action à réaliser sur les objets découverts" à la page 97).

Si vous travaillez en mode automatique (cf. section "Sélection du mode de protection" à la page 74), Kaspersky Internet Security appliquera automatiquement l'action recommandée par les experts de Kaspersky Lab en cas de découverte d'objets dangereux. Pour les objets malveillants, il s'agit de l'action **Réparer. Supprimer, si la réparation est impossible**, pour les objets suspects : **Mettre en quarantaine**.

Avant de réparer ou de supprimer un objet, Kaspersky Internet Security crée une copie de sauvegarde au cas où la restauration de l'objet serait requise par la suite ou si la possibilité de le réparer se présentait. Les objets suspects (potentiellement infectés) sont placés en quarantaine. Vous pouvez activer l'analyse automatique des fichiers en quarantaine après chaque mise à jour.

Si la réparation réussit, l'utilisateur peut accéder au message. Dans le cas contraire, l'objet infecté est supprimé du message. Suite au traitement antivirus, un texte spécial est inclus dans l'objet du message. Ce texte indique que le message a été traité par Kaspersky Internet Security.

Un plug-in spécial (cf. section "Analyse du courrier dans Microsoft Office Outlook" à la page 98) qui permet de réaliser une configuration plus fine de l'analyse du courrier a été ajouté à Microsoft Office Outlook.

Si vous utilisez The Bat!, Kaspersky Internet Security peut être utilisé conjointement à d'autres logiciels antivirus. Dans ce cas, les règles de traitement du courrier (cf. section "Analyse du courrier dans The Bat!" à la page 98) sont définies directement dans The Bat! et prévalent sur les paramètres de protection du courrier de l'application.

S'agissant des autres clients de messagerie (dont Microsoft Outlook Express (Windows Mail), Mozilla Thunderbird, Eudora, Incredimail), l'Antivirus Courrier analyse le courrier entrant et sortant via les protocoles SMTP, POP3, IMAP et NNTP.

N'oubliez pas qu'en cas d'utilisation de client de messagerie Thunderbird, les messages transmis via le protocole IMAP ne sont pas soumis à l'analyse antivirus en cas d'utilisation de filtres triant les messages du dossier **Boîte aux lettres**.

### DANS CETTE SECTION



## ACTIVATION ET DESACTIVATION DE L'ANTIVIRUS COURRIER

Par défaut, l'Antivirus Courrier est activé et fonctionne en mode optimal. Vous pouvez désactiver l'Antivirus Courrier le cas échéant.

*Pour désactiver l'utilisation de l'Antivirus Courrier, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Antivirus Courrier**.
3. Dans la partie droite de la fenêtre, cochez la case ☑ **Activer l'Antivirus Courrier**.

# CONSTITUTION DE LA ZONE DE PROTECTION

La zone de protection désigne les types de message qu'il faut analyser. Kaspersky Internet Security analyse par défaut aussi bien les messages entrant que les messages sortant.

Si vous avez choisi l'analyse uniquement des messages entrant, il est conseillé au tout début de l'utilisation de Kaspersky Internet Security d'analyser le courrier sortant car le risque existe que votre ordinateur abrite des vers de messagerie qui se propagent via le courrier électronique. Vous éviterez ainsi les inconvénients liés à la diffusion non contrôlée de messages infectés depuis votre ordinateur.

La zone de protection reprend également les paramètres d'intégration de l'Antivirus Courrier dans le système ainsi que les protocoles analysés. Par défaut, l'Antivirus Courrier s'intègre aux clients de messagerie Microsoft Office Outlook et The Bat!.

*Pour désactiver la protection du courrier sortant, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Antivirus Courrier**.
3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, dans le groupe **Zone de protection** de l'onglet **Général**, sélectionnez l'option **Analyser uniquement le courrier entrant**.

*Pour sélectionner les paramètres d'intégration de l'Antivirus Courrier au système ainsi que les protocoles à analyser, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Antivirus Courrier**.
3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Configuration**.
4. De groupe **Intégration au système** de l'onglet **Avancé** de la fenêtre qui s'ouvre, sélectionnez les paramètres requis.

# MODIFICATION ET RESTAURATION DU NIVEAU DE PROTECTION

En fonction des besoins actuels, vous pourrez choisir un des niveaux de protection prédéfinis pour les fichiers ou la mémoire ou configurer vous-même les paramètres de fonctionnement de l'Antivirus Fichiers.

Les experts de Kaspersky Lab vous déconseillent de configurer vous-même les paramètres de l'Antivirus Courrier. Dans la majorité des cas, il suffit de sélectionner un autre niveau de protection.

Sachez que si vous configurez les paramètres de fonctionnement de l'Antivirus Fichiers, vous pourrez toujours revenir aux paramètres recommandés. Il s'agit des paramètres optimum recommandés par les experts de Kaspersky Lab et regroupés au sein du niveau de protection **Recommandé**.

*Afin de modifier le niveau de protection du courrier, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Antivirus Courrier**.
3. Dans le groupe **Niveau de protection** de la partie droite de la fenêtre, sélectionnez le niveau de protection requis ou cliquez sur le bouton **Configuration** afin de définir manuellement les paramètres d'analyse.

En cas de configuration manuelle, le nom du niveau de protection devient **Autre**.

*Pour restaurer les paramètres de protection du courrier par défaut, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Antivirus Courrier**.
3. Dans la partie droite de la fenêtre, dans le groupe **Niveau de protection**, cliquez sur **Par défaut**.

## UTILISATION DE L'ANALYSE HEURISTIQUE

L'Antivirus Courrier utilise toujours l'*analyse sur la base des signatures* au cours de laquelle Kaspersky Internet Security compare l'objet trouvé aux signatures des bases.

Pour augmenter l'efficacité de la protection, vous pouvez utiliser *l'analyse heuristique* (analyse de l'activité de l'objet dans le système). Cette analyse permet d'identifier de nouveaux objets malveillants dont les définitions n'ont pas encore été ajoutées aux bases.

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Antivirus Courrier**.
3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Général** dans le groupe **Méthode d'analyse** cochez la case **Analyse heuristique** et définissez le niveau de détail de l'analyse.

## MODIFICATION DE L'ACTION A REALISER SUR LES OBJETS IDENTIFIES

En cas de découverte d'objets infectés ou potentiellement infectés, l'application exécute l'action définie.

*Pour modifier l'action à exécuter sur les objets découverts, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Antivirus Courrier**.
3. Dans la partie droite de la fenêtre, dans le groupe **Action en cas de découverte d'une menace**, sélectionnez l'option requise.

## FILTRAGE DES PIECES JOINTES

Bien souvent, les programmes malveillants sont diffusés par courrier sous la forme d'objets joints aux messages. Pour protéger l'ordinateur, par exemple, contre l'exécution automatique du fichier en pièce jointe, vous pouvez activer le filtrage des pièces jointes qui permet de renommer automatiquement ou de supprimer les fichiers du type défini.

*Pour activer le filtrage des pièces jointes, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Antivirus Courrier**.
3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Configuration**.

4. Dans la fenêtre qui s'ouvre, sous l'onglet **Filtre des pièces jointes**, sélectionnez le mode de filtrage des pièces jointes. Lorsque les deux derniers modes sont sélectionnés, la liste des types d'objet (extension) devient active. Elle vous permet de sélectionner les types requis ou d'ajouter un masque d'un nouveau type.

   Pour ajouter un masque d'un nouveau type à la liste, cliquez sur le lien **Ajouter** et ouvrez la fenêtre **Masque de nom de fichiers**, puis saisissez les données requises.

## ANALYSE DES FICHIERS COMPOSES

L'insertion de virus dans des fichiers composés (archives, bases de données, etc.) est une pratique très répandue. Pour identifier les virus dissimulés de cette façon, il faut décompacter le fichier composé, ce qui peut entraîner un ralentissement significatif de l'analyse.

Vous pouvez activer ou désactiver l'analyse des archives jointes et limiter la taille maximale des archives à analyser.

Si votre ordinateur n'est protégé par aucun moyen du réseau local (l'accès à Internet s'opère sans serveur proxy ou pare-feu), il est conseillé de ne pas désactiver l'analyse des archives en pièce jointe.

*Pour configurer les paramètres d'analyse des fichiers composés, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Antivirus Courrier**.
3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Général**, définissez les paramètres requis.

## ANALYSE DU COURRIER DANS MICROSOFT OFFICE OUTLOOK

Si vous utilisez Microsoft Office Outlook, vous pouvez configurer des paramètres complémentaires pour la recherche de virus dans votre courrier.

Lors de l'installation de Kaspersky Internet Security, un plug-in spécial est intégré à Microsoft Office Outlook. Il permet de passer rapidement à la configuration des paramètres de l'Antivirus Courrier et de définir à quel moment la recherche d'éventuels objets dangereux sera lancée dans le message.

Le plug-in se présente sous la forme de l'onglet **Protection du courrier** situé dans le menu **Service** → **Paramètres**.

*Pour choisir le moment auquel l'analyse du courrier aura lieu, procédez comme suit :*

1. Ouvrez la fenêtre principale de Microsoft Office Outlook.
2. Dans le menu de l'application, choisissez l'option **Service** → **Paramètres**.
3. Sous l'onglet **Protection du courrier**, sélectionnez les paramètres requis.

## ANALYSE DU COURRIER DANS THE BAT!

Les actions à réaliser sur les objets infectés des messages électroniques dans The Bat! sont définies par le programme en lui-même.

Les paramètres de l'Antivirus Courrier qui définissent l'analyse ou non du courrier entrant et sortant ainsi que les actions à réaliser sur les objets dangereux de messages et les exclusions sont ignorées. Le seul élément pris en considération par The Bat!, c'est l'analyse des archives jointes.

Les paramètres de la protection du courrier sont diffusés à tous les composants antivirus installés sur l'ordinateur compatibles avec The Bat!.

Il ne faut pas oublier que lors de la réception de messages, ceux-ci sont d'abord analysés par l'Antivirus Courrier, puis ensuite uniquement après par le plug-in du client de messagerie The Bat!. Kaspersky Internet Security signalera sans défaut la découverte d'un objet malveillant. Si dans la fenêtre de notification de l'Antivirus Courrier vous choisissez l'option **Réparer** (**Supprimer**), les actions liées à la suppression de la menace seront exécutées par l'Antivirus Courrier. Si vous choisissez **Ignorer**, alors l'objet sera neutralisé par le plug-in de The Bat!. Lors de l'envoi de courrier, les messages sont d'abord analysés par le plug-in puis par l'Antivirus Courrier.

Vous devez définir les critères suivants :

- Le flux de messagerie qui sera soumis à l'analyse (courrier entrant, sortant) ;
- Le moment où il faudra analyser les objets du message (à l'ouverture du message, avant l'enregistrement sur le disque) ;
- Les actions exécutées par le client de messagerie en cas de découverte d'objets dangereux dans les messages électroniques. Vous pouvez par exemple choisir :
  - **Tenter de réparer les parties infectées** : quand cette option est choisie, une tentative de réparation de l'objet sera lancée. Si elle échoue, l'objet restera dans le message.
  - **Supprimer les parties infectées** : quand cette option est choisie, l'objet dangereux du message sera supprimé, qu'il soit infecté ou potentiellement infecté.

Par défaut, tous les objets infectés des messages sont placés en quarantaine par The Bat! sans réparation.

Les messages électroniques qui contiennent des objets dangereux ne sont pas différenciés dans The Bat! par un titre spécial.

*Pour configurer les paramètres de la protection du courrier dans The Bat!, procédez comme suit :*

1. Ouvrez la fenêtre principale de The Bat!.
2. Dans le menu **Propriétés** du client de messagerie, sélectionnez l'option **Configuration**.
3. Dans l'arborescence des paramètres, choisissez l'objet **Protection contre les virus**.

# ANTIVIRUS INTERNET

Chaque fois que vous utilisez Internet, vous exposez votre ordinateur et les données qu'il contient à un risque d'infection par des programmes dangereux. Ils peuvent s'infiltrer dans votre ordinateur tandis que vous téléchargez des programmes gratuits ou que vous consultez des informations sur des sites web apparemment inoffensifs, mais soumis à des attaques de pirates avant votre visite. De plus, les vers de réseau peuvent s'introduire sur votre ordinateur avant l'ouverture des pages Web ou le téléchargement d'un fichier, à savoir directement dès l'ouverture de la connexion Internet.

Le composant *Antivirus Internet* a été développé pour protéger votre ordinateur durant l'utilisation d'Internet. Il protège les informations reçues via les protocoles HTTP et HTTPS et empêche l'exécution des scripts dangereux.

La protection Internet prévoit le contrôle du flux de données qui transite uniquement via les ports indiqués dans la liste des ports contrôlés. La liste des ports le plus souvent utilisés pour le transfert de données est livrée avec Kaspersky Internet Security. Si vous utilisez des ports qui ne figurent pas dans cette liste, ajoutez-les à la liste des ports contrôlés (cf. rubrique "Composition de la liste des ports contrôlés" à la page 133) afin de garantir la protection du flux de données transitant par ceux-ci.

L'analyse du flux de données se déroule selon un ensemble défini de paramètres désigné sous le concept de niveau de protection (cf. rubrique "Sélection du niveau de protection pour l'Antivirus Internet" à la page 102). Quand l'Antivirus Internet découvre une menace, il exécute l'action définie.

Les experts de Kaspersky Lab vous déconseillent de configurer vous-même les paramètres de l'Antivirus Internet. Dans la majorité des cas, il suffit de sélectionner le niveau de protection qui convient.

### Algorithme de fonctionnement du composant

L'Antivirus Internet protège les informations qui arrivent sur l'ordinateur et qui sont envoyées depuis celui-ci via les protocoles HTTP et HTTPS et empêche l'exécution de scripts dangereux sur l'ordinateur. Par défaut, l'analyse des connexions cryptées (via le protocole HTTPS) est désactivée. Vous pouvez l'activer et la configurer (cf. rubrique "Analyse des connexions cryptées" à la page 130).

La protection des données s'opère selon l'algorithme suivant :

1. Chaque page ou fichier qui reçoit une requête de l'utilisateur ou d'un programme quelconque via le protocole HTTP ou HTTPS est intercepté et analysé par l'Antivirus Internet pour découvrir la présence éventuelle de code malveillant. L'identification des objets malveillants est réalisée à l'aide des bases utilisées par Kaspersky Internet Security et d'un algorithme heuristique. Les bases contiennent la définition de tous les programmes malveillants connus à ce jour et les moyens de les neutraliser. L'algorithme heuristique permet d'identifier les nouveaux virus dont les définitions ne sont pas encore reprises dans les bases.

2. Les comportements suivants sont possibles en fonction des résultats de l'analyse :

   - Si la page Web ou l'objet que souhaite ouvrir l'utilisateur contient un code malveillant, l'accès est bloqué. Dans ce cas, un message apparaît à l'écran pour avertir l'utilisateur que l'objet ou la page demandé est infecté.

   - Si aucun code malveillant n'a été découvert dans le fichier ou la page Web, l'utilisateur pourra y accéder immédiatement.

L'analyse des scripts est réalisée selon l'algorithme suivant :

1. Chaque script lancé est intercepté par l'Antivirus Internet et soumis à la recherche d'un code malveillant éventuel.

2. Si le script contient un code malveillant, l'Antivirus Internet le bloque et avertit l'utilisateur via un message spécial.

3. Si le script ne contient aucun code malveillant, le script est exécuté.

L'Antivirus Internet intercepte uniquement les scripts basés sur la technologie Microsoft Windows Script Host.

### DANS CETTE SECTION



# ACTIVATION ET DESACTIVATION DE L'ANTIVIRUS INTERNET

Deux méthodes s'offrent à vous pour activer ou désactiver le composant :

- Depuis la fenêtre principale de l'application (cf. section "Fenêtre principale de Kaspersky Internet Security" à la page 42) ;
- Depuis la fenêtre de configuration (cf. rubrique "Fenêtre de configuration des paramètres de l'application" à la page 46).

*Pour activer ou désactiver l'Antivirus Internet depuis la fenêtre principale, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et dans la partie gauche de la fenêtre, sélectionnez la rubrique **Protection**.
2. Dans la partie droite de la fenêtre, cliquez sur le bouton gauche de la souris et ouvrez le groupe **Contrôle de l'utilisation du réseau** ou **Protection du système et des applications**.
3. Ouvrez le menu des actions du composant en cliquant sur le bouton **Antivirus Internet**, puis sélectionnez l'option **Activer Antivirus Internet** pour l'activer ou **Désactiver Antivirus Internet** s'il faut désactiver le composant.

   Quand un composant est activé, l'icône à côté de son nom devient vert. Elle est grise lorsqu'il est désactivé.

*Pour activer ou désactiver l'Antivirus Internet depuis la fenêtre de configuration, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dan la section **Protection**, sélectionnez le composant **Antivirus Internet**.

3. Dans la partie droite de la fenêtre, cochez la case **Activer l'Antivirus Internet** s'il faut activer le composant. Décochez cette case s'il faut désactiver le composant.

## SELECTION DU NIVEAU DE PROTECTION POUR L'ANTIVIRUS INTERNET

Le niveau de protection désigne un ensemble de paramètres prédéfinis de l'Antivirus Internet qui assure un certain niveau de protection des données reçues ou envoyées via les protocoles HTTP et HTTPS. Les experts de Kaspersky Lab ont configuré trois niveaux de protection :

- élevé : garantit la protection maximale, indispensable dans un environnement dangereux ;
- recommandé : garantit la protection optimale, recommandé dans la majorité des cas ;
- faible : garantit l'exécution la plus rapide.

La sélection du niveau de protection est déterminée par l'utilisateur en fonction des conditions d'utilisation et de la situation en vigueur.

*Pour sélectionner un des niveaux de protection prédéfinis, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dan la section **Protection**, sélectionnez le composant **Antivirus Internet**.
3. Dans la partie droite de la fenêtre, sélectionnez le niveau de protection requis en déplaçant le curseur sur le niveau souhaité.

Si aucun des niveaux proposés ne répond à vos besoins, vous pouvez configurer les paramètres de fonctionnement de l'Antivirus Internet, par exemple modifier le niveau de détail de l'analyse dans le cadre de l'analyse heuristique. Si vous modifiez la configuration, le nom du niveau de protection devient **Autre**.

Si vous devez rétablir un des niveaux prédéfinis de protection, rétablissez les paramètres de fonctionnement de l'application (cf. rubrique "Restauration des paramètres de fonctionnement de l'Antivirus Internet" à la page 107).

## SELECTION DES ACTIONS A EXECUTER SUR LES OBJETS DANGEREUX

Si l'analyse d'un objet du trafic HTTP détermine la présence d'un code malveillant, la suite des opérations de l'Antivirus Internet dépendra de l'action que vous aurez spécifiée.

S'agissant des actions sur les scripts dangereux, l'Antivirus Internet bloque toujours leur exécution et affiche un message qui informe l'utilisateur sur l'action exécutée. La modification de l'action à réaliser sur un script dangereux n'est pas possible. Seule la désactivation de l'analyse des scripts est autorisée (cf. rubrique "Blocage des scripts dangereux" à la page 104).

Si vous travaillez en mode automatique, Kaspersky Internet Security appliquera automatiquement l'action recommandée par les experts de Kaspersky Lab en cas de découverte d'objets dangereux.

*Pour sélectionner l'action à exécuter sur les objets découverts, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dan la section **Protection**, sélectionnez le composant **Antivirus Internet**.
3. Dans le groupe **Action en cas de découverte d'une menace** de la partie droite de la fenêtre, sélectionnez l'action que l'application devra exécuter sur l'objet dangereux découvert.

# ANALYSE DES LIENS PAR RAPPORT AUX BASES D'URL DE PHISHING OU SUSPECTES

L'Antivirus Internet peut rechercher la présence éventuelle de virus dans le trafic HTTP et déterminer si les liens appartiennent à la liste des URL suspectes ou des URL de phishing.

L'analyse des liens pour voir s'ils appartiennent à la liste des adresses de phishing permet d'éviter les attaques de phishing qui, en règle générale, se présentent sous la forme de messages électroniques prétendument envoyés par une institution financière et qui contiennent des liens vers le site de ces institutions. Le texte du message invite le destinataire à cliquer sur le lien et à saisir des données confidentielles (numéro de carte de crédit, code d'accès aux services de banque en ligne) sur la page qui s'affiche. L'exemple type est le message envoyé par la banque dont vous êtes client et qui contient un lien vers un site officiel. En cliquant sur le lien, vous ouvrez en réalité une copie conforme du site Internet de la banque et il arrive même que l'adresse du site s'affiche, toutefois vous vous trouvez en fait sur un site fictif. Toutes vos actions sur ce site sont surveillées et pourraient servir au vol de votre argent.

La liste des adresses de phishing est reprise dans la distribution de Kaspersky Internet Security. Dans la mesure où le lien vers un site de phishing peut figurer non seulement dans un courrier, mais également dans un message ICQ, l'Antivirus Internet contrôle les tentatives d'accès à un site de phishing au niveau de l'analyse du trafic HTTP et bloque l'accès à ces sites Web.

*Pour que l'Antivirus Internet analyse les liens en fonction des bases d'URL suspectes ou de phishing, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dan la section **Protection**, sélectionnez le composant **Antivirus Internet**.
3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Configuration**.

   La fenêtre **Antivirus Internet** s'ouvre.
4. Vérifiez que sous l'onglet **Général**, dans le groupe **Méthodes d'analyse**, les cases **Analyser les liens selon la base des URL suspectes** et **Analyser les liens selon la base des URL de phishing** sont cochées.

# UTILISATION DE L'ANALYSE HEURISTIQUE

L'*analyse heuristique* est une méthode d'analyse particulière. Elle analyse l'activité de l'objet dans le système. Si cette activité est typique des objets malveillants, alors l'objet peut être considéré avec une certitude élevée comme un objet malveillant ou suspect, même si le code malveillant qu'il contient n'est pas encore connu des experts antivirus.

Vous pouvez sélectionner le niveau de détail de l'analyse pendant l'analyse heuristique :

- Superficielle : analyse rapide ;
- Minutieuse : analyse détaillée qui requiert beaucoup de temps ;
- Moyenne : combinaison optimale de vitesse et de profondeur de l'analyse, convient à la majorité des cas.

Si l'analyse heuristique décèle la présence d'un objet malveillant, Kaspersky Internet Security vous prévient et propose d'exécuter une action sur l'objet découvert.

L'analyse heuristique est activée par défaut et fonctionne selon le niveau **moyen**.

*Pour activer l'analyse heuristique et définir le niveau de détail ou pour désactiver cette analyse, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dan la section **Protection**, sélectionnez le composant **Antivirus Internet**.

3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Configuration**.

   La fenêtre **Antivirus Internet** s'ouvre.

4. Pour activer l'utilisation de l'analyse heuristique, sous l'onglet **Général** dans le groupe **Méthodes d'analyse**, cochez la case **Analyse heuristique**. Dans le champ du dessous, définissez le niveau de détail de l'analyse en déplaçant le curseur sur la position qui correspond au niveau souhaité. Décochez la case **Analyse heuristique** s'il n'est pas nécessaire d'utiliser ce mode d'analyse.

## BLOCAGE DES SCRIPTS DANGEREUX

L'Antivirus Internet peut analyser tous les scripts traités par Microsoft Internet Explorer ainsi que n'importe quel script WSH (JavaScript, Visual Basic Script, etc.) lancé pendant l'utilisateur travaille sur l'ordinateur. Si le script constitue une menace pour l'ordinateur, son exécution sera bloquée.

*Pour que l'Antivirus Internet analyse et bloque les scripts, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dan la section **Protection**, sélectionnez le composant **Antivirus Internet**.
3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Configuration**.

   La fenêtre **Antivirus Internet** s'ouvre.

4. Assurez-vous, sous l'onglet **Général** dans le groupe **Avancé**, que la case **Bloquer les scripts dangereux dans Microsoft Internet Explorer** est cochée.

## OPTIMISATION DE L'ANALYSE

Afin d'augmenter l'efficacité de la détection des codes malveillants, l'Antivirus Internet utilise la technologie de mise en cache de fragments des objets envoyés via Internet. Dans cette méthode, l'analyse de l'objet est réalisée uniquement une fois que l'objet entier a été reçu. Ensuite, l'objet est soumis à une recherche de virus et il est transmis à l'utilisateur ou bloqué en fonction des résultats de celle-ci.

Le recours à la mise en cache augmente la durée de traitement de l'objet et retarde son transfert à l'utilisateur. De plus, la mise en cache peut entraîner des problèmes lors du téléchargement et du traitement de grands objets en raison de l'expiration du délai d'attente de la connexion du client HTTP.

Pour résoudre ce problème, il est conseillé de limiter dans le temps la mise en cache des fragments des objets. Une fois le délai écoulé, chaque partie de l'objet reçue sera transmise à l'utilisateur sans vérification et l'objet sera analysé complètement une fois qu'il aura été copié. Ceci permet d'accélérer le transfert de l'objet à l'utilisateur et de résoudre le problème de la déconnexion. Le niveau de protection de l'utilisation d'Internet ne sera pas réduit pour la cause.

La levée de la restriction sur la durée de la mise en cache améliore l'efficacité de l'analyse antivirus mais provoque en même temps un léger ralentissement de l'accès à l'objet.

*Pour limiter la durée de la mise en cache des fragments ou pour supprimer cette limite, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dan la section **Protection**, sélectionnez le composant **Antivirus Internet**.
3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Configuration**.

   La fenêtre **Antivirus Internet** s'ouvre.

4. Pour limiter dans le temps la mise en cache du trafic, sous l'onglet **Général** du groupe **Avancé**, cochez la case **Limiter la durée de mise en cache du trafic pour l'optimisation de l'analyse**. S'il faut lever la restriction, décochez la case.

# MODULE D'ANALYSE DES LIENS

Kaspersky Internet Security propose un module d'analyse des liens qui est administré par l'Antivirus Internet. Le module est intégré aux navigateurs Microsoft Internet Explorer et Mozilla Firefox sous la forme d'un plug-in.

Le module analyse tous les liens sur une page afin de voir s'il s'agit de liens suspects ou de phishing. Vous pouvez composer la liste des URL des sites dont le contenu ne doit pas être soumis à la recherche de liens suspects ou de phishing, ainsi que la liste des URL de sites dont le contenu doit absolument être analysé. Vous pouvez également désactiver l'analyse des liens.

Les options de configuration reprises ci-dessous pour le module d'analyse des liens peuvent être réalisées non seulement dans la fenêtre de configuration de l'application, mais également dans la fenêtre de configuration du module ouvert depuis le navigateur.

- *Pour composer la liste des URL dont le contenu ne doit pas être soumis à la recherche de liens suspects ou de phishing, procédez comme suit :*

  1. Ouvrez la fenêtre de configuration de l'application.
  2. Dans la partie gauche de la fenêtre, dan la section **Protection**, sélectionnez le composant **Antivirus Internet**.
  3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Configuration**.

     La fenêtre **Antivirus Internet** s'ouvre.
  4. Sous l'onglet **Navigation sécurisée** dans le groupe **Module d'analyse des liens**, choisissez l'option **Vers toutes les URL, sauf les exceptions**, puis cliquez sur le bouton **Exclusions**.
  5. Dans la fenêtre **Exclusions** qui s'ouvre, composez la liste des URL des sites dont le contenu ne doit pas être soumis à la recherche de liens suspects ou de phishing.

- *Pour composer la liste des URL dont le contenu doit être soumis à la recherche de liens suspects ou de phishing, procédez comme suit :*

  1. Ouvrez la fenêtre de configuration de l'application.
  2. Dans la partie gauche de la fenêtre, dan la section **Protection**, sélectionnez le composant **Antivirus Internet**.
  3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Configuration**.

     La fenêtre **Antivirus Internet** s'ouvre.
  4. Sous l'onglet **Navigation sécurisée** dans le groupe **Module d'analyse des liens**, choisissez l'option **Uniquement vers les URL indiquées**, puis cliquez sur le bouton **Indiquer**.
  5. Dans la fenêtre **URL analysées** qui s'ouvre, composez la liste des URL des sites dont le contenu doit absolument être soumis à la recherche de liens suspects ou de phishing.

- *Pour qu'aucun lien ne soit analysé par le module, procédez comme suit :*

  1. Ouvrez la fenêtre de configuration de l'application.
  2. Dans la partie gauche de la fenêtre, dan la section **Protection**, sélectionnez le composant **Antivirus Internet**.
  3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Configuration**.

     La fenêtre **Antivirus Internet** s'ouvre.
  4. Sous l'onglet **Navigation sécurisée**, dans le groupe **Module d'analyse des liens**, sélectionnez l'option **Ne pas analyser les liens**.

*Pour ouvrir la fenêtre de configuration du module d'analyse des liens depuis la fenêtre du navigateur,*

cliquez sur le bouton avec l'icône de Kaspersky Internet Security dans la barre d'outils du navigateur.

## BLOCAGE DE L'ACCES AUX SITES DANGEREUX

Vous pouvez interdire l'accès aux sites considérés comme suspects ou de phishing suite à l'analyse réalisée par le module d'analyse des liens (cf. rubrique "Module d'analyse des liens" à la page 105).

Si l'application ne parvient pas à poser un diagnostic univoque sur la sécurité du site vers lequel le lien mène, vous aurez la possibilité d'ouvrir ce site en environnement protégé (cf. page 159) (uniquement lors de l'utilisation des navigateurs Internet Microsoft Internet Explorer et Mozilla Firefox). Dans l'environnement protégé, les objets malveillants ne constituent pas une menace pour l'ordinateur.

*Pour bloquer l'accès aux sites web dangereux, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dan la section **Protection**, sélectionnez le composant **Antivirus Internet**.
3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Configuration**.

   La fenêtre **Antivirus Internet** s'ouvre.
4. Sous l'onglet **Navigation sécurisée**, dans le groupe **Module du blocage des sites web dangereux**, cochez la case **Bloquer les sites web dangereux**.

## CONTROLE DES REQUETES ADRESSEES AUX DOMAINES REGIONAUX

L'Antivirus Internet, en mode de Filtrage par géo localisation, peut selon le choix de l'utilisateur interdire ou autoriser l'accès aux sites web sur la base de leur appartenance à des domaines régionaux de l'Internet. Il est ainsi possible, par exemple, d'interdire l'accès à des sites web appartenant à des domaines régionaux présentant un risque d'infection très élevé.

*Pour autoriser ou interdire l'accès aux sites web appartenant à des domaines précis, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dan la section **Protection**, sélectionnez le composant **Antivirus Internet**.
3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Configuration**.

   La fenêtre **Antivirus Internet** s'ouvre.
4. Sous l'onglet **Filtrage par géo localisation**, cochez la case **Filtrer la navigation Internet vers les sites étrangers** et dans la liste du dessous des domaines contrôlés, indiquez les domaines auxquels il faut autoriser ou interdire l'accès et les domaines pour lesquels l'application doit demander l'autorisation d'accès à l'aide d'une notification (cf. rubrique "Demande d'autorisation de connexion à un site du domaine régional" à la page 208).

   Pour les domaines régionaux correspondant à votre situation géographique, l'accès est autorisé par défaut. Pour les autres domaines, la demande d'autorisation d'accès est prévue par défaut.

## CONTROLE DES REQUETES ADRESSEES AUX SERVICES DE TRANSACTIONS BANCAIRES EN LIGNE

L'utilisateur qui emploie des services de transactions bancaires en ligne a besoin d'une protection particulière car dans ce cas-ci, la fuite d'informations confidentielles peut entraîner des pertes financières. L'Antivirus Internet peut contrôler

les requêtes adressées aux ressources que vous utilisez pour réaliser vos transactions bancaires en ligne et les ouvre dans le navigateur protégé, ce qui offre une couche de protection supplémentaire. L'Antivirus Internet définit automatiquement quelles sont les ressources Internet qui correspondent aux services de transactions bancaires en ligne. Pour une identification garantie d'une ressource Internet en tant que service de transactions bancaires en ligne, vous pouvez saisir son adresse dans la liste correspondante.

*Pour activer le contrôle des connexions aux services de transactions bancaires en ligne, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dan la section **Protection**, sélectionnez le composant **Antivirus Internet**.
3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Configuration**.

   La fenêtre **Antivirus Internet** s'ouvre.
4. Sous l'onglet **Banque en ligne** cochez la case **Activer le contrôle**. Vous serez invité à lancer l'Assistant d'installation des certificats, à l'aide duquel vous allez pouvoir installer le certificat de Kaspersky Lab pour analyser les connexions cryptées.
5. Le cas échéant, formez la liste des ressources qui doivent être obligatoirement identifiées par l'application comme services de transactions bancaires en ligne.

## COMPOSITION D'UNE LISTE D'ADRESSES DE CONFIANCE

Vous pouvez composer une liste d'URL dont le contenu ne présente absolument aucun danger. L'Antivirus Internet n'analysera pas les informations en provenance de ces adresses à la recherche d'objets dangereux. Cette fonctionnalité peut être utilisée, par exemple, si l'Antivirus Internet empêche le téléchargement d'un fichier depuis un site web que vous connaissez.

*Pour composer une liste d'URL de confiance, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dan la section **Protection**, sélectionnez le composant **Antivirus Internet**.
3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Configuration**.

   La fenêtre **Antivirus Internet** s'ouvre.
4. Sous l'onglet **Sites de confiance**, cochez la case **Ne pas analyser le trafic HTTP en provenance des URL de confiance** et composez la liste des adresses dont vous considérez le contenu comme étant fiable.

S'il faut à l'avenir exclure temporairement une adresse de la liste des sites de confiance, il n'est pas nécessaire de la supprimer de la liste. Il suffit simplement de décocher la case située à gauche.

## RESTAURATION DES PARAMETRES DE FONCTIONNEMENT DE L'ANTIVIRUS INTERNET

Si les résultats de la modification des paramètres de fonctionnement de l'Antivirus Internet ne vous conviennent pas, vous pouvez restaurer les paramètres recommandés par Kaspersky Lab. Ces paramètres sont repris dans le niveau de protection **Recommandé**.

*Pour restaurer les paramètres de fonctionnement par défaut de l'Antivirus Internet, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dan la section **Protection**, sélectionnez le composant **Antivirus Internet**.

3. Dans la partie droite de la fenêtre, dans le groupe **Niveau de protection**, cliquez sur **Par défaut**.

   Le niveau de protection prendra la valeur **Recommandé**.

# ANTIVIRUS IM ("CHAT")

L'Antivirus IM est prévu pour analyser le trafic transmis par les *clients de messageries instantanées*.

Les messages transmis via les clients de messagerie instantanée peuvent contenir des liens vers des sites web suspects ou vers des sites web utilisés par les individus mal intentionnés dans le cadre d'attaques de phishing. Les programmes malveillants utilisent les clients de messagerie instantanée pour diffuser des messages non sollicités ainsi que des liens vers des applications (voire les applications elles-mêmes) qui volent les numéros et les mots de passe des utilisateurs.

Kaspersky Internet Security garantit la sécurité des communications dans une multitude de clients de messagerie instantanée, y compris ICQ, MSN, AIM, Yahoo! Messenger, Jabber, Google Talk, Mail.Ru Agent et IRC.

Certains clients de messagerie instantanée, par exemple, Yahoo! Messenger et Google Talk utilisent une connexion sécurisée. Pour analyser le trafic de ces applications, il faut activer l'analyse des connexions cryptées (cf. page 130).

Les messages sont interceptés par l'Antivirus IM et soumis à la recherche d'objets dangereux ou de liens. Vous pouvez sélectionner les types de messages (cf. page 109) qu'il faut analyser et sélectionner les différentes méthodes d'analyse.

Quand il découvre une menace dans un message, l'Antivirus IM remplace le message par un avertissement pour l'utilisateur.

Les fichiers transmis par la messagerie instantanée sont analysés par l'Antivirus Fichiers pendant la tentative d'enregistrement.

### DANS CETTE SECTION



# ACTIVATION ET DESACTIVATION DE L'ANTIVIRUS IM

Par défaut, l'Antivirus IM est activé et fonctionne en mode optimal. Vous pouvez désactiver l'Antivirus IM le cas échéant.

*Pour désactiver l'utilisation de l'Antivirus IM, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Antivirus IM ("Chat")**.
3. Dans la partie droite de la fenêtre, désélectionnez la case **Activer l'Antivirus IM**.

## CONSTITUTION DE LA ZONE DE PROTECTION

La zone de protection désigne les types de message qu'il faut analyser. Kaspersky Internet Security analyse par défaut aussi bien les messages entrant que les messages sortant. Si vous êtes convaincu que les messages que vous envoyez ne peuvent contenir aucun objet dangereux, vous pouvez vous passer de l'analyse du trafic sortant.

- *Pour désactiver l'analyse des messages sortant, procédez comme suit :*

  1. Ouvrez la fenêtre de configuration de l'application.
  2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Antivirus IM ("Chat")**.
  3. Choisissez l'option **Analyser uniquement le courrier entrant** dans le groupe **Zone de protection** de la partie droite de la fenêtre.

## SELECTION DE LA METHODE D'ANALYSE

La méthode d'analyse désigne l'analyse des liens, inclus dans les messages envoyés par messagerie instantanée, pour savoir s'ils appartiennent à la liste des adresses suspectes et/ou à la liste des adresses de phishing.

Pour augmenter l'efficacité de la protection, vous pouvez utiliser *l'analyse heuristique* (analyse de l'activité de l'objet dans le système). Cette analyse permet d'identifier de nouveaux objets malveillants dont les définitions n'ont pas encore été ajoutées aux bases. Lors de l'analyse heuristique, n'importe quel script contenu dans les messages de client de messagerie instantanée est exécuté dans l'environnement protégé. Si l'activité du script est caractéristique des objets malveillants, alors l'objet peut être considéré, avec une probabilité élevée, comme un objet malveillant ou suspect. L'analyse heuristique est activée par défaut.

- *Pour analyser les liens des messages selon la base des adresses suspectes, procédez comme suit :*

  1. Ouvrez la fenêtre de configuration de l'application.
  2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Antivirus IM ("Chat")**.
  3. Cochez la case **Analyser les liens selon la base des URL suspectes** dans le groupe **Méthodes d'analyse** de la partie droite de la fenêtre.

- *Pour analyser les liens des messages selon la base des adresses de phishing, procédez comme suit :*

  1. Ouvrez la fenêtre de configuration de l'application.
  2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Antivirus IM ("Chat")**.
  3. Cochez la case **Analyser les liens selon la base des URL de phishing** dans le groupe **Méthodes d'analyse** de la partie droite de la fenêtre.

- *Pour activer l'utilisation de l'analyse heuristique, procédez comme suit :*

  1. Ouvrez la fenêtre de configuration de l'application.
  2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Antivirus IM ("Chat")**.
  3. Cochez la case **Analyse heuristique** dans le groupe **Méthodes d'analyse** de la partie droite de la fenêtre.

# DEFENSE PROACTIVE

La Défens Proactive protège l'ordinateur contre les nouvelles menaces dont les informations ne figurent pas encore dans les bases de Kaspersky Internet Security.

Les technologies préventives sur lesquelles repose la Défense Proactive évitent les pertes de temps et permettent de neutraliser la nouvelle menace avant qu'elle n'ait pu nuire à votre ordinateur. À la différence des technologies réactives qui réalisent l'analyse selon les enregistrements des bases de Kaspersky Internet Security, les technologies préventives identifient les nouvelles menaces en suivant les séquences d'actions exécutées par une application quelconque. Si l'analyse de la séquence d'actions de l'application éveille des soupçons, Kaspersky Internet Security bloque l'activité de cette application.

Ainsi, si un programme se copie dans une ressource de réseau, dans le répertoire de démarrage et dans la base de registres, on peut affirmer sans crainte qu'il s'agit d'un ver. Parmi les séquences d'actions dangereuses, nous pouvons citer également les tentatives de modification du fichier HOSTS, la dissimulation de l'installation de pilotes, etc. Vous pouvez néanmoins refuser de contrôler (cf. page 111) une activité dangereuse (cf. page 111) ou l'autre.

À la différence du composant Contrôle des Applications, la Défense Proactive réagit précisément à la séquence d'actions de l'application. L'analyse de l'activité porte sur toutes les applications, y compris celles placées dans le groupe **De confiance** par le composant Contrôle des Applications.

Vous pouvez créer un groupe d'applications (cf. page 111) de confiance pour la Défense Proactive. Les notifications sur l'activité de ces applications ne seront pas affichées.

Si l'ordinateur tourne sous Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista, Microsoft Windows Vista x64, Microsoft Windows 7 ou Microsoft Windows 7 x64, certains événements ne seront pas contrôlés. Ceci est lié aux particularités des systèmes d'exploitation cités. Ainsi, l'envoi des données par les applications de confiance et l'activité suspecte dans le système ne seront pas contrôlés en entier.

### DANS CETTE SECTION



# ACTIVATION ET DESACTIVATION DE LA DEFENSE PROACTIVE

La Défense Proactive est activée par défaut et fonctionne selon le mode optimal. Le cas échéant, vous pouvez désactiver la Défense Proactive.

*Pour désactiver la Défense Proactive, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Défense Proactive**.
3. Dans la partie droite de la fenêtre, désélectionnez la case **Activer la Défense Proactive**.

## CONSTITUTION D'UN GROUPE D'APPLICATIONS DE CONFIANCE

Les applications auxquelles Contrôle des Applications a attribué l'état **De confiance** ne présentent aucun danger pour le système. Toutefois, l'activité de ces applications est contrôlée également par la Défense Proactive. Vous pouvez composer des groupes d'applications de confiance dont l'activité sera ignorée par la Défense Proactive. Les applications dotées d'une signature numérique et les applications figurant dans la base de Kaspersky Security Network sont reprises par défaut dans la catégorie des applications de confiance.

*Pour modifier les paramètres de composition d'un groupe d'applications de confiance, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Défense Proactive**.
3. Dans le groupe **Applications de confiance** de la partie droite de la fenêtre cochez la case ☑ en regard des paramètres requis.

## UTILISATION DE LA LISTE DES ACTIVITES DANGEREUSES

La liste des actions en rapport avec les activités dangereuses ne peut être modifiée. Vous pouvez néanmoins refuser de contrôler une activité dangereuse ou l'autre.

*Pour refuser de contrôler une activité dangereuse, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Défense Proactive**.
3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre **Défense Proactive** qui s'ouvre, décochez la case ☑ située en regard du nom de l'activité dont vous refusez le contrôle.

## MODIFICATION D'UNE REGLE DE CONTROLE DE L'ACTIVITE DANGEREUSE

Il est impossible de modifier l'action des applications dont l'activité est jugée dangereuse. Vous pouvez exécuter les opérations suivantes :

- refuser de contrôler une activité quelconque (cf. page 111) ;
- composer une liste d'exclusions (cf. page 172), reprenant les applications que vous n'estimez pas dangereuses ;
- Modifier la règle qui définit le fonctionnement de la Défense Proactive lors de la découverte d'activités dangereuses ;

*Afin de modifier les règles de la Défense Proactive, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Défense Proactive**.
3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre **Défense Proactive** qui s'ouvre, dans la colonne **Evènement**, sélectionnez l'événement pour lequel la règle doit être modifiée.

5. Pour l'événement sélectionné, configurez les paramètres nécessaires de la règle à l'aide des liens dans le bloc de **Description de la règle**. Par exemple :

   a. Cliquez sur le lien indiquant l'action établie et dans la fenêtre **Sélectionner une action** ouverte, sélectionnez l'action nécessaire parmi les actions proposées ;

   b. Cliquez sur le lien **Act./Désact.**, pour indiquer la nécessité de créer un rapport sur l'opération exécutée.

# SURVEILLANCE DU SYSTEME

La Surveillance du système récolte des données sur l'activité des applications sur l'ordinateur et offre ces informations aux autres composants afin qu'ils puissent offrir une protection plus efficace.

Si la conservation de l'historique de l'activité des applications a été activée, La Surveillance du système permet de revenir à l'état antérieur aux actions réalisées par les programmes malveillants (cf. page 113). Le retour à l'état antérieur aux actions en cas de découverte d'une activité malveillante (cf. rubrique "Utilisation des modèles de comportement dangereux (BSS)" à la page 113) dans le système peut être lancé par le composant de Surveillance du système sur la base de modèles de comportement dangereux, par la Défense Proactive ainsi que pendant l'exécution de la tâche d'analyse ou pendant le fonctionnement de l'Antivirus Fichiers (cf. page 88).

La réaction du composant face à des actions d'application qui correspondent aux modèles de comportement dangereux et la remise à l'état antérieur aux actions du programme malveillant dépendent du mode de fonctionnement de Kaspersky Internet Security.

Lorsque les composants de la protection de Kaspersky Internet Security découvrent des événements suspects dans le système, ils peuvent demander des informations complémentaires à la Surveillance de l'activité. En cas d'utilisation de Kaspersky Internet Security en mode interactif, vous pouvez consulter les données sur l'incident récoltées par la Surveillance du système sous la forme d'un rapport sur l'historique de l'activité dangereuse afin de pouvoir prendre une décision lors de la sélection de l'action dans la fenêtre de la notification. Ainsi, lors de la détection du programme potentiellement malveillant par le composant, un lien vers le rapport de la Surveillance de l'activité apparaît dans la partie supérieure de la fenêtre des notifications (cf. page 209) et propose une action.

### DANS CETTE SECTION



# ACTIVATION/DESACTIVATION DE LA SURVEILLANCE DE L'ACTIVITE

La Surveillance du système est activée par défaut et fonctionne selon le mode de fonctionnement de Kaspersky Internet Security : automatique ou interactif.

Il est déconseillé de désactiver le composant sans raison car cela réduirait l'efficacité du fonctionnement de la Défense Proactive et du Contrôle des Applications, ainsi que d'autres composants de la protection qui peuvent demander les données récoltées par la Surveillance de l'activité pour préciser la menace potentielle détectée.

*Pour désactiver l'utilisation de la Surveillance de l'activité, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.

2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Surveillance du système**.

3. Dans la partie droite de la fenêtre, désélectionnez la case **Activer la Surveillance du système**.

## UTILISATION DES MODELES DE COMPORTEMENT DANGEREUX (BSS)

Les modèles de comportement dangereux (BSS, Behavior Stream Signatures) contiennent la séquence d'actions d'applications considérées comme dangereuses. Lorsque l'activité d'une application correspond à un des modèles de comportement dangereux, Kaspersky Internet Security exécute l'action définie.

Les modèles de comportement utilisés par la Surveillance du système sont enrichis lors de la mise à jour de Kaspersky Internet Security afin de garantir une protection à jour et efficace.

Par défaut, en cas d'utilisation de Kaspersky Internet Security en mode automatique, si l'activité de l'application correspond à un modèle de comportement dangereux, la Surveillance du système place cette application en quarantaine et en mode interactif (cf. page 74), elle demande à l'utilisateur de confirmer l'action. Vous pouvez indiquer l'action à exécuter quand l'activité d'une application correspond à un modèle de comportement dangereux.

Outre les équivalences exactes entre l'activité d'une application et les modèles de comportement dangereux, la Surveillance de l'activité découvre les actions qui correspondent en partie aux modèles de comportement dangereux et qui sont suspectes, suite à l'analyse heuristique. En cas de découverte d'une activité suspecte, la Surveillance du système demande à l'utilisateur de confirmer l'action, quel que soit le mode de fonctionnement.

- *Pour sélectionner l'action à exécuter en cas de correspondance entre l'activité d'une application et un modèle de comportement dangereux, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Surveillance du système**.
3. Dans la partie droite de la fenêtre, dans le groupe **Analyse heuristique**, cochez la case **Utiliser les modèles de comportement dangereux (BSS) actualisés**.
4. Sélectionnez l'option **Exécuter l'action**, puis choisissez l'action requise dans la liste déroulante.

## RETOUR A L'ETAT ANTERIEUR AUX ACTIONS DU PROGRAMME MALVEILLANT

Vous pouvez utiliser la fonction du rétablissement du système à l'état antérieur aux actions du programme malveillant. Pour pouvoir revenir à l'état antérieur, la Surveillance du système doit conserver l'historique de l'activité des applications.

Par défaut, lorsque Kaspersky Internet Security fonctionne en mode automatique, le retour à l'état antérieur s'opère automatiquement lorsque les composants de la protection découvrent une activité malveillante. En mode interactif (cf. page 74), la Surveillance du système demande à l'utilisateur de confirmer l'action. Vous pouvez désigner l'action à exécuter en cas de découverte d'une activité malveillante.

Le retour à l'état antérieur aux actions du programme malveillant touche un ensemble de données clairement délimité. Cette procédure n'a aucun impact négatif sur le fonctionnement du système d'exploitation, ni sur l'intégrité des informations enregistrées sur l'ordinateur.

- *Pour configurer le retour à l'état antérieur aux actions du programme malveillant, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Surveillance du système**.
3. Dans le groupe **Historique de l'activité des applications** de la partie droite de la fenêtre, cochez la case **Conserver l'historique de l'activité**.

4. Sélectionnez l'option **Exécuter l'action**, puis choisissez l'action requise dans la liste déroulante.

# CONTROLE DES APPLICATIONS

Le Contrôle des Applications empêche l'exécution d'actions dangereuses pour le système par les applications et garantit le contrôle de l'accès à vos données personnelles.

Le composant enregistre les actions exécutées par les applications dans le système et régit l'activité des applications en fonction du groupe de confiance auquel elles appartiennent.

Chaque application exécutée reçoit un état qui définit le groupe de confiance. Chaque état est associé à un ensemble défini de règles. Les règles du Contrôle des Applications régissent les activités potentiellement dangereuses comme l'accès des applications aux ressources protégées (fichiers et répertoires, clés de registre, adresses de réseau, etc.) en fonction du classement de danger des applications.

Lors de la tentative d'exécution d'une action soumise à des restrictions, le Contrôle des Applications vérifie si l'application possède les autorisations requises et exécute l'action définie par la règle pour l'état de cette application.

Afin de contrôler l'accès des applications à différentes ressources de l'ordinateur, vous pouvez utiliser la liste prédéfinie de ressources protégées ou composer vous-même la zone de protection (cf. page 115).

À la première exécution de l'application, le Contrôle des Applications vérifie la sécurité et lui attribue un état particulier.

Tout d'abord, le composant recherche une entrée sur l'application dans la base de données interne des applications connues de Kaspersky Internet Security, puis envoie une requête à la base Kaspersky Security Network (cf. rubrique "Participation au Kaspersky Security Network" à la page 193) (si une connexion à Internet existe et si le chargement des règles depuis Kaspersky Security Network (cf. page 117)) est activé. Si l'enregistrement figure dans la base, l'application reçoit l'état enregistré dans la base, et les règles chargées depuis Kaspersky Security Network sont appliquées pour cette application.

Par défaut, si l'application ou l'objet parent possède une signature numérique confirmée, alors l'application attribue automatiquement l'état de confiance. Vous pouvez modifier la condition de composition d'un groupe d'applications de confiance (cf. page 117).

Le comportement des applications jugées de confiance par le Contrôle des Applications sera malgré tout analysé par la Défense proactive (cf. page 110).

Les applications inconnues (qui ne figurent pas dans la base de Kaspersky Internet Security et qui ne possèdent pas de signature numérique) sont soumises par défaut à l'analyse heuristique qui permet de définir le niveau de danger de l'application. Les applications dont le niveau de danger est faible obtiennent l'état **Restrictions faibles**.

Si le classement de l'application est élevé, Kaspersky Internet Security vous avertit et vous propose l'état à attribuer à une application potentiellement indésirable. La notification reprend des informations sur les statistiques d'utilisation de cette application par les participants au Kaspersky Security Network. Sur la base de ces informations et en connaissant l'historique de l'apparition de l'application sur l'ordinateur, vous pouvez prendre une décision plus objective (cf. page 122) sur l'état à attribuer à l'application.

Pour contribuer au fonctionnement plus efficace du Contrôle des Applications, il est conseillé de participer au Kaspersky Security Network.

Au deuxième lancement de l'application, le Contrôle des Applications vérifie son intégrité. Si l'application n'a pas été modifiée, le composant applique la règle existante. En cas de modification de l'application, le Contrôle des Applications l'analysera à nouveau, comme à l'occasion de la première exécution.

Vous pouvez modifier les conditions de définition de l'état des applications (cf. page 117), l'état d'une application en particulier (cf. rubrique "Modification et restauration de l'état de l'application sélectionnée" à la page 118), ainsi que modifier les règles pour les états ou pour des applications distinctes (cf. page 119).

**DANS CETTE SECTION**



# ACTIVATION ET DESACTIVATION DU CONTROLE DES APPLICATIONS

Le Contrôle des Applications est activé par défaut et fonctionne selon le mode défini par les experts de Kaspersky Lab, mais vous pouvez le désactiver si nécessaire.

*Pour désactiver le Contrôle des Applications, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Contrôle des Applications**.
3. Dans la partie droite de la fenêtre, désélectionnez la case ☑ **Activer le Contrôle des Applications**.

# CONSTITUTION DE LA ZONE DE PROTECTION

Le Contrôle des Applications gère les privilèges des applications au niveau des actions à exécuter sur différentes catégories de ressources du système d'exploitation et des données personnelles. La zone de protection désigne les ressources, dont l'accès est régi par les règles du Contrôle des Applications.

Les experts de Kaspersky Lab ont sélectionné des catégories de ressources à protéger. Il n'est pas permis de modifier cette liste. Vous pouvez toutefois désactiver le contrôle d'une catégorie de ressource ou d'une autre ou enrichir la liste.

Outre les catégories de données personnelles prédéfinies, il est possible d'ajouter des catégories de ressources protégées définies par l'utilisateur. De plus, vous pouvez ajouter des ressources définies aux exclusions et l'accès à celles-ci ne sera pas contrôlé.

*Pour ajouter des données personnelles à protéger, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.

2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Contrôle des Applications**.

3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Ressources**.

4. Dans la fenêtre qui s'ouvre, sous l'onglet **Données personnelles**, sélectionnez la catégorie de données personnelles requise dans la liste déroulante **Catégorie** et ouvrez la fenêtre d'ajout des ressources en cliquant sur le lien **Ajouter**.

5. Dans la fenêtre **Ressource définie par l'utilisateur** qui s'ouvre, cliquez le bouton **Parcourir** et définissez les paramètres requis en fonction de la ressource ajoutée.

Une fois que la ressource a été ajoutée à la zone de protection, vous pouvez la modifier ou la supprimer à l'aide des liens du même nom dans la partie inférieure de l'onglet. Si vous souhaitez exclure une ressource de la zone de protection décochez la case ☑ en regard.

*Pour créer une catégorie de données personnelles à protéger, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.

2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Contrôle des Applications**.

3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Ressources**.

4. Dans la fenêtre qui s'ouvre, sous l'onglet **Données personnelles**, ouvrez la fenêtre d'ajout de catégories de ressource en cliquant sur le lien **Ajouter une catégorie**.

5. Dans la fenêtre **Catégorie des ressources d'utilisateur** qui s'ouvre, saisissez le nom de la nouvelle catégorie de ressource.

*Pour ajouter des paramètres et des ressources du système d'exploitation à protéger, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.

2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Contrôle des Applications**.

3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Ressources**.

4. Dans la fenêtre qui s'ouvre, sous l'onglet **Système d'exploitation**, sélectionnez la catégorie d'objet du système d'exploitation requise dans la liste déroulante **Catégorie** et ouvrez la fenêtre d'ajout des ressources en cliquant sur le lien **Ajouter**.

5. Dans la fenêtre **Ressource définie par l'utilisateur** qui s'ouvre, cliquez le bouton **Parcourir** et définissez les paramètres requis en fonction de la ressource ajoutée.

Une fois que la ressource a été ajoutée à la zone de protection, vous pouvez la modifier ou la supprimer à l'aide des liens du même nom dans la partie inférieure de l'onglet. Si vous souhaitez exclure une ressource de la zone de protection décochez la case ☑ en regard.

*Pour ajouter une ressource aux exclusions, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.

2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Contrôle des Applications**.

3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Ressources**.

4. Dans la fenêtre qui s'ouvre, sous l'onglet **Exclusions**, cliquez sur le lien **Ajouter** et dans le menu qui s'ouvre, sélectionnez le type de ressource requis.

5. Dans la fenêtre **Ressource définie par l'utilisateur**, définissez les paramètres indispensables en fonction de la ressource ajoutée.

## CONFIGURATION DE LA DEFINITION AUTOMATIQUE DES ETATS DES APPLICATIONS

La première étape de la définition de l'état de l'application est, par défaut, la recherche d'informations dans la base de Kaspersky Security Network. Les statistiques de Kaspersky Security Network permettent de définir avec un degré de précision élevé l'état des applications à la première exécution et d'appliquer les règles les mieux adaptées au contrôle de ces applications. Si l'application ne figurait pas dans la base de Kaspersky Security Network au moment de la première exécution, mais que les données à son sujet ont été ajoutées par la suite, les règles de contrôle de cette application seront automatiquement actualisées. Vous pouvez désactiver le téléchargement de règles depuis Kaspersky Security Network ou actualiser automatiquement les règles pour les applications jusque là inconnues.

L'état **De confiance** est attribué aux applications qui ne présentent pas de danger pour le système. Cet état est attribué par défaut aux applications qui possèdent une signature numérique et si la signature numérique est présente chez l'objet parent. Vous pouvez désactiver l'attribution automatique de l'état **De confiance** à ces applications.

L'analyse heuristique est utilisée par défaut pour définir l'état des applications inconnues à la première exécution. Le degré de danger de l'application sur la base duquel un état particulier sera attribué est défini. Vous pouvez désigner un état défini qui sera automatiquement attribué aux applications inconnues.

Pendant l'analyse heuristique, le Contrôle des Applications analyse l'application pendant 30 secondes. Si le niveau de danger n'est pas défini à l'issue de cette période, l'application reçoit l'état **Restrictions faibles**. La définition du niveau se poursuit en arrière-plan et l'application reçoit alors sont état définitif.

Vous pouvez modifier la durée consacrée à l'analyse des applications exécutées. Si vous êtes convaincu que toutes les applications exécutées sur votre ordinateur ne menacent pas la sécurité, vous pouvez réduire la durée de l'analyse. Si, au contraire, vous installez une application dont vous ne pouvez garantir la fiabilité en matière de sécurité, il est conseillé d'augmenter la durée de l'analyse.

- *Pour désactiver l'attribution automatique de l'état **De confiance** aux applications dotées d'une signature numérique, procédez comme suit :*

  1. Ouvrez la fenêtre de configuration de l'application.
  2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Contrôle des Applications**.
  3. Dans le groupe **Règles de traitement des applications** de la partie droite de la fenêtre, décochez la case **Faire confiance aux applications dotées de la signature numérique**.

- *Pour désactiver le téléchargement de règles depuis Kaspersky Security Network, procédez comme suit :*

  1. Ouvrez la fenêtre de configuration de l'application.
  2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Contrôle des Applications**.
  3. Pour le composant sélectionné, dans le groupe **Règles de traitement des applications** de la partie droite de la fenêtre, décochez la case **Charger les règles pour l'application depuis Kaspersky Security Network (KSN)**.

- *Pour désactiver la mise à jour des règles de Kaspersky Security Network pour les applications jusque là inconnues, procédez comme suit :*

  1. Ouvrez la fenêtre de configuration de l'application.
  2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Contrôle des Applications**.

3. Dans le groupe **Règles de traitement des applications** de la partie droite de la fenêtre, décochez la case **Actualiser les règles pour les applications inconnues jusqu'ici depuis KSN**.

*Pour utiliser l'analyseur heuristique dans la définition de l'état des autres applications, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Contrôle des Applications**.
3. Dans le groupe **Règles de traitement des applications** de la partie droite de la fenêtre, sélectionnez l'option **Déterminer l'état à l'aide de l'analyse heuristique**.

*Pour attribuer aux applications inconnues l'état défini, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Contrôle des Applications**.
3. Dans le groupe **Règles de traitement des applications** de la partie droite de la fenêtre, sélectionnez l'option **Attribuer automatiquement l'état** et choisissez l'état requis dans la liste déroulante.

*Pour modifier la durée accordée à la définition de l'état, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Contrôle des Applications**.
3. Dans le groupe **Règles de traitement des applications** de la partie droite de la fenêtre, modifiez la valeur du paramètre **Durée maximale pour déterminer l'état de l'application**.

## MODIFICATION ET RESTAURATION DE L'ETAT DE L'APPLICATION SELECTIONNEE

Au premier lancement de l'application, le Contrôle des Applications lui attribue un état automatiquement. Si vous êtes convaincu que l'état attribué est erroné, vous pouvez le changer manuellement. Vous pouvez revenir à n'importe quel moment à l'état défini automatiquement.

Les experts de Kaspersky Lab déconseillent de modifier les états des applications attribués automatiquement. Au lieu de cela, modifiez si nécessaire les règles pour l'application en question (cf. rubrique "Modification des règles pour l'application sélectionnée" à la page 119).

*Pour modifier l'état de l'application, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et sélectionnez la rubrique **Protection**.
2. Dans la partie droite de la fenêtre, cliquez sur le bouton gauche de la souris et ouvrez la liste des composants **Protection du système et des applications**.
3. Cliquez sur le lien **Surveillance des Applications**.
4. Dans la fenêtre **Surveillance des Applications** qui s'ouvre, sélectionnez la catégorie requise dans la liste **Catégorie**.
5. Pour l'application requise, dans la colonne **Etat**, cliquez sur le bouton gauche de la souris afin d'ouvrir le menu contextuel et sélectionnez l'état requis.

*Pour revenir à l'état attribué automatiquement, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et sélectionnez la rubrique **Protection**.
2. Dans la partie droite de la fenêtre, cliquez sur le bouton gauche de la souris et ouvrez la liste des composants **Protection du système et des applications**.
3. Cliquez sur le lien **Surveillance des Applications**.
4. Dans la fenêtre **Surveillance des Applications** qui s'ouvre, sélectionnez la catégorie requise dans la liste **Catégorie**.
5. Pour l'application requise, dans la colonne **Etat**, cliquez sur le bouton gauche de la souris afin d'ouvrir le menu contextuel et sélectionnez le point **Rétablir l'état par défaut**.

## MODIFICATION DES REGLES POUR L'ETAT DE L'APPLICATION

Les règles d'état de l'application déterminent les règles d'accès aux ressources protégées auxquelles seront soumises les applications d'un état particulier. Vous pouvez modifier les règles proposées pour les états des applications.

*Pour modifier la règle pour l'état, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Contrôle des Applications**.
3. Dans la partie droite de la fenêtre, dans le groupe **Configuration des privilèges des applications et des ressources protégées**, cliquez sur le bouton **Applications**.
4. Dans la fenêtre **Applications** qui s'ouvre, sélectionnez l'état requis dans la liste.
5. Cliquez sur le bouton **Modifier**.
6. Dans la fenêtre **Règles pour les états des applications** qui s'ouvre, choisissez l'onglet correspondant à la catégorie de ressources requise (**Fichiers et base de registres**, **Privilèges**).
7. Pour la ressource requise, cliquez sur le bouton droit de la souris dans la colonne de l'action correspondante afin d'ouvrir le menu contextuel et sélectionnez les paramètres requis.

## MODIFICATION DES REGLES POUR L'APPLICATION SELECTIONNEE

Par défaut, l'application hérite des règles de l'état qui lui est attribué. Vous pouvez modifier les règles pour une application en particulier. Dans ce cas, l'application reçoit l'état **Paramètres de l'utilisateur**. Le cas échéant, vous pouvez restaurer l'état (cf. rubrique "Modification et restauration de l'état de l'application sélectionnée" à la page 118) par défaut de l'application.

De plus, vous pouvez désactiver l'héritage des règles de l'état pour une catégorie distincte de ressources à protéger. L'accès de l'application à ces ressources sera soumis aux règles pour l'application.

*Pour modifier une règle pour l'application, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et choisissez la section **Protection**.
2. Dans la partie droite de la fenêtre, cliquez sur le bouton gauche de la souris et ouvrez la liste des composants **Protection du système et des applications**.
3. Cliquez sur le lien **Surveillance des Applications**.

4. Dans la fenêtre **Surveillance des Applications** qui s'ouvre, sélectionnez la catégorie requise dans la liste **Catégorie**.

5. Pour l'application requise, dans la colonne **Etat**, cliquez sur le bouton gauche de la souris afin d'ouvrir le menu contextuel et sélectionnez l'option **Règles pour l'application**.

6. Dans la fenêtre **Règles pour l'application** qui s'ouvre, choisissez l'onglet correspondant à la catégorie de ressources requise (**Fichiers et base de registres**, **Privilèges**, **Règles de réseau**).

7. Pour la ressource requise, cliquez sur le bouton droit de la souris dans la colonne de l'action correspondante afin d'ouvrir le menu contextuel et sélectionnez les paramètres requis.

*Pour désactiver l'héritage des règles de l'état, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et choisissez la rubrique **Protection**.

2. Dans la partie droite de la fenêtre, cliquez sur le bouton gauche de la souris et ouvrez la liste des composants **Protection du système et des applications**.

3. Cliquez sur le lien **Surveillance des Applications**.

4. Dans la fenêtre **Surveillance des Applications** qui s'ouvre, sélectionnez la catégorie requise dans la liste **Catégorie**.

5. Pour l'application requise, dans la colonne **Etat**, cliquez sur le bouton gauche de la souris afin d'ouvrir le menu contextuel et sélectionnez l'option **Règles pour l'application**.

6. Dans la fenêtre **Règles pour l'application** qui s'ouvre, choisissez l'onglet correspondant à la catégorie de ressources requise (**Fichiers et base de registres** ou **Privilèges**).

7. Pour la ressource requise, cliquez sur le bouton droit de la souris dans la colonne de l'action requise, ouvrez le menu contextuel, puis choisissez l'option **Hériter** avec la coche.

## CREATION D'UNE REGLE DE RESEAU POUR UNE APPLICATION

Les règles de réseau réglementent l'accès des applications à divers réseaux. Par défaut, l'application hérite des règles de l'état qui lui est attribué. Si vous devez organiser d'une manière spéciale l'accès d'une application à un service de réseau en particulier, vous pouvez créer une règle qui régit l'activité de réseau de cette application.

Vous pouvez également utiliser les règles de réseau pour les applications à l'aide du composant Pare-feu (cf. page 123).

*Pour créer une règle de réseau, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et choisissez la rubrique **Protection**.

2. Dans la partie droite de la fenêtre, cliquez sur le bouton gauche de la souris et ouvrez la liste des composants **Protection du système et des applications**.

3. Cliquez sur le lien **Surveillance des Applications**.

4. Dans la fenêtre **Surveillance des Applications** qui s'ouvre, sélectionnez la catégorie requise dans la liste **Catégorie**.

5. Pour l'application requise, dans la colonne **Etat**, cliquez sur le bouton gauche de la souris afin d'ouvrir le menu contextuel et sélectionnez l'option **Règles pour l'application**.

6. Dans la fenêtre qui s'ouvre, sous l'onglet **Règles de réseau**, ouvrez la fenêtre de création d'une règle de réseau en cliquant sur le lien **Ajouter**.

7. Dans la fenêtre **Règle de réseau** qui s'ouvre, définissez les paramètres requis.

8. Définissez la priorité de la nouvelle règle à l'aide des liens **Haut** et **Bas**.

## EXCLUSION DES ACTIONS DE LA REGLE POUR L'APPLICATION

Lors de l'application de règles pour l'application, Kaspersky Internet Security contrôle par défaut toute action de l'application : l'accès aux fichiers et aux répertoires, l'accès au milieu d'exécution et l'accès au réseau. Vous pouvez ajouter des actions définies des applications aux exclusions de la règle.

Toutes les exclusions créées dans les règles pour les applications sont accessibles dans la fenêtre de configuration (cf. rubrique "Fenêtre de configuration des paramètres de l'application" à la page 46) des paramètres de l'application, dans le groupe **Menaces et exclusions**.

*Pour ajouter des exclusions à la règle, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et sélectionnez la rubrique **Protection**.
2. Dans la partie droite de la fenêtre, cliquez sur le bouton gauche de la souris et ouvrez la liste des composants **Protection du système et des applications**.
3. Cliquez sur le lien **Surveillance des Applications**.
4. Dans la fenêtre **Surveillance des Applications** qui s'ouvre, sélectionnez la catégorie requise dans la liste **Catégorie**.
5. Pour l'application requise, dans la colonne **Etat**, cliquez sur le bouton gauche de la souris afin d'ouvrir le menu contextuel et sélectionnez l'option **Règles pour l'application**.
6. Dans la fenêtre qui s'ouvre, sous l'onglet **Exclusions**, cochez la case en regard des actions à exclure. En cas d'exclusion de l'analyse du trafic de réseau de l'application, configurez les paramètres avancés d'exclusion.

## HERITAGE DES RESTRICTIONS DU PROCESSUS PARENT

L'utilisateur ou une autre application en cours d'exécution peut être à l'origine du lancement d'une application. Si l'application a été lancée par une autre, alors la séquence de lancement est composée des applications mère et fille.

Lorsque l'application tente d'accéder à la ressource contrôlée, le Contrôle des Applications analyse les privilèges de tous les processus parent de cette application afin de voir s'ils peuvent accéder à la ressource. Dans ce cas, c'est la règle de la priorité minimale qui est appliquée : lorsque les privilèges d'accès de l'application et du processus parent sont comparés, les privilèges d'accès avec la priorité minimale seront appliqués à l'activité de l'application.

Priorité des privilèges d'accès :

1. Autoriser. Ces privilèges d'accès ont une priorité élevée.
2. Confirmer l'action.
3. Interdire. Ces privilèges d'accès ont une priorité faible.

Ce mécanisme empêche l'utilisation d'applications de confiance par des applications douteuses ou dont les privilèges sont réduits pour exécuter des actions avec des privilèges.

Si l'activité de l'application est bloquée à cause du manque des droits chez un des processus parental, vous pouvez changer ces règles (cf. section "Modification des règles pour l'application sélectionnée" à la page 119).

Modifiez les privilèges du processus parent et désactivez l'héritage des restrictions uniquement si vous êtes absolument certain que l'activité du processus ne menace pas la sécurité du système !

*Pour désactiver l'héritage des restrictions du processus parent, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et choisissez la rubrique **Protection**.
2. Dans la partie droite de la fenêtre, cliquez sur le bouton gauche de la souris et ouvrez la liste des composants **Protection du système et des applications**.
3. Cliquez sur le lien **Surveillance des Applications**.
4. Dans la fenêtre **Surveillance des Applications** qui s'ouvre, sélectionnez la catégorie requise dans la liste **Catégorie**.
5. Pour l'application requise, dans la colonne **Etat**, cliquez sur le bouton gauche de la souris afin d'ouvrir le menu contextuel et sélectionnez l'option **Règles pour l'application**.
6. Dans la fenêtre **Règles pour l'application** qui s'ouvre, sélectionnez l'onglet **Exclusions**, puis cochez la case **Restriction non héritée du processus parent (application)**.

## SUPPRESSION DE REGLES POUR LES APPLICATIONS NON UTILISEES

Les règles pour les applications qui n'ont pas été utilisées depuis 60 jours sont supprimées automatiquement par défaut. Vous pouvez modifier la durée de conservation des règles pour les applications non utilisées et désactiver la suppression automatique.

*Pour configurer la suppression automatique des règles pour les applications non utilisées, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Contrôle des Applications**.
3. Dans le groupe **Avancé** de la partie droite de la fenêtre, cochez la case **Supprimer les règles d'applications qui n'ont plus été lancées depuis** et définissez le nombre de jours requis.

## INTERPRETATION DES DONNEES SUR L'UTILISATION DE L'APPLICATION PAR LES PARTICIPANTS AU KSN

Les informations sur l'utilisation de l'application par les participants de Kaspersky Security Network (cf. page 193) aideront à prendre une décision objective sur l'état à attribuer à l'application potentiellement dangereuse lancée sur votre ordinateur. Il est possible d'évaluer plus précisément la protection de l'application sur la base des données depuis KSN, si l'histoire d'apparition de cette application sur votre ordinateur est connue.

Les experts de Kaspersky Lab ont élaboré des sources suivantes possibles d'apparition d'une nouvelle application sur l'ordinateur :

- le téléchargement depuis Internet et le lancement ultérieur du fichier d'installation par l'utilisateur ;
- le téléchargement automatique et le lancement du fichier d'installation lors du passage de l'utilisateur à la page web ;
- le lancement par l'utilisateur du fichier d'installation situé sur le CD/DVD ou copié de là sur le disque dur ;
- le lancement par l'utilisateur du fichier d'installation situé sur l'ensemble de mémoire USB ou copié de là sur le disque dur ;
- le lancement par l'utilisateur du fichier d'installation reçu dans un message par courrier électronique, messagerie instantanée ou réseau social.

Les statistiques d'utilisation de l'application par les participants de Kaspersky Security Network incluent la fréquence et la prescription d'utilisation de cette application. Les options suivantes des statistiques d'utilisation de l'application sont les options principales :

- **très rare** (moins de 100 participants à KSN utilisent cette application) et **récent** (le fichier a apparu quelques jours avant) ;
- **rare** (moins de 1000 participants à KSN) et relativement **longtemps** (quelques mois avant), la plupart des utilisateurs limitent l'activité de cette application ;
- **souvent** (plus de 100000 participants à KSN) et **longtemps** (plus de six mois avant), la plupart des utilisateurs font confiance à cette application ;
- **souvent** (plus de 100000 participants à KSN) et **récent** (quelques semaines avant), la plupart des utilisateurs font confiance ou limitent cette application ;
- **très souvent** (plus de 100000 participants à KSN) et **récent**, la plupart des utilisateurs font confiance à cette application.

# PROTECTION DU RESEAU

Les différents composants de la protection, les outils et les paramètres de Kaspersky Internet Security garantissent la protection et le contrôle de votre utilisation du réseau.

Les rubriques suivantes contiennent des informations détaillées sur les principes de fonctionnement et la configuration du Pare-feu, de la Prévention des intrusions, l'analyse des connexions cryptées, la surveillance de l'activité de réseau, les paramètres du serveur proxy et le contrôle des ports de réseau.

### DANS CETTE SECTION



# PARE-FEU

Le Pare-feu vous protège pendant l'utilisation des réseaux locaux et d'Internet.

Le composant filtre toute l'activité de réseau conformément aux règles définies. La règle de Pare-feu est une action que le Pare-feu exécute lorsqu'il détecte une tentative de connexion avec un état déterminé. L'état est attribué à chaque connexion de réseau et est défini par les paramètres suivants : sens et protocole du transfert de données, adresses et de ports utilisés pour la connexion.

Le Pare-feu analyse les paramètres du réseau auquel vous connectez l'ordinateur. Si l'application fonctionne en mode interactif, le Pare-feu vous informera de l'état du réseau contacté lors de la première connexion. Si le mode interactif est désactivé, le Pare-feu déterminera l'état en fonction du type de réseau, de la plage d'adresses et d'autres caractéristiques. Vous pouvez modifier l'état (cf. page 124) de la connexion de réseau manuellement.

**DANS CETTE SECTION**



## ACTIVATION ET DESACTIVATION DU PARE-FEU

Par défaut, le Pare-feu est activé et fonctionne en mode optimal. Le cas échéant, vous pouvez désactiver le Pare-feu.

*Pour activer le Pare-feu, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Pare-feu**.
3. Dans la partie droite de la fenêtre, désélectionnez la case **Activer le Pare-feu**.

## MODIFICATION DE L'ETAT DU RESEAU

La sélection des règles appliquées au filtrage de l'activité de réseau de la connexion sélectionnée dépend de l'état de la connexion. Le cas échéant, vous pouvez modifier l'état du réseau.

*Pour modifier l'état d'une connexion de réseau, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Pare-feu**.
3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Réseaux**, sélectionnez une connexion de réseau active, puis cliquez sur le lien **Configurer** afin d'ouvrir la fenêtre des paramètres du réseau.
5. Dans la fenêtre qui s'ouvre, sous l'onglet **Propriétés**, sélectionnez l'état requis dans la liste déroulante.

## UTILISATION DES REGLES DU PARE-FEU

Le Pare-feu fonctionne sur la base de règles de deux types :

- *Règles pour les paquets.* Elles sont utilisées pour définir des restrictions pour les paquets quelles que soient les applications. Le plus souvent, ces règles limitent l'activité de réseau entrante sur des ports particuliers des protocoles TCP et UDP et filtrent les messages ICMP.
- *Règles pour les applications*. Elles sont utilisées pour définir des restrictions pour l'activité de réseau d'une application particulière. Ces règles permettent de configurer en détail le filtrage de l'activité lorsque, par exemple, un type déterminé des connexions de réseau est interdit pour certaines applications mais autorisé pour d'autres.

La priorité des règles pour les paquets est plus élevée que la priorité des règles pour les applications. Si des règles pour les paquets et des règles pour les applications sont définies pour la même activité de réseau, celle-ci sera traitée selon les règles pour les paquets. De plus, la priorité d'exécution est définie (cf. page 126) séparément pour chaque règle.

### CREATION D'UNE REGLE POUR UN PAQUET

Les règles pour les paquets sont un ensemble de conditions et d'actions à réaliser sur les paquets lorsque les conditions définies sont vérifiées.

Au moment de créer des règles pour les paquets, n'oubliez pas qu'elles ont priorité sur les règles pour les applications.

*Pour créer une règle pour un paquet, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Pare-feu**.
3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Règles pour les paquets**, cliquez sur le lien **Ajouter** pour ouvrir la fenêtre de création d'une règle de réseau.
5. Dans la fenêtre **Règle de réseau** qui s'ouvre, définissez les paramètres requis.
6. Pour définir la priorité de la nouvelle règle, déplacez-la vers le haut ou vers le bas de la liste à l'aide des liens **Haut** et **Bas**.

Une fois que vous aurez créé une règle, vous pourrez modifier ses paramètres ou la supprimer à l'aide des liens de la partie inférieure de l'onglet. Pour désactiver une règle, décochez la case en regard de son nom.

### CREATION DE REGLES POUR L'APPLICATION

À l'instar du composant Contrôle des Applications (cf. page 114), le Pare-feu utilise par défaut les états des applications pour définir les règles qui seront appliquées au filtrage de l'activité de réseau.

Le cas échéant, vous pouvez créer des règles de réseau (cf. page 120) pour les applications à l'aide du composant Contrôle des Applications.

Vous pouvez modifier les règles de réseau pour les états et créer des règles complémentaires pour un filtrage plus fin de l'activité de réseau.

Les règles définies par l'utilisateur pour des applications en particulier ont une priorité supérieure à celle des règles héritées de l'état.

*Pour créer une règle pour une application, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Pare-feu**.
3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Règles pour les applications**, sélectionnez l'application et cliquez sur le lien **Configurer** afin d'ouvrir la fenêtre de configuration des règles.
5. Dans la fenêtre qui s'ouvre, sous l'onglet **Règles de réseau**, ouvrez la fenêtre de création d'une règle de réseau pour l'application en cliquant sur le lien **Ajouter**.
6. Dans la fenêtre **Règle de réseau** qui s'ouvre, définissez les paramètres requis.

7. Pour définir la priorité de la nouvelle règle, déplacez-la vers le haut ou vers le bas de la liste à l'aide des liens **Haut** et **Bas**.

Une fois que vous aurez créé une règle, vous pourrez modifier ses paramètres ou la supprimer à l'aide des liens de la partie inférieure de l'onglet. Pour désactiver une règle, décochez la case en regard de son nom.

### MODIFICATION DES REGLES POUR L'ETAT DE L'APPLICATION

Les règles de réseau des états des applications déterminent les règles d'accès à diverses ressources auxquelles seront soumises les applications d'un état particulier. Vous pouvez modifier les règles de réseau proposées pour les états des applications.

*Pour modifier une règle de réseau pour un état, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Pare-feu**.
3. Dans la partie droite de la fenêtre, dans le groupe **Règles pour les états des applications**, cliquez sur le bouton **Configuration des règles**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Règles pour les applications**, sélectionnez l'état requis et cliquez sur le bouton droit de la souris dans la colonne **Réseaux** pour ouvrir le menu contextuel et choisir le paramètre requis.

### MODIFICATION DE LA PRIORITE D'UNE REGLE

La priorité d'une règle dépend de sa position dans la liste des règles. La première règle de la liste est celle qui possède la priorité la plus élevée.

Chaque règle de paquet créée manuellement est ajoutée à la fin de la liste.

Les règles pour les applications sont regroupées par nom d'application et la priorité des règles concerne uniquement le groupe déterminé. Les règles créées manuellement pour les applications ont une priorité supérieure à celle des règles de l'état héritées.

*Pour modifier la priorité de la règle pour un paquet, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Pare-feu**.
3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Règles de paquet**, sélectionnez la règle et déplacez-la à l'endroit souhaité dans la liste à l'aide des liens **Haut** ou **Bas**.

*Pour modifier la priorité de la règle pour une application, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Pare-feu**.
3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Règles pour les applications**, sélectionnez l'application et ouvrez la fenêtre de configuration des règles à l'aide du lien **Configurer**.
5. Dans la fenêtre qui s'ouvre, sous l'onglet **Règles de réseau**, sélectionnez la règle et déplacez-la à l'endroit souhaité dans la liste à l'aide des liens **Haut** ou **Bas**.

## CONFIGURATION DES NOTIFICATIONS SUR LES MODIFICATIONS DU RESEAU

Les paramètres des connexions de réseau peuvent changer pendent l'utilisation. Vous pouvez recevoir des notifications sur les modifications des paramètres.

*Pour configurer les notifications sur les modifications des paramètres de connexion de réseau, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Pare-feu**.
3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Réseaux**, sélectionnez une connexion de réseau active et ouvrez la fenêtre de configuration des paramètres de réseau en cliquant sur le lien **Configurer**.
5. Dans la fenêtre qui s'ouvre, sous l'onglet **Avancé**, cochez les cases en regard des événements au sujet desquels vous souhaitez être averti.

## PARAMETRES DE FONCTIONNEMENT AVANCES DU PARE-FEU

Vous pouvez définir des paramètres complémentaires pour le Pare-feu tels que l'autorisation du mode actif pour FTP, le blocage des connexions s'il est impossible de demander une confirmation de l'action (l'interface de l'application n'est pas chargée) ou le fonctionnement jusqu'à l'arrêt complet du système.

Tous les paramètres sont activés par défaut.

*Afin de définir les paramètres de fonctionnement avancés du Pare-feu, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Pare-feu**.
3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Règles pour les paquets**, ouvrez la fenêtre de configuration des paramètres avancés à l'aide du lien **Avancé**.
5. Dans la fenêtre **Avancé** qui s'ouvre, cochez/décochez les cases  en regard des paramètres requis.

# PREVENTION DES INTRUSIONS

La Prévention des intrusions recherche dans le trafic entrant toute trace d'activité caractéristique des attaques de réseau. Dès qu'il décèle une tentative d'attaque contre votre ordinateur, Kaspersky Internet Security bloque toute activité de réseau de l'ordinateur qui vous attaque.

Par défaut, le blocage dure une heure. Vous pouvez modifier les paramètres de blocage (cf. page 129). Un message vous avertit qu'une tentative d'attaque de réseau a été menée et vous fournit des informations relatives à l'ordinateur à l'origine de l'attaque. Les descriptions des attaques de réseau connues à l'heure actuelle (cf. section "Types d'attaques de réseau identifiées" à la page 128) et les moyens de lutter contre celles-ci figurent dans les bases de Kaspersky Internet Security. L'enrichissement de la liste avec les attaques découvertes par la Protection contre les attaques de réseau a lieu lors de la mise à jour (cf. section "Mise à jour" à la page 83) des bases.

**DANS CETTE SECTION**



# TYPES D'ATTAQUES DE RESEAU IDENTIFIEES

Il existe à l'heure actuelle de nombreux types d'attaques de réseau différentes. Ces attaques exploitent des vulnérabilités du système d'exploitation ou d'autres programmes système ou applicatif.

Afin de garantir la protection de l'ordinateur en permanence, il est bon de connaître les menaces qui planent sur lui. Les attaques de réseau connues peuvent être scindées en trois grands groupes :

- *Balayage des ports* : ce type de menace n'est pas une attaque en tant que telle mais elle devance d'habitude l'attaque car il s'agit d'une des principales manières d'obtenir des informations sur le poste distant. Cette méthode consiste à balayer les ports UDP/TCP utilisés par les services de réseau sur l'ordinateur convoité afin de définir leur état (ouvert ou fermé).

  Le balayage des ports permet de comprendre les types d'attaque qui pourraient réussir. De plus, les informations obtenues suite au balayage donnent à l'individu malintentionné une idée du système d'exploitation utilisé sur l'ordinateur distant. Ceci limite encore plus le cercle des attaques potentielles et, par conséquent, le temps consacré à leur organisation et cela permet également d'utiliser des vulnérabilités propres à ce système d'exploitation.

- *Les attaques par déni de service* sont des attaques qui rendent le système pris pour cible instable ou totalement inopérationnel. Parmi les conséquences de ce genre d'attaque, citons l'impossibilité d'utiliser les ressources informatiques ciblées par l'attaque (par exemple, impossible d'accéder à Internet).

  Il existe deux types principaux d'attaques DoS :

  - Envoi vers la victime de paquets spécialement formés et que l'ordinateur n'attend pas. Cela entraîne une surcharge ou un arrêt du système ;

  - Envoi vers la victime d'un nombre élevé de paquets par unité de temps ; l'ordinateur est incapable de les traiter, ce qui épuise les ressources du système.

  Voici des exemples frappants de ce groupe d'attaques :

  - *L'attaque Ping of death* : envoi d'un paquet ICMP dont la taille dépasse la valeur admise de 64 Ko. Cette attaque peut entraîner une panne dans certains systèmes d'exploitation.

  - *L'attaque Land* consiste à envoyer vers le port ouvert de votre ordinateur une requête de connexion avec lui-même. Suite à cette attaque, l'ordinateur entre dans une boucle, ce qui augmente sensiblement la charge du processeur et qui entraîne une panne éventuelle du système d'exploitation.

  - *L'attaque ICMP Flood* consiste à envoyer vers l'ordinateur de l'utilisateur un grand nombre de paquets ICMP. Cette attaque fait que l'ordinateur est obligé de répondre à chaque nouveau paquet, ce qui entraîne une surcharge considérable du processeur.

  - *L'attaque SYN Flood* consiste à envoyer vers votre ordinateur un nombre élevé de requêtes pour l'ouverture d'une connexion. Le système réserve des ressources définies pour chacune de ces connexions. Finalement, l'ordinateur gaspille toutes ses ressources et cesse de réagir aux autres tentatives de connexion.

- *Attaques d'intrusion* qui visent à s'emparer du système. Il s'agit du type d'attaque le plus dangereux car en cas de réussite, le système passe entièrement aux mains de l'individu malintentionné.

Ce type d'attaque est utilisé lorsque l'individu malintentionné doit absolument obtenir des informations confidentielles sur l'ordinateur distant (par exemple, numéro de carte de crédit, mots de passe) ou simplement pour s'introduire dans le système en vue d'utiliser ultérieurement les ressources au profit de l'individu malintentionné (utilisation du système dans un réseau de zombies ou comme base pour de nouvelles attaques).

Ce groupe reprend le plus grand nombre d'attaques. Elles peuvent être réparties en trois sous-groupes en fonction du système d'exploitation utilisés par les victimes : attaques sous Microsoft Windows, attaques sous Unix et un groupe commun pour les services de réseau utilisés dans les deux systèmes d'exploitation.

Les attaques utilisant les services de réseau du système d'exploitation les plus répandues sont :

- *Attaque par débordement de tampon*. Le débordement de tampon survient en cas d'absence de contrôle (ou de contrôle insuffisant) lors de l'utilisation de massifs de données. Il s'agit de l'une des vulnérabilités les plus anciennes et les plus faciles à exploiter.

- *Attaques qui reposent sur des erreurs dans les chaînes de format*. Les erreurs dans les chaînes de format surviennent en raison d'un contrôle insuffisant des valeurs des paramètres entrant des fonctions d'entrée-sortie de format de type *printf()*, *fprintf()*, *scanf()* ou autres de la bibliothèque standard du langage C. Lorsqu'une telle vulnérabilité est présente dans un logiciel, l'individu malintentionné, qui peut envoyer des requêtes formulées spécialement, peut prendre le contrôle complet du système.

  Le système de détection des intrusions analyse automatiquement l'utilisation de telles vulnérabilité et les bloque dans les services de réseau les plus répandus (FTP, POP3, IMAP), s'ils fonctionnent sur l'ordinateur de l'utilisateur.

- *Les attaques ciblant les ordinateurs fonctionnant sous Microsoft Windows,* reposent sur l'exploitation de vulnérabilités d'un logiciel installé (par exemple, des applications telles que Microsoft SQL Server, Microsoft Internet Explorer, Messenger ainsi que les composants systèmes accessibles via le réseau tels que DCom, SMB, Wins, LSASS, IIS5).

De plus, dans certains cas, les attaques d'intrusion exploitent divers types de scripts malveillants, y compris des scripts traités par Microsoft Internet Explorer et diverses versions du ver Helkern. L'attaque Helkern consiste à envoyer vers l'ordinateur distant des paquets UDP d'un certain type capable d'exécuter du code malveillant.

## ACTIVATION ET DESACTIVATION DE LA PREVENTION DES INTRUSIONS

Par défaut, la Prévention des intrusions est activée et fonction en mode optimal. Le cas échéant, vous pouvez désactiver la Prévention des intrusions.

*Pour désactiver la Prévention des intrusions, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.

2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Prévention des intrusions**.

3. Dans la partie droite de la fenêtre, désélectionnez la case **Activer la Prévention des intrusions**.

## MODIFICATION DES PARAMETRES DE BLOCAGE

Par défaut la Prévention des intrusions bloque l'activité de l'ordinateur attaquant durant une heure. Vous pouvez annuler le blocage de l'ordinateur sélectionné ou modifier la durée du blocage.

*Pour modifier la durée du blocage de l'ordinateur attaquant, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.

2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Prévention des intrusions**.

3. Dans la partie droite de la fenêtre, cochez la case **Ajouter l'ordinateur à l'origine de l'attaque à la liste des ordinateurs bloqués pendant** et définissez la durée du blocage.

*Pour annuler le blocage de l'ordinateur attaquant, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et choisissez la rubrique **Protection**.
2. Dans la partie droite de la fenêtre, cliquez sur le bouton gauche de la souris et ouvrez la liste des composants **Protection sur Internet**.
3. Cliquez sur le lien **Surveillance du réseau**.
4. Dans la fenêtre **Surveillance du réseau** qui s'ouvre, sous l'onglet **Ordinateurs bloqués**, sélectionnez l'ordinateur bloqué, puis cliquez sur le lien **Débloquer**.

# ANALYSE DES CONNEXIONS SECURISEES

Les connexions à l'aide des protocoles SSL/TLS protègent le canal d'échange des données sur Internet. Les protocoles SSL/TLS permettent d'identifier les parties qui échangent les données sur la base de certificats électroniques, de crypter les données transmises et de garantir leur intégrité tout au long de la transmission.

Ces particularités du protocole sont exploitées par les individus mal intentionnés afin de diffuser leurs logiciels malveillants car la majorité des logiciels antivirus n'analyse pas le trafic SSL/TLS.

Kaspersky Internet Security analyse les connexions cryptées à l'aide d'un certificat de Kaspersky Lab. Ce certificat sera toujours utilisé pour l'analyse de la sécurité de la connexion.

Par la suite, l'analyse du trafic SSL aura lieu à l'aide du certificat de Kaspersky Lab. Si un certificat non valide est découvert au moment d'établir la connexion avec le serveur (par exemple, il a été remplacé par un individu malintentionné), un message s'affichera et invitera l'utilisateur à accepter ou non le certificat ou à consulter les informations relatives à ce dernier. Si l'application fonctionne en mode automatique, la connexion qui utilise le certificat incorrect sera coupée sans notification.

L'installation automatique du certificat a lieu uniquement lors de l'utilisation de Microsoft Internet Explorer. Vous pouvez utiliser l'Assistant d'installation du certificat pour installer le certificat d'analyse des connexions cryptées en mode semi-automatique dans les navigateurs Microsoft Internet Explorer, Mozilla Firefox (s'il n'est pas lancé) et Google Chrome ainsi que pour obtenir des instructions sur l'installation du certificat de Kaspersky Lab pour le navigateur Opera.

*Pour activer l'analyse des connexions cryptées et installer le certificat de Kaspersky Lab, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, choisissez le composant **Réseau** dans la rubrique **Paramètres avancés**.
3. Dans la fenêtre qui s'ouvre, cochez la case **Analyse des connexions sécurisées**. Quand ce paramètre est activé pour la première fois, l'Assistant d'installation du certificat est lancé automatiquement.
4. Si l'Assistant ne démarre pas, cliquez sur **Installer le certificat**. Cette action lance un Assistant dont il faudra suivre les indications pour l'installation du certificat de Kaspersky Lab.

## DANS CETTE SECTION

## ANALYSE DES CONNEXIONS CRYPTEES DANS MOZILLA FIREFOX

Le navigateur Mozilla Firefox n'utilise pas le référentiel des certificats de Microsoft Windows. Pour analyser les connexions cryptées à l'aide de Firefox, il faut installer manuellement le certificat de Kaspersky Lab.

Vous pouvez également utiliser l'Assistant d'installation du certificat si le navigateur n'est pas lancé.

- *Pour installer manuellement le certificat de Kaspersky Lab, procédez comme suit :*

  1. Dans le menu du navigateur, sélectionnez l'option **Outils** → **Configuration**.
  2. Dans la fenêtre qui s'ouvre, cliquez sur l'onglet **Avancé**.
  3. Dans le groupe **Certificats**, sélectionnez l'onglet **Sécurité** et cliquez sur **Voir le certificat**.
  4. Dans la fenêtre qui s'ouvre, sélectionnez l'onglet **Centres de certification**, puis cliquez sur le bouton **Restaurer**.
  5. Dans la fenêtre qui s'ouvre, sélectionnez le fichier de certificat de Kaspersky Lab. Chemin d'accès au fichier du certificat de Kaspersky Lab : *%AllUsersProfile%\Application Data\Kaspersky Lab\AVP11\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.
  6. Dans la fenêtre qui s'ouvre, cochez les cases afin de choisir les actions dont l'analyse sera soumise à l'application du certificat installé. Pour consulter les informations relatives au certificat, cliquez sur **Voir**.

- *Pour installer manuellement le certificat de Kaspersky Lab pour Mozilla Firefox version 3.x, procédez comme suit :*

  1. Dans le menu du navigateur, sélectionnez l'option **Outils** → **Configuration**.
  2. Dans la fenêtre qui s'ouvre, cliquez sur l'onglet **Avancé**.
  3. Sous l'onglet **Cryptage**, cliquez sur **Voir le certificat**.
  4. Dans la fenêtre qui s'ouvre, sélectionnez l'onglet **Centres de certification** puis cliquez sur le bouton **Importer**.
  5. Dans la fenêtre qui s'ouvre, sélectionnez le fichier de certificat de Kaspersky Lab. Chemin d'accès au fichier du certificat de Kaspersky Lab : *%AllUsersProfile%\Application Data\Kaspersky Lab\AVP11\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.
  6. Dans la fenêtre qui s'ouvre, cochez les cases afin de choisir les actions dont l'analyse sera soumise à l'application du certificat installé. Pour consulter les informations relatives au certificat, cliquez sur **Voir**.

Si votre ordinateur fonctionne sous le système d'exploitation Microsoft Windows Vista ou Microsoft Windows 7, alors le chemin d'accès au fichier du certificat de Kaspersky Lab sera : *%AllUsersProfile%\Kaspersky Lab\AVP11\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.

## ANALYSE DES CONNEXIONS CRYPTEES DANS OPERA

Le navigateur Opera n'utilise pas le référentiel de certificats de Microsoft Windows. Pour analyser les connexions cryptées à l'aide d'Opera, il faut installer manuellement le certificat de Kaspersky Lab.

- *Pour installer le certificat de Kaspersky Lab, procédez comme suit :*

  1. Dans le menu du navigateur, sélectionnez l'option **Outils** → **Configuration**.
  2. Dans la fenêtre qui s'ouvre, cliquez sur l'onglet **Avancé**.

3. Sélectionnez l'onglet **Sécurité** dans la partie gauche de la fenêtre et cliquez sur le bouton **Administration des certificats**.

4. Dans la fenêtre qui s'ouvre, sélectionnez l'onglet **Editeurs**, puis cliquez sur le bouton **Importer**.

5. Dans la fenêtre qui s'ouvre, sélectionnez le fichier de certificat de Kaspersky Lab. Chemin d'accès au fichier du certificat de Kaspersky Lab :
*%AllUsersProfile%\Application Data\Kaspersky Lab\AVP11\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.

6. Dans la fenêtre qui s'affiche, cliquez sur **Installer**. Le certificat de Kaspersky Lab sera installé. Pour consulter les informations relatives au certificat et pour sélectionner les actions qui utiliseront le certificat, sélectionnez le certificat dans la liste et cliquez sur le bouton **Voir**.

*Pour installer le certificat de Kaspersky Lab pour Opera version 9.x, procédez comme suit :*

1. Dans le menu du navigateur, sélectionnez l'option **Outils** → **Configuration**.

2. Dans la fenêtre qui s'ouvre, cliquez sur l'onglet **Avancé**.

3. Sélectionnez l'onglet **Sécurité** dans la partie gauche de la fenêtre et cliquez sur le bouton **Administration des certificats**.

4. Dans la fenêtre qui s'ouvre, sélectionnez l'onglet **Centres de certification** puis cliquez sur le bouton **Importer**.

5. Dans la fenêtre qui s'ouvre, sélectionnez le fichier de certificat de Kaspersky Lab. Chemin d'accès au fichier du certificat de Kaspersky Lab :
*%AllUsersProfile%\Application Data\Kaspersky Lab\AVP11\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.

6. Dans la fenêtre qui s'affiche, cliquez sur **Installer**. Le certificat de Kaspersky Lab sera installé.

Si votre ordinateur fonctionne sous le système d'exploitation Microsoft Windows Vista et Microsoft Windows 7, alors le chemin d'accès au fichier du certificat de Kaspersky Lab sera :
*%AllUsersProfile%\Kaspersky Lab\AVP11\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.

# SURVEILLANCE DU RESEAU

La Surveillance du réseau est un outil conçu pour consulter les informations relatives à l'activité de réseau en temps réel.

*Pour lancer la Surveillance du réseau, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et sélectionnez la rubrique **Protection**.

2. Dans la partie droite de la fenêtre, cliquez sur le bouton gauche de la souris et ouvrez la liste des composants **Protection sur Internet**.

3. Cliquez sur le lien **Surveillance du réseau**.

   La fenêtre **Surveillance du réseau** qui s'ouvre reprend les informations relatives à l'activité de réseau.

Si vous travaillez sur un ordinateur fonctionnant sous Microsoft Windows Vista ou Microsoft Windows 7, vous pouvez lancer la Surveillance du réseau à l'aide du Kaspersky Gadget. Pour ce faire, Kaspersky Gadget doit être configuré de telle manière qu'un de ses boutons est associé à la fonction d'ouverture de la fenêtre de surveillance du réseau (cf. rubrique "Utilisation de Kaspersky Gadget" à la page 71).

*Pour lancer la Surveillance du réseau depuis le gadget,*

cliquez sur le bouton avec l'icône de **Surveillance du réseau** dans l'interface de Kaspersky Gadget.

La fenêtre **Surveillance du réseau** qui s'ouvre reprend les informations relatives à l'activité de réseau.

## CONFIGURATION DES PARAMETRES DU SERVEUR PROXY

Si la connexion à Internet s'opère via un serveur proxy, il faudra alors peut-être configurer les paramètres de connexion à ce dernier. Kaspersky Internet Security applique ces paramètres à quelques composants de la protection ainsi qu'à la mise à jour des bases et des modules de l'application.

Si votre réseau est doté d'un serveur proxy qui utilise un port inhabituel, il faudra l'ajouter à la liste des ports contrôlés (cf. section "Constitution de la liste des ports contrôlés" à la page 133).

*Pour configurer les paramètres du serveur proxy, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, choisissez le composant **Réseau** dans la rubrique **Paramètres avancés**.
3. Dans le groupe **Serveur proxy**, cliquez sur le bouton **Paramètres du serveur proxy**.
4. Dans la fenêtre **Paramètres du serveur proxy** qui s'ouvre, modifiez les paramètres du serveur proxy.

## CONSTITUTION DE LA LISTE DES PORTS CONTROLES

Les composants de la protection tels que l'Antivirus Courrier, l'Anti-Spam (cf. page 134), l'Antivirus Internet (cf. page 99) et l'Antivirus IM contrôlent les flux de données transmis par des protocoles définis et qui transitent par certains TCP-ports ouverts de l'ordinateur. Ainsi, l'Antivirus Courrier analyse les données transmises via le protocole SMTP tandis que l'Antivirus Internet analyse les paquets HTTP.

Vous pouvez activer le contrôle de tous les ports de réseau ou des ports sélectionnés uniquement. Dans le cadre du contrôle des ports sélectionnés, vous pouvez composer une liste d'applications pour lesquelles il faudra contrôler tous les ports.

*Pour ajouter un port à la liste des ports contrôlés, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, choisissez le composant **Réseau** dans la rubrique **Paramètres avancés**.
3. Dans le groupe **Ports contrôlés**, cliquez sur **Sélection**.
4. Dans la fenêtre **Ports de réseau** qui s'ouvre, cliquez sur le lien **Ajouter** afin d'ouvrir la fenêtre d'ajout d'un port de réseau.
5. Saisissez les données requises dans la fenêtre **Port de réseau** qui s'ouvre.

*Pour exclure un port à la liste des ports contrôlés, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, choisissez le composant **Réseau** dans la rubrique **Paramètres avancés**.
3. Dans le groupe **Ports contrôlés**, cliquez sur **Sélection**.
4. Dans la fenêtre **Ports de réseau**, désélectionnez la case ☑ en regard de la description du port.

*Pour composer la liste des applications dont l'ensemble des ports devra être analysé, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.

2. Dans la partie gauche de la fenêtre, choisissez le composant **Réseau** dans la rubrique **Paramètres avancés**.

3. Dans le groupe **Ports contrôlés**, cliquez sur **Sélection**.

4. Dans la fenêtre **Ports de réseau** qui s'ouvre, cochez la case ☑ **Contrôler tous les ports pour les applications indiquées**, puis cliquez sur le lien **Ajouter** dans le groupe du dessous.

5. Sélectionnez l'application dans le menu qui s'ouvre. Si vous sélectionnez **Parcourir**, vous ouvrirez une fenêtre dans laquelle il faudra saisir le chemin d'accès au fichier exécutable. Si vous sélectionnez **Applications**, vous ouvrirez la liste des applications en cours d'exécution.

6. Dans la fenêtre **Application** qui s'ouvre, saisissez une description de l'application sélectionnée.

# ANTI-SPAM

Kaspersky Internet Security reprend le composant *Anti-Spam* qui permet d'identifier les messages non sollicités (spam) et de les traiter conformément aux règles de votre client de messagerie. Ce composant permet de gagner du temps lors de l'utilisation du courrier électronique.

L'Anti-Spam se présente sous la forme d'un plug-in dans les clients de messagerie suivants :

- Microsoft Office Outlook (cf. page 149) ;
- Microsoft Outlook Express (Windows Mail) (cf. page 149) ;
- The Bat! (cf. page 150) ;
- Thunderbird (cf. page 151).

La composition de listes d'expéditeurs autorisés et interdits permet d'indiquer à l'Anti-Spam les messages qu'il faudra considérer comme du courrier normal ou comme du courrier indésirable. Les messages qui ne vous sont pas adressés pourront être également considérés comme indésirables (cf. page 144). De plus, l'Anti-Spam peut rechercher la présence éventuelle dans le message d'expressions autorisées ou interdites, ainsi que d'expressions figurant dans la liste des expressions vulgaires.

Afin qu'Anti-Spam puisse établir efficacement une distinction entre courrier indésirable et courrier normal, il faut l'entraîner (cf. section "Entraînement d'Anti-Spam" à la page 137).

### Algorithme de fonctionnement du composant

L'Anti-Spam utilise l'algorithme d'apprentissage automatique qui permet au composant d'établir une distinction plus précise entre courrier indésirable et courrier normal au fil du temps. Le contenu du message constitue la source de données pour l'algorithme.

Le fonctionnement du composant Anti-Spam est scindé en deux étapes :

1. Application de critères de filtrage stricts aux messages. Ceux-ci permettent de déterminer rapidement si un message appartient ou non au courrier indésirable. L'Anti-Spam attribue l'état *courrier indésirable* ou *courrier normal* au message, l'analyse est suspendue et le message est transmis au client de messagerie pour traitement (cf. étapes 1 à 5 de l'algorithme ci-après).

2. Etude des messages qui ont répondu aux critères stricts de sélection des étapes précédentes. Ces messages ne peuvent pas être automatiquement considérés comme du courrier indésirable. Pour cette raison, l'Anti-Spam doit calculer la *probabilité* de leur appartenance au courrier indésirable.

L'algorithme de fonctionnement de l'Anti-Spam contient les étapes suivantes :

1. L'adresse de l'expéditeur du message est contrôlée afin de voir si elle figure dans les listes des expéditeurs autorisés ou interdits.

- Si l'adresse de l'expéditeur se trouve dans la liste des adresses autorisées, le message reçoit l'état *courrier normal*.

- Si l'adresse de l'expéditeur figure dans la liste des adresses interdites, le message reçoit l'état *courrier indésirable*.

2. Si le message a été envoyé via Microsoft Exchange Explorer et que l'analyse de tels messages est désactivée, le message reçoit l'état *courrier normal*.

3. Le composant vérifie si le message contient des expressions tirées de la liste des expressions autorisées. Si le message contient ne serait-ce qu'une expression de la liste, le message reçoit l'état *courrier normal*. Cette étape est ignorée par défaut.

4. L'analyse du message cherche à déterminer la présence de texte issu de la liste des expressions interdites et de la liste des expressions vulgaires. Le coefficient pondéré est calculé en fonction du nombre de mots de ces listes présents dans le message. Si la somme du coefficient pondéré est supérieure à 100, le message est considéré comme appartenant au *courrier indésirable*. Cette étape est ignorée par défaut.

5. Si le texte contient une adresse reprise dans la base des URL de phishing ou suspectes, le message reçoit l'état *courrier indésirable*.

6. Le message est analysé selon les règles heuristiques. Si l'analyse met en évidence des éléments caractéristiques du courrier indésirable, la probabilité que le message appartienne au courrier indésirable augmente.

7. Le message est analysé à l'aide de la technologie GSG. L'Anti-Spam analyse les images incluses dans le message. Si celles-ci contiennent des éléments caractéristiques du courrier indésirable, la probabilité que le message appartienne au courrier indésirable augmente.

8. Les documents au format .rtf joints au message sont analysés. L'Anti-Spam recherche les éléments caractéristiques du courrier indésirable dans les documents joints. A la fin de l'analyse, l'Anti-Spam calcule l'augmentation de la probabilité qu'un message appartienne au courrier indésirable. La technologie est désactivée par défaut.

9. Le composant procède à la recherche de signes complémentaires caractéristiques du courrier indésirable. Chaque fois qu'un de ces signes est identifié, la probabilité que le message appartienne au courrier indésirable augmente.

10. Si l'Anti-Spam a été entraîné, le message est analysé à l'aide de la technologie iBayes. L'algorithme d'auto-apprentissage iBayes calcule la probabilité qu'un message appartienne au courrier indésirable sur la base de la fréquence d'utilisation d'expressions propres au courrier indésirable dans le message.

Suite à l'analyse du message, l'application détermine la probabilité que le message est un message non sollicité via la valeur de l'*indice de courrier indésirable*. Le message reçoit l'état *courrier indésirable* ou courrier *indésirable potentiel* en fonction des seuils d'indice de courrier indésirable (cf. rubrique "Régulation des seuils d'indice de courrier indésirable" à la page 146). De plus, par défaut, le **texte [!! SPAM]** ou **[!! Probable Spam]** est ajouté par défaut à l'objet du courrier indésirable ou indésirable potentiel (cf. rubrique "**Ajout d'une remarque à l'objet du message**" à la page 147). Ensuite, le message est traité selon les règles pour les clients de messagerie que vous avez définies (cf. rubrique "Configuration du traitement du courrier indésirable par les clients de messagerie" à la page 148).

**DANS CETTE SECTION**



# ACTIVATION ET DESACTIVATION DE L'ANTI-SPAM

Deux méthodes s'offrent à vous pour activer ou désactiver le composant :

- Depuis la fenêtre principale de l'application (cf. section "Fenêtre principale de Kaspersky Internet Security" à la page 42) ;
- Depuis la fenêtre de configuration (cf. rubrique "Fenêtre de configuration des paramètres de l'application" à la page 46).

*Pour activer ou désactiver l'Anti-Spam depuis la fenêtre principale, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et dans la partie gauche de la fenêtre, sélectionnez la rubrique **Protection**.
2. Dans la partie droite de la fenêtre, cliquez sur le bouton gauche de la souris et ouvrez le groupe **Contrôle de l'utilisation du réseau** ou **Protection du système et des applications**.
3. Ouvrez le menu des actions du composant en cliquant sur le bouton **Anti-Spam**, puis sélectionnez l'option **Activer Anti-Spam** pour l'activer ou **Désactiver Anti-Spam** s'il faut désactiver le composant.

   Quand un composant est activé, l'icône à côté de son nom devient vert. Elle est grise lorsqu'il est désactivé.

*Pour activer ou désactiver l'Anti-Spam depuis la fenêtre de configuration, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Anti-Spam**.
3. Dans la partie droite de la fenêtre, cochez la case **Activer l'Anti-Spam** s'il faut activer le composant. Décochez cette case s'il faut désactiver le composant.

# SELECTION DU NIVEAU DE PROTECTION CONTRE LE COURRIER INDESIRABLE

Vous pouvez sélectionner le niveau de protection contre le courrier indésirable en fonction de la fréquence de réception de messages de ce type. Les niveaux de protection contre le courrier indésirable correspondent aux niveaux de protection définis par les experts de Kaspersky Lab.

- **Elevé**. Ce niveau de protection doit être utilisé si vous recevez souvent des messages non sollicités, par exemple lors de l'utilisation de service de messagerie en ligne gratuite. Si vous sélectionnez ce niveau, la fréquence d'identification d'un courrier normal en tant que courrier indésirable peut augmenter.

- **Recommandé**. Ce niveau de protection doit être utilisé dans la majorité des cas.

- **Faible**. Ce niveau de protection doit être utilisé si vous recevez rarement du courrier indésirable, par exemple si vous travaillez dans un milieu protégé (système de messagerie d'entreprise). Si vous sélectionnez ce niveau, la fréquence d'identification d'un courrier normal en tant que courrier indésirable ou potentiellement indésirable peut diminuer.

*Pour sélectionner un des niveaux de protection proposés, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.

2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Anti-Spam**.

3. Dans la partie droite de la fenêtre, sélectionnez le niveau de protection requis en déplaçant le curseur sur le niveau souhaité.

   Le nom du niveau sélectionné apparaît sous le titre du groupe **Niveau de protection**.

Si aucun des niveaux de protection ne répond pas à vos besoins, vous pouvez configurer les paramètres de l'Anti-Spam, par exemple modifier le seuil de l'indice de courrier indésirable ou activer l'analyse des messages de Microsoft Exchange Server. Si vous modifiez la configuration, le nom du niveau de protection devient **Autre**.

Si le fonctionnement de l'Anti-Spam ne vous satisfait pas après la modification des paramètres, vous pouvez restaurer les paramètres de fonctionnement du composant (cf. rubrique "Restauration des paramètres de fonctionnement recommandés de l'Anti-Spam" à la page 151).

# ENTRAINEMENT D'ANTI-SPAM

Un des outils d'identification du courrier indésirable est l'algorithme d'auto-apprentissage iBayes. À l'issue de l'exécution de cet algorithme, l'application décide d'attribuer un certain statut au message sur la base des expressions qu'il renferme. Avant de pouvoir utiliser l'algorithme iBayes, il faut lui présenter des échantillons de phrases de messages utiles et de messages non sollicités, c'est-à-dire l'*entraîner*.

Il existe plusieurs approches pour entraîner l'Anti-Spam :

- Utilisation de l'Assistant d'apprentissage (apprentissage groupé). L'entraînement à l'aide de l'Assistant d'apprentissage est préférable au tout début de l'utilisation de l'Anti-Spam.

- Entraînement de l'Anti-Spam sur les messages sortants.

- Entraînement directement pendant l'utilisation du courrier électronique à l'aide du client de messagerie dont la fenêtre reprend des boutons et des options de menu spéciaux pour l'apprentissage.

- Entraînement lors de l'utilisation des rapports de l'Anti-Spam.

DANS CETTE SECTION



## UTILISATION DE L'ASSISTANT D'APPRENTISSAGE

L'Assistant d'apprentissage permet d'entraîner l'Anti-Spam par lot. Pour ce faire, il faut désigner les répertoires des comptes utilisateur des clients de messagerie Microsoft Office Outlook et Microsoft Outlook Express (Windows Mail) qui contiennent le courrier indésirable et le courrier normal.

Pour assurer une identification efficace du courrier indésirable, il est indispensable de réaliser l'entraînement sur un minimum de 50 exemplaires de courrier normal et de 50 exemplaires de courrier indésirable. L'algorithme iBayes ne fonctionnera pas si ces actions ne sont pas exécutées.

Afin de gagner du temps, l'Assistant réalisera l'entraînement uniquement sur 50 messages de chaque dossier sélectionné.

L'Assistant se compose d'une série de fenêtres (étapes) entre lesquelles vous pouvez naviguer grâce aux boutons **Précédent** et **Suivant**. Pour quitter l'Assistant, cliquez sur le bouton **Terminer**. Pour interrompre l'Assistant à n'importe quelle étape, cliquez sur le bouton **Annuler**.

*Pour lancer l'Assistant, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Anti-Spam**.
3. Dans la partie droite de la fenêtre, dans le groupe **Entraînement d'Anti-Spam**, cliquez sur le bouton **Entraîner**.

Lors de l'apprentissage sur la base du courrier normal, les adresses des expéditeurs sont ajoutées automatiquement à la liste des expéditeurs autorisés. Vous pouvez désactiver cette fonction (cf. rubrique "Ajout d'adresses à la liste des expéditeurs autorisés" à la page 139).

## ENTRAINEMENT D'ANTI-SPAM SUR LE COURRIER SORTANT

Vous pouvez entraîner l'Anti-Spam sur la base de 50 exemples de messages sortants. Une fois que l'apprentissage aura été activé, l'Anti-Spam analysera chaque message que vous envoyez et les utilisera en tant que modèle de courrier normal. L'apprentissage sera terminé après l'envoi de 50 messages.

*Pour activer l'apprentissage de l'Anti-Spam sur la base du courrier sortant, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Anti-Spam**.
3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Configuration**.

   La fenêtre **Anti-Spam** s'ouvre.

4. Sous l'onglet **Avancé**, dans le groupe **Courrier sortant**, cochez la case **Apprentissage sur le courrier sortant**.

Lors de l'apprentissage sur le courrier sortant, les adresses des destinataires de ces messages sont ajoutées automatiquement à la liste des expéditeurs autorisés. Vous pouvez désactiver cette fonction (cf. rubrique "Ajout d'adresses à la liste des expéditeurs autorisés" à la page 139).

## UTILISATION DES ELEMENTS DE L'INTERFACE DU CLIENT DE MESSAGERIE

Vous pouvez entraîner l'Anti-Spam pendant l'utilisation du courrier électronique à l'aide des éléments spéciaux de l'interface de votre client de messagerie (boutons dans la barre d'outils ou éléments du menu).

N'oubliez pas que les boutons et les éléments de menu prévus pour l'apprentissage de l'Anti-Spam apparaîtront dans l'interface du client de messagerie uniquement après l'installation de Kaspersky Internet Security.

*Pour entraîner l'Anti-Spam à l'aide du client de messagerie, procédez comme suit :*

1. Lancez le client de messagerie.
2. Sélectionnez le message à l'aide duquel vous souhaitez entraîner l'Anti-Spam.
3. Exécutez une des actions suivantes en fonction du client de messagerie que vous utilisez :
   - Cliquez sur le bouton **Courrier indésirable** ou **Courrier normal** dans la barre d'outils de Microsoft Office Outlook ;
   - Cliquez sur le bouton **Courrier indésirable** ou **Courrier normal** dans la barre d'outils de Microsoft Outlook Express (Windows Mail) ;
   - Utilisez les éléments **Marquer comme courrier indésirable** ou **Marquer comme courrier normal** dans le menu **Spécial** du client de messagerie The Bat! ;
   - Utilisez le bouton **Courrier indésirable/Courrier normal** dans la barre d'outils du client de messagerie Mozilla Thunderbird.

Une fois que vous aurez choisi une des actions ci-dessus, l'Anti-Spam poursuivra son entraînement sur la base du message sélectionné. Si vous sélectionnez plusieurs messages, l'entraînement portera sur tous les messages sélectionnés.

Si un message est considéré comme normal, l'adresse de l'expéditeur est ajoutée automatiquement à la liste des expéditeurs autorisés. Vous pouvez désactiver cette fonction (cf. rubrique "Ajout d'adresses à la liste des expéditeurs autorisés" à la page 139).

Si vous êtes forcé de sélectionner directement plusieurs messages ou si vous êtes convaincus qu'un dossier ne contient des messages que d'une seule catégorie (courrier indésirable ou courrier normal), il est possible de réaliser un entraînement groupé à l'aide de l'Assistant d'apprentissage (cf. section "Apprentissage d'Anti-Spam" à la page 137).

## AJOUT D'ADRESSES A LA LISTE DES EXPEDITEURS AUTORISES

Lors de l'apprentissage de l'Anti-Spam sur la base du courrier normal à l'aide de l'Assistant d'apprentissage, ainsi que lors de l'apprentissage directement dans la fenêtre du client de messagerie, les adresses des expéditeurs des messages normaux sont ajoutées automatiquement à la liste des expéditeurs autorisés. Cette liste est également enrichie des adresses des destinataires des messages sortants lors de l'apprentissage sur la base du courrier sortant.

Vous pouvez désactiver cette fonction afin que la liste des expéditeurs autorisés ne soit pas enrichie automatiquement suite à l'apprentissage.

*Pour désactiver l'ajout d'adresses à la liste des expéditeurs autorisés, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.

2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Anti-Spam**.

3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Configuration**.

   La fenêtre **Anti-Spam** s'ouvre.

4. Sous l'onglet **Général** dans le groupe **Considérer les messages suivants comme du courrier normal**, cochez la case **D'expéditeurs autorisés** et cliquez sur le bouton **Sélection**.

   La fenêtre **Expéditeurs autorisés** s'ouvre.

5. Décochez la case **Ajouter les adresses des expéditeurs autorisés pendant l'apprentissage d'Anti-Spam**.

### ENTRAINEMENT A L'AIDE DES RAPPORTS

Il est possible d'entraîner l'Anti-Spam sur la base de ses rapports qui reprennent les informations relatives aux messages classés dans la catégorie de courrier indésirable potentiel. L'apprentissage consiste à associer au message le commentaire **courrier indésirable** ou **courrier normal** et à les ajouter à la liste des expéditeurs autorisés ou interdits (cf. rubrique "Expéditeurs interdits et autorisés" à la page 143).

*Pour entraîner l'Anti-Spam sur la base du rapport, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.

2. Le lien **Rapports** ouvre la fenêtre des rapports de Kaspersky Internet Security.

3. Dans la fenêtre qui s'ouvre, sous l'onglet **Rapport**, cliquez sur le bouton **Rapport détaillé**.

   La fenêtre **Rapport détaillé** s'ouvre.

4. Dans la partie gauche de la fenêtre, choisissez la rubrique **Anti-Spam**.

5. Dans la partie droite de la fenêtre, à l'aide des entrées de la colonne **Objet**, définissez les messages qui vont servir à l'apprentissage de l'Anti-Spam. Pour chacun de ces messages, ouvrez le menu contextuel (d'un clic droit de la souris) et sélectionnez un des points du menu pour définir l'action à exécuter sur le message :

   - Marquer comme courrier indésirable.
   - Marquer comme courrier normal.
   - Ajouter à la liste autorisée.
   - Ajouter à la liste interdite.

## ANALYSE DES LIENS DANS LES MESSAGES

L'Anti-Spam permet d'analyser les liens contenus dans les messages électroniques afin de voir s'ils appartiennent à la liste des URL suspectes et des URL de phishing. Ces listes sont livrées avec Kaspersky Internet Security. Si un lien suspect ou de phishing est détecté dans le message, ce dernier sera considéré comme indésirable.

*Pour activer l'analyse des liens selon les bases des URL suspectes et de phishing procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.

2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Anti-Spam**.

3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Configuration**.

   La fenêtre **Anti-Spam** s'ouvre.

4. Sous l'onglet **Général**, dans le groupe **Considérer les messages suivants comme du courrier indésirable**, les cases ☑ **Contenant des liens de la base des URL suspectes** et ☑ **Contenant des liens de la base des URL de phishing** doivent être cochées par défaut. Si les cases ne sont pas cochées, cochez-les.

# IDENTIFICATION DU COURRIER INDESIRABLE SUR LA BASE DES EXPRESSIONS ET DES ADRESSES. COMPOSITION DES LISTES

Vous pouvez composer des listes d'expressions interdites, autorisées ou vulgaires ainsi que des listes d'adresses d'expéditeurs autorisés ou interdits et une liste avec vos propres adresses. En cas d'utilisation de ces listes, l'Anti-Spam analyse le contenu du message afin d'identifier la présence d'expression figurant dans les listes et il vérifie également les adresses de l'expéditeur et des destinataires pour voir si elles correspondent aux entrées des listes. S'il découvre une expression ou une adresse, l'Anti-Spam classe le message dans la catégorie courrier normal ou courrier indésirable en fonction de la liste dans laquelle figure l'expression ou l'adresse.

Les messages suivants sont classés dans la catégorie courrier indésirable :

- Les messages contenant des expressions interdites ou vulgaires dont le coefficient pondéré total dépasse100 ;
- Les messages envoyés depuis une adresse interdite ou qui ne vous sont pas adressés.

Les messages suivants sont classés dans la catégorie courrier normal :

- Les messages contenant des expressions autorisées ;
- Les messages en provenance d'adresses autorisées.

### Masques d'expressions clés et d'adresses d'expéditeurs

Vous pouvez utiliser des *masques d'expression* dans les listes d'expressions autorisées, interdites ou vulgaires. Vous pouvez utiliser des *masques d'adresse* dans les listes d'adresses d'expéditeur autorisé et interdit ainsi que dans la liste des adresses de confiance.

*Un masque* est un modèle de ligne auquel l'expression ou l'adresse est comparée. Certains caractères sont employés dans le masque pour remplacer d'autres caractères : ***** remplace n'importe quelle séquence de caractères, tandis que **?** remplace un caractère. Si de tels caractères sont utilisés dans le masque, celui-ci pourra correspondre à plusieurs expressions ou à plusieurs adresses (cf. exemples ci-dessous).

Si le caractère ***** ou **?** fait partie de l'expression (par exemple, *Quelle heure est-il?*), il faudra le faire précéder du caractère **** afin que l'Anti-Spam l'interprète correctement. Ainsi, au lieu du caractère *****, il faudra utiliser la combinaison *****, et au lieu de **?**, la combinaison **\?** (par exemple, *Quelle heure est-il\?*).

Exemple de masques d'expression :

- *Visitez notre ** : ce masque correspond au message commençant par *Visitez notre* suivi de n'importe quel autre texte.

Exemples de masques d'adresses :

- *admin@test.com* : ce masque correspond uniquement à l'adresse *admin@test.com*.
- *admin@** : ce masque correspond à l'adresse d'un expéditeur portant le nom *admin*, par exemple : *admin@test.com*, *admin@exemple.org.*
- **@test** : ce masque correspond à l'adresse de n'importe quel expéditeur d'un domaine de messagerie commençant par *test*, par exemple : *admin@test.com*, *info@test.org.*
- *info.*@test.???* : ce masque correspond à l'adresse de n'importe quel expéditeur dont le nom commence par *info.* et dont le domaine de messagerie commence par *test.* et se termine par trois caractères quelconques, par exemple : *info.product@test.com*, *info.company@test.org*, mais pas *info.product@test.ru*.

**DANS CETTE SECTION**



# EXPRESSIONS INTERDITES ET AUTORISEES

La liste des *expressions interdites* peut reprendre des expressions qui, d'après vos observations, sont caractéristiques des messages non sollicités et vous pouvez associer un coefficient pondéré à chaque expression. Le *coefficient pondéré* permet d'indiquer à quel point une expression est propre au courrier indésirable : plus le coefficient est élevé, plus il est probable que le message contenant cette expression est indésirable. La valeur du coefficient pondéré de l'expression peut être comprise entre 0 et 100. Si la somme des coefficients pondérés de toutes les expressions découvertes dans le message est supérieure à 100, le message est traité comme un message non sollicité.

Les expressions clés caractéristiques du courrier normal peuvent être saisies dans la liste des *expressions autorisées*. Quand il identifie une de ces expressions dans un message, l'Anti-Spam considère ce dernier comme normal.

La liste des expressions autorisées ou interdites accepte aussi bien des expressions complètes que des masques (cf. rubrique "Identification du courrier indésirable sur la base des expressions et des adresses. Composition des listes" à la page 141).

*Pour composer la liste des expressions autorisées ou interdites, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Anti-Spam**.
3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Configuration**.

   La fenêtre **Anti-Spam** s'ouvre.
4. Sous l'onglet **Général**, procédez comme suit :

   - S'il faut créer une liste d'expressions interdites, dans le groupe **Considérer les messages suivants comme du courrier indésirable**, cochez la case **Contenant des expressions interdites**, puis cliquez sur le bouton **Sélection**, situé à droite.

     La fenêtre **Expressions interdites** s'ouvre.

   - S'il faut créer une liste d'expressions autorisées, dans le groupe **Considérer les messages suivants comme du courrier normal**, cochez la case **Contenant des expressions autorisées**, puis cliquez sur le bouton **Sélection**, situé à droite.

     La fenêtre **Expressions autorisées** s'ouvre.
5. Cliquez sur le lien **Ajouter** pour ouvrir la fenêtre **Expression interdite** (ou la fenêtre **Expression autorisée**).
6. Saisissez l'expression entière ou un masque d'expression et pour l'expression interdite, définissez le coefficient pondéré, puis cliquez sur le bouton **OK**.

Si, à l'avenir, vous ne souhaitez plus utiliser un masque, il n'est pas nécessaire de le supprimer. Il suffit de désélectionner la case en regard du masque en question.

## EXPRESSIONS VULGAIRES

Les experts de Kaspersky Lab ont composé la liste d'expressions vulgaires utilisée par Kaspersky Internet Security. La liste contient les expressions vulgaires dont la présence dans un message permet d'affirmer avec une certitude très élevée qu'il s'agit d'un message non sollicité. Vous pouvez enrichir la liste et y ajouter des expressions complètes ou des masques d'expression (cf. rubrique "Identification du courrier indésirable sur la base des expressions et des adresses. Composition des listes" à la page 141).

*Pour modifier la liste des expressions vulgaires, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Anti-Spam**.
3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Configuration**.

   La fenêtre **Anti-Spam** s'ouvre.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Général**, dans le groupe **Considérer les messages suivants comme du courrier indésirable**, cochez la case **Contenant des expressions interdites** puis cliquez sur le bouton **Sélection**.

   La fenêtre **Expressions interdites** s'ouvre.
5. Cochez la case **Considérer les expressions vulgaires comme interdites**, puis cliquez sur le lien **expressions vulgaires** pour ouvrir la fenêtre **Accord**.
6. Lisez le texte du contrat et si vous en acceptez les dispositions présentées dans la fenêtre, cochez la case dans la partie inférieure de la fenêtre, puis cliquez sur **OK**.

   La fenêtre **Expressions vulgaires** s'ouvre.
7. Cliquez sur le lien **Ajouter** pour ouvrir la fenêtre **Expression interdite**.
8. Saisissez l'expression complète ou son masque et définissez le coefficient pondéré de l'expression, puis cliquez sur **OK**.

Si, à l'avenir, vous ne souhaitez plus utiliser un masque quelconque, il n'est pas nécessaire de le supprimer. Il suffit de désélectionner la case en regard du masque en question dans la fenêtre **Langage vulgaire**.

## EXPEDITEURS INTERDITS ET AUTORISES

La liste des *expéditeurs interdits* reprend les adresses des expéditeurs dont les messages seront considérés comme indésirables par l'Anti-Spam. Les adresses des expéditeurs qui ne devraient pas envoyer de courrier indésirable sont reprises dans la liste des *expéditeurs autorisés*. Cette liste est créée automatiquement pendant l'entraînement du composant Anti-Spam (cf. rubrique "Ajout d'adresses à la liste des expéditeurs autorisés" à la page 139). De plus, vous pouvez enrichir vous-même cette liste.

Vous pouvez ajouter à la liste des expéditeurs autorisés ou interdits des adresses complètes ou des masques d'adresses (cf. rubrique "Identification du courrier indésirable sur la base des expressions et des adresses. Composition des listes" à la page 141).

*Pour composer la liste des expéditeurs autorisés ou interdits, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Anti-Spam**.
3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Configuration**.

   La fenêtre **Anti-Spam** s'ouvre.

4. Sous l'onglet **Général**, procédez comme suit :

   - S'il faut créer une liste d'expéditeurs interdits, dans le groupe **Considérer les messages suivants comme du courrier indésirable**, cochez la case **D'expéditeurs interdits**, puis cliquez sur le bouton **Sélection**, situé à droite.

     La fenêtre **Expéditeurs interdits** s'ouvre.

   - S'il faut créer une liste d'expéditeurs autorisés, dans le groupe **Considérer les messages suivants comme du courrier normal**, cochez la case **D'expéditeurs autorisés**, puis cliquez sur le bouton **Sélection**, situé à droite.

     La fenêtre **Expéditeurs autorisés** s'ouvre.

5. Cliquez sur le lien **Ajouter** pour ouvrir la fenêtre **Masque d'adresse de courrier électronique**.

6. Saisissez le masque de l'adresse, puis cliquez sur **OK**.

Si, à l'avenir, vous ne souhaitez plus utiliser un masque, il n'est pas nécessaire de le supprimer. Il suffit de désélectionner la case en regard du masque en question.

## VOS ADRESSES

Vous pouvez composer une liste reprenant vos adresses électroniques afin que l'Anti-Spam considère comme du courrier indésirable les messages qui ne vous sont pas adressés.

*Pour composer la liste de vos adresses, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.

2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Anti-Spam**.

3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Configuration**.

   La fenêtre **Anti-Spam** s'ouvre.

4. Sous l'onglet **Général**, cochez la case **Dont je ne suis pas le destinataire** et cliquez sur **Mes adresses**.

   La fenêtre **Mes adresses** s'ouvre.

5. Cliquez sur le lien **Ajouter** pour ouvrir la fenêtre **Masque d'adresse de courrier électronique**.

6. Saisissez le masque de l'adresse, puis cliquez sur **OK**.

Si, à l'avenir, vous ne souhaitez plus utiliser un masque quelconque, il n'est pas nécessaire de le supprimer. Il suffit de désélectionner la case en regard du masque en question dans la fenêtre **Mes adresses**.

## EXPORTATION ET IMPORTATION DES LISTES D'EXPRESSIONS ET D'ADRESSES

Une fois que vous avez créé une liste d'adresses et d'expressions, vous pouvez l'utiliser à plusieurs reprises : par exemple, transférer les adresses dans une liste identique sur un autre ordinateur doté de Kaspersky Internet Security.

Voici la marche est à suivre :

1. Procédez à une *exportation*, c.-à-d. copiez les entrées de la liste dans un fichier.

2. Transférez le fichier créé sur un autre ordinateur (par exemple, envoyez-le par courrier électronique ou via une clé USB).

3. Procédez à une *importation*, c.-à-d. ajoutez les entrées du fichier à une liste identique sur un autre ordinateur.

Lors de l'exportation de la liste, vous serez invité à copier uniquement l'élément sélectionné de la liste ou toute la liste. Lors de l'importation, vous pouvez ajouter de nouveaux éléments à la liste ou écraser la liste existante par la liste importée.

*Pour exporter les entrées de la liste, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Anti-Spam**.
3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Configuration**.

   La fenêtre **Anti-Spam** s'ouvre.
4. Sous l'onglet **Général**, cochez la case dans la ligne contenant le nom de la liste de laquelle il faut exporter les entrées, puis cliquez sur le bouton qui lui correspond à droite.
5. Dans la fenêtre qui s'ouvre avec la liste, cochez les cases en regarde des entrées qu'il faut inclure dans le fichier.
6. Cliquez sur le lien **Exporter**.

   Une fenêtre s'ouvre et vous avez la possibilité d'exporter uniquement les éléments sélectionnés. Exécutez dans cette fenêtre une des opérations suivantes :

   - Cliquez sur le bouton **Oui** s'il faut uniquement inclure les entrées sélectionnées ;
   - Cliquez sur le bouton **Non** s'il faut inclure la liste complète.
7. Dans la fenêtre qui s'ouvre, désignez le type et le nom du fichier à enregistrer et confirmez l'enregistrement.

*Pour importer les entrées d'un fichier dans la liste, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Anti-Spam**.
3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Configuration**.

   La fenêtre **Anti-Spam** s'ouvre.
4. Sous l'onglet **Général**, cochez la case dans la ligne contenant le nom de la liste dans laquelle il faut importer les entrées, puis cliquez sur le bouton à droite.
5. Dans la fenêtre contenant la liste, cliquez sur le lien **Importer**. Si vous importez la liste des expéditeurs autorisés, alors un menu dans lequel il faudra choisir l'option **Importer depuis un fichier** apparaît. Pour les autres listes, il n'est pas nécessaire de choisir une option du menu.

   Si la liste n'est pas vide, une fenêtre s'ouvre et vous avez la possibilité d'ajouter les éléments importés. Exécutez dans cette fenêtre une des opérations suivantes :

   - Cliquez sur le bouton **Oui** s'il faut ajouter des entrées du fichier à la liste ;
   - Cliquez sur le bouton **Non** s'il faut remplacer les entrées actuelles de la liste par celles du fichier.
6. Dans la fenêtre qui s'ouvre, sélectionnez le fichier contenant la liste des entrées qu'il faut importer.

### Importation de la liste des expéditeurs autorisés depuis le carnet d'adresses

Il est possible d'importer les adresses du carnet d'adresses de Microsoft Office Outlook/Microsoft Outlook Express (Windows Mail) dans la liste des expéditeurs autorisés.

*Pour importer la liste des expéditeurs autorisés depuis le carnet d'adresses, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Anti-Spam**.
3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Configuration**.

   La fenêtre **Anti-Spam** s'ouvre.
4. Sous l'onglet **Général** dans le groupe **Considérer les messages suivants comme du courrier normal**, cochez la case **D'expéditeurs autorisés** et cliquez sur le bouton **Sélection**.

   La fenêtre **Expéditeurs autorisés** s'ouvre.
5. Cliquez sur le lien **Importer** afin d'ouvrir la fenêtre de sélection de la source, puis choisissez l'option **Importer depuis le carnet d'adresses**.
6. Dans la fenêtre qui s'ouvre, sélectionnez le carnet d'adresses requis.

## REGULATION DES SEUILS D'INDICE DE COURRIER INDESIRABLE

L'identification du courrier indésirable repose sur l'utilisation de technologies modernes de filtrage qui permettent à l'Anti-Spam de séparer (cf. rubrique "Entraînement d'Anti-Spam" à la page 137) le courrier (potentiellement) indésirable du courrier normal. Chaque élément de courrier normal ou de courrier indésirable se voit attribuer un coefficient.

Quand un message arrive dans votre boîte aux lettres, l'Anti-Spam exploite la technologie iBayes pour voir si le message contient des éléments de courrier indésirable ou de courrier normal. Les coefficients de chaque élément de courrier indésirable (courrier normal) sont ajoutés pour obtenir l'*indice de courrier indésirable*. Plus l'indice de courrier indésirable est élevé, plus la probabilité que le message soit un message non sollicité est grande. Par défaut, un message est considéré comme normal si l'indice de courrier indésirable est inférieur à 60. Si l'indice de courrier indésirable est supérieur à 60, alors le message est classé dans la catégorie du courrier indésirable potentiel. Et si la valeur est supérieure à 90, le message est considéré comme du courrier indésirable. Vous pouvez modifier le seuil de l'indice de courrier indésirable.

*Pour modifier le seuil de l'indice de courrier indésirable, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Anti-Spam**.
3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Configuration**.

   La fenêtre **Anti-Spam** s'ouvre.
4. Sous l'onglet **Avancé**, dans le groupe **Indice de courrier indésirable**, modifiez la valeur de l'indice à l'aide du curseur ou du champ de saisie.

## UTILISATION DES SIGNES COMPLEMENTAIRES QUI INFLUENCENT L'INDICE DE COURRIER INDESIRABLE

Les résultats du calcul de l'indice de courrier indésirable peuvent être influencés par des éléments complémentaires du message tels que l'absence d'adresse du destinataire dans le champ "À" ou un objet un peu trop long (plus de 250 caractères). Quand ces signes sont présents, la probabilité que le message soit non sollicité augmente. Et par

conséquent, la valeur de l'indice de courrier indésirable augmente. Vous pouvez choisir les éléments complémentaires à prendre en compte durant l'analyse des messages.

*Pour utiliser des éléments complémentaires qui augmenteront la valeur de l'indice de courrier indésirable, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Anti-Spam**.
3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Configuration**.

   La fenêtre **Anti-Spam** s'ouvre.
4. Sous l'onglet **Avancé**, cliquez sur le bouton **Avancé**.
5. Dans la fenêtre **Avancé** qui s'ouvre, cochez la case ☑ en regard des éléments dont il faudra tenir compte pendant l'analyse des messages et qui augmenteront l'indice de courrier indésirable.

## SELECTION DE L'ALGORITHME D'IDENTIFICATION DU COURRIER INDESIRABLE

La recherche des messages non sollicités dans le courrier s'opère à l'aide d'algorithmes d'identification :

- **Analyse heuristique**. L'Anti-Spam analyse les messages à l'aide de règles heuristiques. L'analyse heuristique est toujours utilisée.
- **Identification des images (GSG)**. L'Anti-Spam applique la technologie GSG pour identifier le courrier indésirable sous la forme d'images.
- **Analyse des documents .rtf joints**. L'Anti-Spam analyse les documents joints au message afin de voir s'ils présentent des éléments caractéristiques du courrier indésirable.
- **Algorithme d'auto-apprentissage par l'analyse de texte (iBayes)**. L'algorithme d'iBayes repose sur l'analyse de la fréquence d'utilisation de mots caractéristiques du spam dans le texte du message. À l'issue de l'analyse, le message est considéré comme indésirable ou normal. Avant de commencer à utiliser l'algorithme iBayes, vous devez absolument entraîner l'Anti-Spam (cf. rubrique "Entraînement d'Anti-Spam" à la page 137).

*Afin d'utiliser/de ne pas utiliser un algorithme quelconque d'identification du courrier indésirable lors de l'analyse du courrier, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Anti-Spam**.
3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Configuration**.

   La fenêtre **Anti-Spam** s'ouvre.
4. Sous l'onglet **Avancé** dans le groupe **Algorithmes d'identification**, cochez/décochez les cases correspondantes.

## AJOUT D'UNE REMARQUE A L'OBJET DU MESSAGE

L'Anti-Spam peut ajouter les indications suivantes au champ **Objet** des messages qui ont été classés dans la catégorie courrier indésirable ou courrier indésirable potentiel :

- **[!! SPAM]** : pour les messages considérés comme indésirables.

- **[?? Probable Spam]** : pour les messages considérés comme courrier indésirable potentiel.

La présence de cette remarque dans l'objet du message peut vous aider à différencier visuellement le courrier indésirable et potentiellement indésirable lors du survol de la liste des messages.

*Pour que l'Anti-Spam ajoute/n'ajoute pas de remarque à l'objet des messages, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Anti-Spam**.
3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Configuration**.

   La fenêtre **Anti-Spam** s'ouvre.
4. Sous l'onglet **Avancé**, dans le groupe **Actions**, cochez les cases ☑ en regard des remarques qu'il faut ajouter à l'objet des messages. Une fois la case cochée, vous pouvez modifier le texte de la remarque. Pour ne pas ajouter de remarque, désélectionnez la case correspondante.

## EXCLUSION DES MESSAGES MICROSOFT EXCHANGE SERVER DE L'ANALYSE

Vous pouvez exclure de la recherche du courrier indésirable les messages envoyés dans le cadre du réseau interne (par exemple, le courrier d'entreprise). N'oubliez pas que les messages seront considérés comme des messages internes si Microsoft Office Outlook est utilisé sur tous les postes du réseau et que les boîtes aux lettres des utilisateurs se trouvent sur un même serveur Exchange ou que ces serveurs sont unis par des connecteurs X400.

Par défaut, l'Anti-Spam n'analyse pas les messages de Microsoft Exchange Server.

*Pour que l'Anti-Spam analyse les messages de Microsoft Exchange Server, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Anti-Spam**.
3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Configuration**.

   La fenêtre **Anti-Spam** s'ouvre.
4. Dans la fenêtre qui s'ouvre, Sous l'onglet **Avancé** dans le groupe **Exclusions**, décochez la case ☑ **Ne pas analyser les messages Microsoft Exchange Server**.

## CONFIGURATION DU TRAITEMENT DU COURRIER INDESIRABLE PAR LES CLIENTS DE MESSAGERIE

Si l'analyse indique que le message est un exemplaire de courrier indésirable ou de courrier indésirable potentiel, la suite des opérations réalisées par l'Anti-Spam dépendra de l'état du message et de l'action sélectionnée. Par défaut, les messages électroniques classés comme courrier indésirable ou courrier indésirable potentiel sont modifiés : le texte **[!! SPAM]** ou **[?? Probable Spam]** est ajouté respectivement au champ **Objet du message** (cf. rubrique "Ajout d'une remarque à l'objet du message" à la page 147).

Vous pouvez sélectionner des actions complémentaires à exécuter sur le courrier indésirable et le courrier indésirable potentiel. Des plug-ins spéciaux sont prévus dans les clients de messagerie Microsoft Office Outlook et Microsoft Outlook Express (Windows Mail). Pour les clients de messagerie The Bat! et Thunderbird, vous pouvez configurer des règles de filtrage.

**DANS CETTE SECTION**



## MICROSOFT OFFICE OUTLOOK

Par défaut, le courrier qui est considéré comme courrier indésirable ou courrier indésirable potentiel par l'Anti-Spam est marqué à l'aide du texte **[!! SPAM]** ou **[?? Probable Spam]** dans l'**Objet**. Si un traitement complémentaire des messages après l'analyse par l'Anti-Spam s'impose, vous pouvez configurer Microsoft Office Outlook. La fenêtre de configuration du traitement du courrier indésirable s'ouvre automatiquement au premier lancement du client de messagerie après le chargement de Kaspersky Internet Security. De plus, les paramètres de traitement du courrier indésirable et du courrier indésirable potentiel dans Microsoft Office Outlook sont repris sur l'onglet spécial **Anti-Spam** du menu **Service** → **Paramètres**.

## MICROSOFT OUTLOOK EXPRESS (WINDOWS MAIL)

Par défaut, le courrier qui est considéré comme courrier indésirable ou courrier indésirable potentiel par l'Anti-Spam est marqué à l'aide du texte **[!! SPAM]** ou **[?? Probable Spam]** dans l'**Objet**. Si un traitement complémentaire des messages après l'analyse par l'Anti-Spam s'impose, vous pouvez configurer Microsoft Outlook Express (Windows Mail).

La fenêtre de configuration du traitement du courrier indésirable s'ouvre au premier lancement du client de messagerie après l'installation de l'application. Vous pouvez l'ouvrir également en cliquant sur le bouton **Configuration** situé dans la barre d'outils du client de messagerie à côté des boutons **Courrier indésirable** et **Courrier normal**.

## CREATION DE REGLES DE TRAITEMENT DES MESSAGES POUR LE COURRIER INDESIRABLE

Les instructions ci-dessous décrivent la création d'une règle de traitement des messages pour le courrier indésirable en utilisant l'Anti-Spam dans le client de messagerie Microsoft Office Outlook. Vous pouvez vous inspirer de ces instructions pour créer vos propres règles.

*Pour créer une règle de traitement d'un message à la recherche de courrier indésirable, procédez comme suit :*

1. Lancez Microsoft Office Outlook et utilisez la commande **Service** →**Règles et notifications** de la fenêtre principale de l'application. La méthode à employer pour ouvrir l'Assistant dépend de la version de Microsoft Office Outlook que vous utilisez. Dans notre cas, nous envisageons la création d'une règle dans Microsoft Office Outlook 2003.

2. Dans la fenêtre **Règles et notification**, passez à l'onglet **Règles pour le courrier électronique** et cliquez sur **Nouvelle**. Cette action entraîne le lancement de l'Assistant de création d'une règle. Il contient une succession de fenêtres (étapes) :

   a. Vous devez choisir entre la création d'une règle à partir de zéro ou selon un modèle. Sélectionnez l'option **Créer une règle** et en guise de condition de l'analyse, sélectionnez **Analyse des messages après la réception**. Cliquez sur **Suivant**.

   b. Dans la fenêtre de sélection des conditions de tri des messages, cliquez sur **Suivant** sans cocher aucune case. Confirmez l'application de cette règle à tous les messages reçus dans la fenêtre de confirmation.

c. Dans la fenêtre de sélection des actions sur les messages, cochez la case ☑ **exécuter une action complémentaire** dans la liste des actions. Dans la partie inférieure de la fenêtre, cliquez sur le lien **action complémentaire**. Dans la fenêtre qui s'ouvre, sélectionnez **Kaspersky Anti-Spam** dans la liste déroulante, puis cliquez sur **OK**.

d. Dans la fenêtre des exclusions de la règle, cliquez sur **Suivant** sans cocher aucune case.

e. Dans la fenêtre finale de création de la règle, vous pouvez changer son nom (le nom par défaut est Kaspersky Anti-Spam). Assurez-vous que la case ☑ **Activer la règle** est cochée, puis cliquez sur **Terminer**.

3. Par défaut, la nouvelle règle sera ajoutée en tête de la liste des règles de la fenêtre **Règles et notifications**. Déplacez cette règle à la fin de la liste si vous voulez qu'elle soit appliquée en dernier lieu au message.

Tous les messages qui arrivent dans la boîte aux lettres sont traités sur la base des règles. L'ordre d'application des règles dépend de la priorité attribuée à chaque règle. Les règles sont appliquées dans l'ordre de la liste. Chaque règle a une priorité inférieure à la règle précédente. Vous pouvez élever ou réduire la priorité d'application d'une règle en la déplaçant vers le haut ou vers le bas dans la liste. Si vous ne souhaitez pas que le message, après l'exécution d'une règle quelconque, soit traité par une règle de l'Anti-Spam, il faudra cocher la case ☑ **arrêter le traitement ultérieur des règles** dans les paramètres de cette règle (cf. Etape 3 de la fenêtre de création des règles).

## THE BAT!

Les actions à exécuter sur le courrier indésirable et le courrier indésirable potentiel dans The Bat! sont définies à l'aide des outils du client.

➧ *Pour passer à la configuration des règles de traitement du courrier indésirable dans The Bat!, procédez comme suit :*

1. Dans le menu **Configuration** dans le menu **Propriétés** du client de messagerie.

2. Sélectionnez l'objet **Protection contre le courrier indésirable** dans l'arborescence des paramètres.

Les paramètres de protection contre le courrier indésirable sont appliqués à tous les modules de l'Anti-Spam installés sur l'ordinateur compatibles avec The Bat!.

Vous devez définir le niveau d'évaluation et indiquer comment agir sur les messages correspondant au niveau défini (pour l'Anti-Spam, la probabilité que le message est un exemple de courrier indésirable) :

- Supprimer les messages dont le niveau d'évaluation est supérieur au niveau indiqué ;
- Déplacer les messages du niveau défini dans un dossier spécial pour les messages non sollicités ;
- Déplacer les messages non sollicités marqués d'un en-tête spécial dans le dossier du courrier indésirable ;
- Laisser les messages non sollicités dans le dossier **Entrant**.

Suite au traitement des messages électroniques, Kaspersky Internet Security attribue le statut courrier indésirable ou courrier indésirable potentiel en fonction d'un indice dont vous pouvez modifier la valeur. Dans The Bat!, on retrouve un algorithme spécial d'évaluation des messages qui repose également sur un indice de courrier indésirable. Afin d'éviter les écarts entre l'indice de courrier indésirable dans Kaspersky Internet Security et dans The Bat!, tous les messages analysés par l'Anti-Spam reçoivent une évaluation correspondant à l'état du message : courrier normal - 0%, courrier indésirable potentiel - 50%, courrier indésirable - 100%. Ainsi, l'évaluation du message dans The Bat! correspond non pas à l'indice de courrier indésirable attribué par l'Anti-Spam mais bien à l'indice de l'état correspondant.

Pour de plus amples informations sur l'évaluation du courrier indésirable et sur les règles de traitement, consultez la documentation relative au client de messagerie The Bat!.

### THUNDERBIRD

Par défaut, le courrier qui est considéré comme courrier indésirable ou courrier indésirable potentiel par l'Anti-Spam est marqué à l'aide du texte **[!! SPAM]** ou **[?? Probable Spam]** dans l'**Objet**. Si un traitement complémentaire des messages après l'analyse par l'Anti-Spam s'impose, vous pouvez configurer Thunderbird dans la fenêtre de configuration accessible via **Outils** → **Filtres de messages** (pour obtenir les instructions d'utilisation détaillées du client de messagerie, consultez l'aide de Mozilla Thunderbird).

Le plug-in de l'Anti-Spam pour Thunderbird permet d'étudier les messages reçus et envoyés à l'aide de ce client de messagerie et de vérifier si le courrier contient des messages non sollicités. Le module est intégré à Thunderbird et transmet les messages à l'Anti-Spam afin qu'ils puissent être analysés à l'aide de la commande du menu **Outils** → **Traquer les indésirables dans ce dossier**. Ainsi, la recherche des messages non sollicités revient à Kaspersky Internet Security et non pas à Thunderbird. Les fonctions de Thunderbird ne sont en rien modifiées.

L'état du plug-in de l'Anti-Spam apparaît sous la forme d'une icône dans la barre d'état de Thunderbird. Une icône grise indique qu'un problème s'est présenté dans le fonctionnement du plug-in ou que l'Anti-Spam est désactivé. Vous pouvez ouvrir la fenêtre de configuration des paramètres de Kaspersky Internet Security d'un double-clique sur l'icône de l'application. Pour passer à la configuration des paramètres de l'**Anti-Spam**, cliquez sur le bouton **Configuration** dans le groupe Anti-Spam.

## RESTAURATION DES PARAMETRES DE FONCTIONNEMENT RECOMMANDES DE L'ANTI-SPAM

Si le fonctionnement de l'Anti-Spam après la modification des paramètres ne vous satisfait pas, vous pouvez restaurer les paramètres recommandés par Kaspersky Lab et repris dans le niveau de protection **Recommandé**.

*Pour restaurer les paramètres de protection par défaut contre le courrier indésirable, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Anti-Spam**.
3. Dans la partie droite de la fenêtre, dans le groupe **Niveau de protection**, cliquez sur **Par défaut**.

   Le niveau de protection prendra la valeur **Recommandé**.

# ANTI-BANNIERE

*L'Anti-bannière* a été développé pour bloquer l'affichage des bannières sur les sites que vous visitez et dans l'interface de quelques applications. Le message publicitaire des bannières peut vous distraire tandis que le chargement des bannières augmente le volume du trafic téléchargé.

Avant de pouvoir s'afficher sur la page Web ou dans la fenêtre de l'application, la bannière doit être téléchargée depuis Internet. L'Anti-bannière vérifie l'adresse d'où le téléchargement a lieu. Si l'adresse correspond à un masque quelconque de la liste livrée avec Kaspersky Internet Security ou de la liste des adresses de bannières interdites que vous ayez créée, l'Anti-bannière bloque le bandeau publicitaire. Le blocage des bannières dont les masques d'adresse ne figurent pas dans les listes citées est décidé par l'analyseur heuristique (cf. section "Sélection des méthodes d'analyse" à la page 153).

De plus, vous pouvez créer la liste des adresses autorisées sur la base de laquelle les bannières seront affichées.

**DANS CETTE SECTION**



# ACTIVATION ET DESACTIVATION DE L'ANTI-BANNIERE

Après l'installation de Kaspersky Internet Security, l'Anti-bannière est désactivé. Il ne bloque pas l'affichage des bannières. Pour pouvoir bloquer les bannières, il faut activer l'Anti-bannière.

Pour que toutes les bannières soient affichées, l'Anti-bannière doit être désactivé. S'il faut autoriser l'affichage de certaines bannières uniquement, il faudra utiliser la liste des adresses de bannière autorisées (cf. section "Composition des listes d'adresses de bannières autorisées ou interdites" à la page 153).

Deux méthodes s'offrent à vous pour activer ou désactiver le composant :

- Depuis la fenêtre principale de l'application (cf. section "Fenêtre principale de Kaspersky Internet Security" à la page 42) ;
- depuis la fenêtre de configuration (cf. rubrique "Fenêtre de configuration des paramètres de l'application à la page 46).

*Pour activer ou désactiver l'Anti-bannière depuis la fenêtre principale, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et dans la partie gauche de la fenêtre, sélectionnez la rubrique **Protection**.
2. Dans la partie droite de la fenêtre, cliquez sur le bouton gauche de la souris et ouvrez le groupe **Contrôle de l'utilisation du réseau**.
3. Ouvrez le menu des actions du composant en cliquant sur le bouton **Anti-bannière**, puis sélectionnez l'option **Activer Anti-bannière** pour l'activer ou **Désactiver Anti-bannière** s'il faut désactiver le composant.

   Quand un composant est activé, l'icône à côté de son nom devient vert. Elle est grise lorsqu'il est désactivé.

*Pour activer ou désactiver l'Anti-bannière depuis la fenêtre de configuration, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Anti-bannière**.
3. Dans la partie droite de la fenêtre, cochez la case **Activer l'Anti-bannière** s'il faut activer le composant. Décochez cette case s'il faut désactiver le composant.

## SELECTION DES METHODES D'ANALYSE

Vous pouvez désigner la méthode que devra utiliser l'Anti-bannière pour analyser les adresses d'où les bannières pourront être chargées. En plus de ces méthodes, l'Anti-bannière analyse l'adresse afin de voir si elle correspond aux masques de la liste des adresses autorisées ou interdites, quand de telles listes sont utilisées.

*Pour sélectionner les méthodes d'analyse des adresses par l'Anti-bannière, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Anti-bannière**.
3. Dans la partie droite de la fenêtre, dans le groupe **Méthodes d'analyse**, cochez la case en regard des noms de méthode à utiliser.

## COMPOSITION DES LISTES D'ADRESSES DE BANNIERES AUTORISEES OU INTERDITES

Les listes d'adresses de bannières autorisées ou interdites permettent d'indiquer les adresses au départ desquelles l'affichage des bannières doit être autorisé ou interdit. Composez une liste de masques d'adresses interdites et l'Anti-bannière bloquera le chargement et l'affichage des bannières depuis les adresses correspondant à ces masques. Composez une liste de masques d'adresses autorisées et l'Anti-bannière chargera et affichera les bannières depuis les adresses correspondant à ces masques.

*Pour ajouter un masque à la liste des adresses autorisées ou interdites, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Anti-bannière**.
3. Dans la partie droite de la fenêtre, dans le groupe **Avancé**, cochez la case **Utiliser la liste des URL interdites** (ou **Utiliser la liste des URL autorisées**), puis cliquez sur le bouton **Configuration** situé sur la même ligne que le nom de la liste.

   La fenêtre **Adresses interdites** (ou **Adresses autorisées**) s'ouvre.
4. Cliquez sur le lien **Ajouter** et ouvrez la fenêtre **Masque d'adresse (URL)**.
5. Saisissez le masque de l'adresse interdite (autorisée) de la bannière et cliquez sur le bouton **OK**.

Si, à l'avenir, vous ne souhaitez plus utiliser un masque, il n'est pas nécessaire de le supprimer. Il suffit de désélectionner la case en regard du masque en question.

## EXPORTATION ET IMPORTATION DES LISTES D'ADRESSES

Une fois que vous aurez créé une liste d'adresses de bannière autorisées ou interdites, vous pourrez la réutiliser, par exemple en transférant les adresses de bannière dans une liste identique sur un autre ordinateur équipé de Kaspersky Internet Security.

Voici la marche est à suivre :

1. Procédez à une *exportation*, c.-à-d. copiez les entrées de la liste dans un fichier.
2. Transférez le fichier créé sur un autre ordinateur (par exemple, envoyez-le par courrier électronique ou via une clé USB).
3. Procédez à une *importation*, c.-à-d. ajoutez les entrées du fichier à une liste identique sur un autre ordinateur.

Lors de l'exportation de la liste, vous serez invité à copier uniquement l'élément sélectionné de la liste ou toute la liste. Lors de l'importation, vous pouvez ajouter de nouveaux éléments à la liste ou écraser la liste existante par la liste importée.

*Pour exporter les adresses de bannière depuis la liste des adresses autorisées ou interdites, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Anti-bannière**.
3. Dans la partie droite de la fenêtre, dans le groupe **Avancé**, cliquez sur le bouton **Configuration** situé sur la ligne du nom de la liste au départ de laquelle il faut copier l'adresse.
4. Dans la fenêtre **Adresses autorisées** (ou **Adresses interdites**), cochez les cases en regard des adresses qu'il faut inclure dans le fichier.
5. Le lien **Exporter** ouvre une fenêtre qui propose d'exporter uniquement les éléments sélectionnés.

   Exécutez dans cette fenêtre une des opérations suivantes :

   - Cliquez sur le bouton **Oui** s'il faut uniquement inclure les adresses sélectionnées ;
   - Cliquez sur le bouton **Non** s'il faut inclure la liste complète.
6. Dans la fenêtre qui s'ouvre, saisissez un nom pour le fichier à enregistrer et confirmez l'enregistrement.

*Pour importer les adresses de bannière d'un fichier dans la liste des adresses autorisées ou interdites, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Anti-bannière**.
3. Dans la partie droite de la fenêtre, dans le groupe **Avancé**, cliquez sur le bouton **Configuration** situé sur la ligne du nom de la liste à laquelle il faut ajouter l'adresse.
4. Dans la fenêtre **Adresses autorisées** (ou la fenêtre **Adresses interdites** qui s'ouvre, cliquez sur le lien **Importer**.

   Si la liste n'est pas vide, une fenêtre s'ouvre et vous avez la possibilité d'ajouter les éléments importés. Exécutez dans cette fenêtre une des opérations suivantes :

   - Cliquez sur le bouton **Oui** s'il faut ajouter des entrées du fichier à la liste ;
   - Cliquez sur le bouton **Non** s'il faut remplacer les entrées actuelles de la liste par celles du fichier.
5. Dans la fenêtre qui s'ouvre, sélectionnez le fichier contenant la liste des entrées qu'il faut importer.

# ENVIRONNEMENT PROTEGE

L'Environnement protégé est un environnement sécurisé et isolé du système d'exploitation principal qui permet d'exécuter des applications dont la sécurité est douteuse ou d'utiliser des services de transactions bancaires en ligne lorsque la sécurité de la saisie des données est un élément primordial. Dans l'Environnement protégé, les objets réels du système d'exploitation ne sont pas soumis aux modifications. C'est pourquoi, même si vous lancez l'application infectée dans l'Environnement protégé, toutes les actions de cette application seront limitées par l'environnement virtuel et n'influenceront pas le système d'exploitation.

L'Environnement protégé de la version actuelle de Kaspersky Internet Security offre les possibilités suivantes :

- bureau sécurisé (cf. section "Lancement et arrêt du fonctionnement sur le Bureau protégé" à la page 156) ;

- lancement d'une application en particulier en Environnement protégé (à la page 156);
- navigation sur les sites web en mode protégé (à la page 159) ;
- clavier virtuel (à la page 61).

Les objets suspects détectés dans l'environnement protégé sont placés en quarantaine en mode normal. Le type de l'environnement protégé et l'emplacement d'origine des fichiers sont enregistrés dans la liste des menaces détectées et dans le rapport complet de Kaspersky Internet Security. Lors de la restauration des objets de la quarantaine, les objets sont restaurés dans le dossier d'origine. Si le dossier d'origine est introuvable, Kaspersky Internet Security propose de définir l'emplacement pour la restauration de l'objet dans l'environnement où la procédure de restauration a été lancée.

L'Environnement protégé n'est pas disponible sur les ordinateurs sous Microsoft Windows XP x64.

Sous Microsoft Windows Vista x64 et Microsoft Windows 7 x64 les fonctions de certaines applications dans l'Environnement protégé sont limitées. Quand une application de ce genre est lancée, un message apparaîtra à l'écran, si les notifications pour l'événement **La fonction de l'application en environnement protégé est limitée** ont été définies. De plus, le Bureau isolé en mode protégé pour l'exécution des applications n'est pas du tout accessible.

### DANS CETTE SECTION



# EXECUTION DES APPLICATIONS EN MODE PROTEGE

Il est conseillé de lancer dans l'Environnement protégé les applications dont vous n'êtes pas sûr, ainsi que les applications de confiance dont les vulnérabilités peuvent être utilisées par des individus malintentionnés pour accéder aux données sur votre ordinateur.

Vous pouvez lancer une application en particulier (cf. section "Lancement d'une application en particulier en Environnement protégé" à la page 156) dans l'Environnement protégé et utiliser le Bureau protégé (cf. section "Lancement et arrêt du fonctionnement sur le Bureau protégé" à la page 156).

Le Bureau protégé s'ouvre en mode plein écran et représente la copie du bureau principal avec tous les objets du système de fichiers.

Vous pouvez composer la liste des applications qui seront automatiquement lancées lors du lancement du Bureau protégé.

Par défaut, à l'arrêt de l'exécution des applications dans l'Environnement protégé, toutes les modifications introduites lors de l'utilisation sont conservées et seront accessibles à la prochaine exécution. Le cas échéant, vous pouvez purger toutes les modifications (à la page 159) de l'Environnement protégé.

**DANS CETTE SECTION**



## LANCEMENT D'UNE APPLICATION EN PARTICULIER EN ENVIRONNEMENT PROTEGE

Il est possible de lancer des applications particulières en Environnement protégé sans passer par le Bureau isolé en environnement protégé. Le lancement d'une application en particulier dans l'Environnement protégé peut s'opérer via le menu contextuel de Microsoft Windows.

Les applications lancées dans l'environnement protégé sont marquées par le cadre vert autour de la fenêtre de l'application. Aussi, elles possèdent l'indice du lancement protégé dans la liste des applications contrôlées par le Contrôle des Applications (cf. section "Contrôle des Applications" à la page 114).

Une fois que l'application sera arrêtée, la purge automatique de toutes les modifications introduites pendant le fonctionnement de cette application sera exécutée.

*Pour lancer l'application en Environnement protégé depuis le menu contextuel de Microsoft Windows, procédez comme suit :*

Ouvrez le menu contextuel de l'objet sélectionné (un raccourci ou un fichier exécutable) d'un clic droit de la souris, puis choisissez le point **Exécuter en environnement protégé**.

## LANCEMENT ET ARRET DU FONCTIONNEMENT SUR LE BUREAU PROTEGE

Il est possible de lancer le Bureau protégé d'une des méthodes suivantes :

- depuis la fenêtre principale de Kaspersky Internet Security (cf. section "Fenêtre principale de Kaspersky Internet Security" à la page 42) ;
- depuis le menu contextuel de Kaspersky Internet Security (cf. section "Menu contextuel" à la page 41) ;
- à l'aide du Gadget (cf. section "Kaspersky Gadget" à la page 47).

Il est possible de terminer l'utilisation du Bureau protégé via le menu **Démarrer** du système d'exploitation, depuis le volet contextuel (cf. section "Utilisation du volet contextuel" à la page 157), ainsi qu'à l'aide de la combinaison de touches **CTRL+ALT+SHIFT+K**.

*Pour lancer le Bureau protégé depuis la fenêtre principale de Kaspersky Internet Security, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et sélectionnez la rubrique **Environnement protégé**.
2. Dans la partie droite de la fenêtre, sélectionnez **Exécution des applications en mode protégé**.

*Pour lancer le Bureau protégé depuis le menu contextuel de Kaspersky Internet Security,*

cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel de l'icône Kaspersky Internet Security dans la zone des notifications et sélectionnez le point **Bureau sécurisé**.

*Pour quitter l'Environnement protégé via le menu Démarrer,*

dans le menu **Démarrer** du système d'exploitation, sélectionnez le point **Exécution des applications en mode protégé - fin de travail**.

*Pour quitter l'Environnement protégé depuis le volet contextuel, procédez comme suit :*

1. Placez le curseur sur la partie supérieure de la fenêtre.
2. Dans le volet contextuel, cliquez sur le bouton  .
3. Dans la fenêtre de sélection de l'action qui s'ouvre, choisissez l'option **Désactiver**.

## PERMUTATION ENTRE LE BUREAU PRINCIPAL ET L'ENVIRONNEMENT PROTEGE

Vous pouvez passer sur le Bureau principal sans arrêter l'Environnement protégé, puis revenir dans l'Environnement protégé. La permutation entre l'Environnement protégé et le Bureau principal peut s'opérer d'une des façons suivantes :

- depuis la fenêtre principale de Kaspersky Internet Security (cf. section "Fenêtre principale de Kaspersky Internet Security" à la page 42) ;
- depuis le menu contextuel de Kaspersky Internet Security (cf. section "Menu contextuel" à la page 41) ;
- depuis le volet contextuel (cf. section "Utilisation du volet contextuel" à la page 157) (disponible uniquement en Environnement protégé) ;
- à l'aide du Gadget (cf. section "Kaspersky Gadget" à la page 47).

*Pour accéder au Bureau principal depuis la fenêtre principale de Kaspersky Internet Security, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et sélectionnez la rubrique **Environnement protégé**.
2. Dans la partie droite de la fenêtre, choisissez l'option **Revenir au Bureau principal**.

*Pour passer au Bureau principal depuis le menu contextuel de Kaspersky Internet Security,*

cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel de l'icône Kaspersky Internet Security dans la zone des notifications et sélectionnez le point **Dans l'environnement principal**.

*Pour passer au Bureau principal via le volet contextuel, procédez comme suit :*

1. Placez le curseur sur la partie supérieure de la fenêtre.
2. Dans le volet contextuel, cliquez sur le bouton  .

## UTILISATION DU VOLET CONTEXTUEL

Le volet contextuel du Bureau protégé permet d'exécuter les actions suivantes :

- Quitter le Bureau protégé (cf. section "Lancement et arrêt du fonctionnement sur le Bureau protégé" à la page 156) ;

- Passer au Bureau principal (cf. section "Permutation entre le Bureau principal et l'Environnement protégé" à la page 157).

*Pour afficher le volet contextuel sur le Bureau protégé,*

placez le curseur sur la partie supérieure de la fenêtre.

*Pour fixer le volet contextuel, procédez comme suit :*

1. Placez le curseur sur la partie supérieure de la fenêtre.
2. Dans le volet contextuel, cliquez sur le bouton  .

## LANCEMENT AUTOMATIQUE DES APPLICATIONS

Vous pouvez composer la liste des applications qui seront automatiquement lancées lors du lancement du Bureau protégé.

La composition du lancement automatique est disponible uniquement lorsque le Bureau protégé est ouvert.

*Pour composer la liste du lancement automatique des applications pour le Bureau protégé, procédez comme suit :*

1. Dans le menu **Démarrer** du système d'exploitation, sélectionnez le point **Applications** → **Lancement automatique** → **Exécution des applications en mode protégé**.
2. Cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel et sélectionnez l'option **Ouvrir**.
3. Dans le dossier qui s'ouvre, copiez les raccourcis des applications à lancer automatiquement lors du lancement du Bureau protégé.

## DOSSIER PARTAGE

Le dossier partagé de l'Environnement protégé sert à échanger les fichiers entre le système d'exploitation principal et l'Environnement protégé. Tous les fichiers enregistrés dans ce dossier depuis l'environnement protégé seront accessibles depuis le Bureau principal.

Le dossier partagé est créé lors de l'installation de l'application. L'emplacement du dossier partagé varie en fonction du système d'exploitation :

- Sous Microsoft Windows XP : c:\Documents and Settings\All Users\Application Data\Kaspersky Lab\SandboxShared ;
- Sous Microsoft Windows Vista et Microsoft Windows 7 : c:\ProgramData\Kaspersky Lab\SandboxShared.

Il est impossible de modifier l'emplacement du dossier partagé.

Il est possible d'ouvrir le dossier partagé de l'environnement protégé selon une des deux méthodes ci-après :

- Depuis la fenêtre principale de l'application (cf. section "Fenêtre principale de Kaspersky Internet Security" à la page 42) ;
- Dans la rubrique Mon ordinateur de l'Assistant Microsoft Windows (le dossier partagé est signalé par l'icône  ).

*Pour ouvrir le dossier partagé depuis la fenêtre principale de Kaspersky Internet Security, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et sélectionnez la rubrique **Environnement protégé**.

2. Dans la partie droite de la fenêtre, à l'aide du lien **Dossier partagé**, dans le groupe **Exécution des applications en mode protégé**, ouvrez le dossier de l'Environnement protégé dans la fenêtre standard Microsoft Windows.

## PURGE DE L'ENVIRONNEMENT PROTEGE POUR LES APPLICATIONS

S'il est nécessaire de supprimer les données enregistrées pendant l'exécution des actions dans l'Environnement protégé et de restaurer les paramètres modifiés, vous pouvez purger l'Environnement protégé.

La purge est réalisée depuis la fenêtre principale de Kaspersky Internet Security sur le Bureau principal et uniquement quand l'exécution des applications en mode protégé est terminée.

Avant de réaliser cette opération, assurez-vous que toutes les informations dont vous pourriez avoir besoin ultérieurement se trouvent dans le dossier partagé de l'environnement protégé. Dans le cas contraire, les données seront supprimées et il sera impossible de les rétablir.

*Pour purger les données de l'environnement protégé, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et choisissez la rubrique **Exécution en Environnement Protégé**.

2. Dans la partie droite de la fenêtre, cliquez sur le lien **Purger**, dans le groupe **Exécution des applications en mode protégé**.

# NAVIGATION SUR LES SITES WEB EN MODE PROTEGE

Tout d'abord, le navigateur protégé est conçu pour accéder aux systèmes d'opérations bancaires en ligne et aux autres sites Web fonctionnant avec des données confidentielles.

Vous pouvez activer le contrôle de l'accès aux services de transactions bancaires en ligne (cf. section "Contrôle des requêtes adressées aux services de transactions bancaires en ligne" à la page 106) pour l'identification automatique des sites de banques et composer votre propre liste de sites pour lesquels vous serez invité à utiliser la navigation dans l'Environnement protégé pour les consulter. De plus, vous pouvez lancer la navigation sur les sites Web en mode protégé manuellement (cf. section "Lancement de la navigation sur les sites Web en mode protégé" à la page 160).

Dans la navigation sur les sites Web en mode protégé, toutes les modifications (fichiers cookies enregistrés, journal de sites Web visités, etc.) restent dans l'Environnement protégé et ne touchent pas le système d'exploitation et par conséquent, elles ne peuvent pas être utilisées par des individus malintentionnés. Le cas échéant, vous pouvez purger toutes les modifications (cf. section "Purge du navigateur après la navigation sur les sites Web en mode protégé" à la page 160) du navigateur protégé et retourner aux paramètres d'origine.

De plus, pendant l'utilisation des navigateurs Microsoft Internet Explorer, Mozilla Firefox et Google Chrome, Kaspersky Internet Security peut identifier automatiquement les tentatives d'accès à des sites inconnus ou potentiellement dangereux et proposer la navigation en mode protégé afin de mettre le système d'exploitation à l'abri des risques liés à la visite d'un site inconnu.

Pour pouvoir définir automatiquement les sites inconnus, la Navigation sécurisée (à la page 106) de l'Antivirus Internet doit être activée.

### DANS CETTE SECTION

### LANCEMENT DE LA NAVIGATION SUR LES SITES WEB EN MODE PROTEGE

Lors du lancement de la navigation sur les sites Web en mode protégé, le navigateur installé par défaut s'ouvre en mode protégé (uniquement pour Microsoft Internet Explorer, Mozilla Firefox et Google Chrome, dans les autres cas, c'est le navigateur Microsoft Internet Explorer qui est lancé pour la navigation sur les sites Web en mode protégé.

La fenêtre du navigateur qui fonctionne en mode protégé est entourée d'un cadre vert.

*Pour lancer la navigation sur les sites Web en mode protégé depuis la fenêtre principale de Kaspersky Internet Security, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et sélectionnez la rubrique **Environnement Protégé**.
2. Dans la partie droite de la fenêtre, sélectionnez **Navigation sur les sites web en mode protégé**.

### PURGE DU NAVIGATEUR APRES LA NAVIGATION SUR LES SITES WEB EN MODE PROTEGE

S'il faut supprimer les données enregistrées pendant la navigation sur les sites en mode sécurisé, il est possible purger le navigateur protégé.

*Pour purger les données du navigateur protégé, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et choisissez la rubrique **Exécution en Environnement Protégé**.
2. Dans la partie droite de la fenêtre, cliquez sur le lien **Purger** dans le groupe **Navigation sur les sites web en mode protégé**.

## CONTROLE PARENTAL

Le *Contrôle Parental* permet de contrôler les actions de différents utilisateurs sur l'ordinateur et sur le réseau. La notion de contrôle inclut la possibilité de limiter l'accès aux ressources et aux applications et de consulter des rapports sur les actions des utilisateurs.

De nos jours, de plus en plus d'enfants et d'adolescents utilisent un ordinateur et Internet. Il faut parvenir à garantir la sécurité car l'utilisation d'Internet et les communications via ce réseau sont liées à toute une série de menaces. Voici quelques-unes des menaces les répandues :

- La visite de sites Internet dont le contenu peut provoquer une perte de temps (chats, jeux) ou d'argent (magasins en ligne, sites d'enchères) ;
- L'accès à des sites Web réservés aux adultes (contenu pornographique, extrémiste, contenu extrême faisant l'apologie des armes, de la drogue, de la violence, etc.) ;
- Le téléchargement de fichiers infectés par des programmes malveillants ;
- Une trop longue utilisation de l'ordinateur, ce qui pourrait nuire à la santé ;
- Les contacts avec des inconnus qui, en se faisant passer pour des amis, peuvent obtenir des informations personnelles de l'utilisateur (nom véridique, adresse, heure à laquelle il n'y a personne à la maison).

Le Contrôle Parental permet de diminuer les risques liés à l'utilisation de l'ordinateur et d'Internet. Pour ce faire, les fonctions suivantes du module sont utilisées :

- Restriction de l'utilisation de l'ordinateur et d'Internet dans le temps ;

- Composition de listes d'applications dont l'exécution est autorisée ou interdite et restriction temporaire sur l'exécution d'applications autorisées ;
- Composition de listes de sites dont la visite est autorisée ou interdite et sélection de catégories de contenu ne pouvant être consulté ;
- Activation du mode de recherche sécurisée à l'aide des moteurs de recherche (dans ce cas, les liens de sites au contenu douteux n'apparaissent pas dans les résultats de la recherche) ;
- Restriction du téléchargement de fichiers depuis Internet ;
- Composition de listes de contacts avec lesquels les communications sont autorisées ou interdites dans les clients de messagerie instantanée ou dans les réseaux sociaux ;
- Consultation du texte des communications via les clients de messagerie et dans les réseaux sociaux ;
- Interdiction du transfert de certaines données personnelles ;
- Recherche de mots clés définis dans les communications.

Toutes les restrictions sont activées séparément, ce qui permet une administration flexible du Contrôle Parental pour divers utilisateurs. Des rapports sont rédigés pour chaque compte utilisateur. Ces rapports reprennent les événements des catégories contrôlées pour une période donnée.

L'administration du composant requiert une autorisation : il faut saisir le nom d'utilisateur et le mot de passe d'administrateur. Si vous n'avez pas encore défini un mot de passe pour l'administration de Kaspersky Internet Security, vous pourrez le faire maintenant.

### DANS CETTE SECTION



# CONFIGURATION DU CONTROLE PARENTAL DE L'UTILISATEUR

Vous pouvez activer et configurer le Contrôle Parental pour chaque compte utilisateur de manière individuelle et définir différentes restrictions pour différents utilisateurs, par exemple en fonction de l'âge. Vous pouvez désactiver le Contrôle Parental pour les utilisateurs dont les actions ne doivent pas être contrôlées.

### DANS CETTE SECTION



## ACTIVATION ET DESACTIVATION DU CONTROLE DE L'UTILISATEUR

Vous pouvez activer ou désactiver le Contrôle Parental de manière individuelle pour chaque compte utilisateur. Par exemple, les actions d'un utilisateur adulte doté d'un compte d'administrateur n'ont pas besoin d'être contrôlées. Vous pouvez désactiver le Contrôle Parental pour un tel utilisateur. Pour les autres utilisateurs dont les actions doivent être contrôlées, il faut activer le Contrôle Parental, puis le configurer, par exemple en chargeant des paramètres de configuration standard depuis un modèle.

Les méthodes suivantes s'offrent à vous pour activer ou désactiver le Contrôle Parental pour chaque compte utilisateur :

- Au départ de la fenêtre principale de l'application ;
- Au départ de la fenêtre **Contrôle Parental** ;
- Au départ de la fenêtre de configuration du Contrôle Parental ;

Vous pouvez activer ou désactiver le Contrôle Parental pour le compte utilisateur en cours depuis le menu contextuel de l'icône de l'application.

*Pour activer ou désactiver le Contrôle Parental pour un compte utilisateur depuis la fenêtre principale, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et dans la partie gauche de la fenêtre, sélectionnez la rubrique **Contrôle Parental**.

2. Dans la partie droite de la fenêtre, dans le groupe avec le compte utilisateur, cliquez sur le bouton  s'il faut activer le Contrôle Parental pour le compte utilisateur. Si le Contrôle Parental doit être désactivé, cliquez sur l'icône  .

- *Pour activer ou désactiver le Contrôle Parental pour un compte utilisateur depuis la fenêtre du Contrôle Parental, procédez comme suit :*

  1. Ouvrez la fenêtre principale de l'application et dans la partie gauche de la fenêtre, sélectionnez la rubrique **Contrôle Parental**.

  2. Dans la partie droite de la fenêtre, cliquez sur le groupe avec le compte utilisateur pour lequel il faut activer ou désactiver le Contrôle Parental.

     La fenêtre **Contrôle Parental** s'ouvre.

  3. Sélectionnez l'onglet **Configuration**, puis dans la partie gauche de la fenêtre, sélectionnez la section **Paramètres du compte utilisateur**.

  4. Dans la partie droite de la fenêtre, cochez la case **Activer le contrôle de l'utilisateur**, s'il faut activer le Contrôle Parental pour le compte utilisateur. Décochez cette case s'il faut désactiver le Contrôle Parental pour ce compte utilisateur.

  5. Cliquez sur le bouton **Appliquer** afin d'enregistrer les modifications introduites.

- *Pour activer ou désactiver le Contrôle Parental pour un compte utilisateur depuis la fenêtre de configuration de l'application, procédez comme suit :*

  1. Ouvrez la fenêtre de configuration de l'application.

  2. Dans la partie gauche de la fenêtre, sélectionnez la section **Paramètres avancés**, sous-section **Contrôle Parental**.

  3. Dans la partie droite de la fenêtre, sélectionnez le compte utilisateur pour lequel il faut activer ou désactiver le Contrôle Parental.

  4. Au-dessus de la liste des utilisateurs, cliquez sur le bouton **Contrôler**, s'il faut activer le Contrôle Parental pour le compte utilisateur. S'il faut désactiver le Contrôle Parental pour le compte utilisateur, cliquez sur le bouton **Désactiver**.

- *Pour activer ou désactiver le Contrôle Parental pour le compte utilisateur en cours depuis le menu contextuel de l'icône de l'application, procédez comme suit :*

  1. Cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel de l'icône de l'application (cf. section "Menu contextuel" à la page 41).

  2. Choisissez l'option **Activer Contrôle Parental** dans le menu s'il faut activer le contrôle pour le compte utilisateur en cours. Choisissez l'option **Désactiver Contrôle Parental** s'il faut désactiver le contrôle pour le compte utilisateur en cours.

## EXPORTATION ET IMPORTATION DES PARAMETRES DU CONTROLE PARENTAL

Si vous avez configuré les paramètres du Contrôle Parental pour un compte utilisateur, vous pouvez les enregistrer dans un fichier distinct (les *exporter*). Plus tard, vous pourrez charger les paramètres de ce fichier pour réaliser une configuration rapide (les *importer*). De plus, vous pouvez appliquer les paramètres de contrôle d'un autre compte ou utiliser un modèle de configuration (ensemble préconfiguré de règles pour divers types d'utilisateurs en fonction de leur âge, de leur expérience et d'autres caractéristiques).

Une fois que l'ensemble de paramètres a été appliqué, vous pouvez en modifier les valeurs. Cela n'aura aucune influence sur les valeurs dans le fichier d'où vous avez importé les paramètres.

- *Pour enregistrer les paramètres de contrôle dans un fichier, procédez comme suit :*

  1. Ouvrez la fenêtre principale de l'application et dans la partie gauche de la fenêtre, sélectionnez la rubrique **Contrôle Parental**.

2. Dans la partie droite de la fenêtre, cliquez sur le groupe contenant le compte utilisateur dont les paramètres de contrôle doivent être enregistrés.

3. Dans la partie gauche de la fenêtre qui s'ouvre, sélectionnez la rubrique **Paramètres du compte utilisateur**.

4. Cliquez sur le bouton **Enregistrer** dans la partie inférieure de la fenêtre et enregistrez le fichier de configuration.

*Pour charger les paramètres de contrôle depuis un fichier, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et dans la partie gauche de la fenêtre, sélectionnez la rubrique **Contrôle Parental**.

2. Dans la partie droite de la fenêtre, cliquez sur le groupe contenant le compte utilisateur pour lequel il faut importer les paramètres de contrôle.

3. Dans la partie gauche de la fenêtre qui s'ouvre, sélectionnez la rubrique **Paramètres du compte utilisateur**.

4. Cliquez sur le bouton **Télécharger** dans la partie inférieure de la fenêtre.

5. Dans la fenêtre **Chargement des paramètres du contrôle** qui s'ouvre, choisissez l'option **Fichier de configuration** et désignez l'emplacement du fichier.

*Pour appliquer les paramètres d'un autre compte utilisateur, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et dans la partie gauche de la fenêtre, sélectionnez la rubrique **Contrôle Parental**.

2. Dans la partie droite de la fenêtre, cliquez sur le groupe contenant le compte utilisateur pour lequel il faut importer les paramètres de contrôle.

3. Dans la partie gauche de la fenêtre qui s'ouvre, sélectionnez la rubrique **Paramètres du compte utilisateur**.

4. Cliquez sur le bouton **Télécharger** dans la partie inférieure de la fenêtre.

5. Dans la fenêtre **Chargement des paramètres du contrôle** qui s'ouvre, choisissez l'option **Autre utilisateur** et désignez le compte utilisateur dont les paramètres doivent être utilisés.

*Pour utiliser un modèle de configuration, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et dans la partie gauche de la fenêtre, sélectionnez la rubrique **Contrôle Parental**.

2. Dans la partie droite de la fenêtre, cliquez sur le groupe contenant le compte utilisateur,

3. Dans la partie gauche de la fenêtre qui s'ouvre, sélectionnez la rubrique **Paramètres du compte utilisateur**.

4. Cliquez sur le bouton **Télécharger** dans la partie inférieure de la fenêtre.

5. Dans la fenêtre **Chargement des paramètres du contrôle** qui s'ouvre, sélectionnez l'option **Modèle** et désignez le modèle dont les paramètres doivent être utilisés.

## REPRESENTATION DU COMPTE UTILISATEUR DANS KASPERSKY INTERNET SECURITY

Vous pouvez sélectionner le pseudonyme et l'image utilisés pour représenter le compte utilisateur dans Kaspersky Internet Security.

*Pour configurer le pseudonyme et la photo associée au compte, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et dans la partie gauche de la fenêtre, sélectionnez la rubrique **Contrôle Parental**.

2. Dans la partie droite de la fenêtre, cliquez sur le groupe contenant le compte utilisateur dont vous souhaitez configurer l'illustration.

3. Dans la partie gauche de la fenêtre qui s'ouvre, sélectionnez la rubrique **Paramètres du compte utilisateur**.

4. Saisissez le pseudonyme de l'utilisateur dans le champ **Pseudonyme**.

5. Sélectionnez l'image pour le compte utilisateur.

6. Cliquez sur le bouton **Appliquer** afin d'enregistrer les modifications introduites.

## DUREE D'UTILISATION DE L'ORDINATEUR

Vous pouvez configurer l'horaire d'accès à l'ordinateur (jours de la semaine et heures de la journée) ainsi que limiter la durée globale d'utilisation de l'ordinateur par jour.

*Pour limiter l'utilisation de l'ordinateur dans le temps, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et dans la partie gauche de la fenêtre, sélectionnez la rubrique **Contrôle Parental**.

2. Dans la partie droite de la fenêtre, cliquez sur le groupe contenant le compte utilisateur pour lequel il faut définir des restrictions.

3. Dans la partie gauche de la fenêtre, sélectionnez la section **Utilisation de l'ordinateur**.

4. Dans la partie droite de la fenêtre, cochez la case **Activer le contrôle**.

5. Définissez les limitations dans le temps pour l'utilisation de l'ordinateur.

6. Cliquez sur le bouton **Appliquer** afin d'enregistrer les modifications introduites.

## LANCEMENT DES APPLICATIONS

Vous pouvez autoriser ou interdire le lancement d'applications en particulier ainsi que limiter l'exécution des applications autorisées dans le temps.

*Pour restreindre le lancement des applications, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et dans la partie gauche de la fenêtre, sélectionnez la rubrique **Contrôle Parental**.

2. Dans la partie droite de la fenêtre, cliquez sur le groupe contenant le compte utilisateur pour lequel il faut définir des restrictions.

3. Dans la partie gauche de la fenêtre sélectionnez la section **Lancement des applications**.

4. Dans la partie droite de la fenêtre, cochez la case **Activer le contrôle**.

5. Composez la liste des applications dont l'exécution est autorisée ou interdite et définissez l'horaire d'utilisation des applications autorisées.

6. Cliquez sur le bouton **Appliquer** afin d'enregistrer les modifications introduites.

## DUREE D'UTILISATION D'INTERNET

Vous pouvez limiter le temps que peut passer un utilisateur sur Internet. Pour ce faire, il faut configurer un horaire d'accès à Internet (jours de la semaine et heures auxquelles l'accès sera autorisé ou interdit) ainsi que limiter la durée totale d'utilisation d'Internet par jour.

*Pour limiter l'utilisation d'Internet dans le temps, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et dans la partie gauche de la fenêtre, sélectionnez la rubrique **Contrôle Parental**.
2. Dans la partie droite de la fenêtre, cliquez sur le groupe contenant le compte utilisateur pour lequel il faut définir des restrictions.
3. Dans la partie gauche de la fenêtre, sélectionnez la section **Utilisation d'Internet**.
4. Dans la partie droite de la fenêtre, cochez la case **Activer le contrôle**.
5. Définissez les limitations dans le temps pour l'utilisation d'Internet.
6. Cliquez sur le bouton **Appliquer** afin d'enregistrer les modifications introduites.

## CONSULTATION DE SITES

Vous pouvez limiter l'accès à certains sites web en fonction de leur contenu. Pour ce faire, il faut sélectionner les catégories de sites web dont l'accès doit être interdit et le cas échéant, formez la liste des exclusions.

Vous pouvez également activer le *mode de recherche sécurisée* qui sera utilisé pendant l'utilisation des moteurs de recherche. Certains moteurs de recherche veulent protéger les utilisateurs contre des sites au contenu inacceptable. Pour ce faire, les mots clés et les expressions, les adresses et les catégories de ressources sont analysées lors de l'indexation des sites Web. Lorsque le mode de recherche sécurisée est activé, tous les sites web appartenant aux catégories indésirables (pornographie, apologie des drogues et de la violence, autre contenu pour adultes) seront exclus des résultats de la recherche.

Lee Contrôle Parental permet d'activer le mode de Recherche sécurisée simultanément pour les moteurs de recherche suivants :

- Google ;
- Bing.com.

*Pour limiter l'accès aux sites Web, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et dans la partie gauche de la fenêtre, sélectionnez la rubrique **Contrôle Parental**.
2. Dans la partie droite de la fenêtre, cliquez sur le groupe contenant le compte utilisateur pour lequel il faut définir des restrictions.
3. Dans la partie gauche de la fenêtre qui s'ouvre, sélectionnez la rubrique **Consultation de sites**.
4. Dans la partie droite de la fenêtre, cochez la case **Activer le contrôle**.
5. Sélectionnez les catégories de sites auxquels l'utilisateur ne pourra pas accéder.
6. S'il faut, à titre d'exception, autoriser l'accès à certains sites qui appartiennent à la catégorie des sites à bloquer ou interdire l'accès à des sites qui ne figurent pas dans la catégorie des sites à bloquer, ajoutez-les à la liste des exclusions. Pour ce faire, ouvrez la fenêtre **Interdiction de sites web: exclusion** via le bouton **Exclusions**.
7. Cochez la case **Activer le mode de recherche protégée** afin d'activer le mode de recherche sécurisée.
8. Cliquez sur le bouton **Appliquer** afin d'enregistrer les modifications introduites.

## TELECHARGEMENT

Vous pouvez définir les types de fichiers que l'utilisateur pourra télécharger.

*Pour restreindre le téléchargement de fichiers depuis Internet, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et dans la partie gauche de la fenêtre, sélectionnez la rubrique **Contrôle Parental**.
2. Dans la partie droite de la fenêtre, cliquez sur le groupe contenant le compte utilisateur pour lequel il faut définir des restrictions.
3. Dans la partie gauche de la fenêtre sélectionnez la section **Téléchargement**.
4. Dans la partie droite de la fenêtre, cochez la case **Activer le contrôle**.
5. Sélectionnez la catégorie de fichiers dont le téléchargement sera autorisé.
6. Cliquez sur le bouton **Appliquer** afin d'enregistrer les modifications introduites.

## COMMUNICATION A L'AIDE DE CLIENTS DE MESSAGERIE INSTANTANEE

Le contrôle de la communication à l'aide de clients de messagerie instantanée désigne le contrôle des contacts avec lesquels les communications sont autorisées, le blocage des communications avec les contacts interdits et le contrôle du contenu des messages. Vous pouvez créer une liste de contacts autorisés ou interdits, définir des mots clés dont la présence dans les messages sera vérifiée et désigner les données personnelles dont le transfert sera interdit.

Si l'échange de messages instantanés avec un contact est interdit, tous les messages envoyés à ce contact ou par celui-ci seront bloqués. Les informations relatives aux messages bloqués, ainsi que la présence de mots clés dans les messages, sont consignées dans un rapport. Le rapport reprend également le texte des messages échangés avec le contact.

Le contrôle de la correspondance possède les limites suivantes :

- Si le client de messagerie instantanée a été lancé avant l'activation du Contrôle Parental, aucun contrôle de la correspondance n'aura lieu tant que le client de messagerie n'aura pas été redémarré.
- Il n'y aura pas de contrôle de la correspondance en cas d'utilisation d'un proxy HTTP.

La version actuelle du Contrôle Parental prend en charge le contrôle des échanges via les clients de messagerie suivants :

- ICQ ;
- QIP ;
- Windows Live Messenger (MSN) ;
- Yahoo Messenger ;
- GoogleTalk ;
- mIRC ;
- Mail.Ru Agent ;
- Psi ;
- Miranda ;
- AIM ;
- Digsby ;
- Pidgin ;

- Qnext ;
- SIM ;
- Trilian ;
- Xchat ;
- Instantbird ;
- RnQ ;
- MSN ;
- Jabber.

Certains clients de messagerie instantanée, par exemple, Yahoo! Messenger et Google Talk utilisent une connexion sécurisée. Pour analyser le trafic de ces applications, il faut activer l'analyse des connexions cryptées (cf. page 130).

*Pour limiter le nombre de contacts avec lesquels l'utilisateur pourra communiquer en utilisant un client de messagerie instantanée, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et dans la partie gauche de la fenêtre, sélectionnez la rubrique **Contrôle Parental**.
2. Dans la partie droite de la fenêtre, cliquez sur le groupe contenant le compte utilisateur pour lequel il faut définir des restrictions.
3. Dans la partie gauche de la fenêtre, sélectionnez la section **Messageries instantanées**.
4. Dans la partie droite de la fenêtre, cochez la case **Activer le contrôle**.
5. Composez la liste des contacts autorisés ou interdits.
6. Indiquez l'action par défaut pour les contacts qui ne figurent pas dans la liste : s'il faut interdire les communications avec ces contacts, cochez la case **Interdire les conversations avec d'autres contacts**. Décochez la case pour autoriser les communications avec les contacts qui ne figurent pas dans la liste des contacts.
7. Cliquez sur le bouton **Appliquer** afin d'enregistrer les modifications introduites.

## COMMUNICATIONS DANS LES RESEAUX SOCIAUX

Le contrôle de la communication dans les réseaux sociaux désigne le contrôle des contacts avec lesquels les communications sont autorisées, le blocage des communications avec les contacts interdits et le contrôle du contenu des messages. Vous pouvez créer une liste de contacts autorisés ou interdits, définir des mots clés dont la présence dans les messages sera vérifiée et désigner les données personnelles dont le transfert sera interdit.

Si l'échange de messages instantanés avec un contact est interdit, tous les messages envoyés à ce contact ou par celui-ci seront bloqués. Les informations relatives aux messages bloqués, ainsi que la présence de mots clés dans les messages, sont consignées dans un rapport. Le rapport reprend également le texte des messages échangés avec le contact.

*Pour limiter le nombre de contacts avec lesquels l'utilisateur pourra communiquer dans les réseaux sociaux, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et dans la partie gauche de la fenêtre, sélectionnez la rubrique **Contrôle Parental**.
2. Dans la partie droite de la fenêtre, cliquez sur le groupe contenant le compte utilisateur pour lequel il faut définir des restrictions.

3. Dans la partie gauche de la fenêtre sélectionnez la section **Réseaux sociaux**.

4. Dans la partie droite de la fenêtre, cochez la case **Activer le contrôle**.

5. Indiquez l'action par défaut pour les contacts qui ne figurent pas dans la liste des contrôlés : s'il faut interdire les communications avec ces contacts, cochez la case **Interdire les conversations avec d'autres contacts**. Décochez la case pour autoriser les communications avec les contacts qui ne figurent pas dans la liste des contacts à contrôler.

6. Sélectionnez l'onglet **Rapports**.

7. Dans la partie gauche de la fenêtre, sélectionnez la section **Réseaux sociaux**.

   La partie droite de la fenêtre reprend la liste des contacts qui ont envoyé un message ou auxquels un message a été envoyé.

8. Indiquez l'action (autoriser ou interdire la correspondance) pour les contacts sélectionnés.

   Les contacts seront ajoutés automatiquement à la liste des contacts à contrôler. Cette liste est consultable sous l'onglet **Configuration**, dans la section **Réseaux sociaux**.

9. Cliquez sur le bouton **Appliquer** afin d'enregistrer les modifications introduites.

## TRANSFERT D'INFORMATIONS CONFIDENTIELLES

Vous pouvez interdire le transfert de données contenant des informations personnelles via les clients de messagerie instantanée, les réseaux sociaux et lors de l'envoi des données sur des sites Web. Pour ce faire, il faut composer une liste d'entrées contenant des données confidentielles (par exemple, adresse du domicile, téléphone).

Les tentatives de transfert des données de la liste sont bloquées et les informations relatives aux messages bloqués sont consignées dans le rapport.

*Pour bloquer le transfert des données personnelles, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et dans la partie gauche de la fenêtre, sélectionnez la rubrique **Contrôle Parental**.

2. Dans la partie droite de la fenêtre, cliquez sur le groupe contenant le compte utilisateur pour lequel il faut définir des restrictions.

3. Dans la partie gauche de la fenêtre, sélectionnez la section **Données personnelles**.

4. Dans la partie droite de la fenêtre, cochez la case **Activer le contrôle**.

5. Composez la liste des données personnelles dont le transfert est interdit.

6. Cliquez sur le bouton **Appliquer** afin d'enregistrer les modifications introduites.

## RECHERCHE DE MOTS CLES

Vous pouvez vérifier si la correspondance de l'utilisateur via les clients de messagerie instantanée, les réseaux sociaux et lors de l'envoi des données sur les sites Web contient des mots ou des expressions déterminés.

La présence de mots clés de la liste dans la correspondance est signalée dans le rapport.

La recherche des mots clés n'est pas possible si le contrôle des communications via les clients de messagerie instantanée ou les réseaux sociaux et le contrôle des visites de sites est désactivé.

*Pour contrôler la présence de mots déterminés dans la correspondance et dans les données envoyées, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et dans la partie gauche de la fenêtre, sélectionnez la rubrique **Contrôle Parental**.
2. Dans la partie droite de la fenêtre, cliquez sur le groupe contenant le compte utilisateur pour lequel il faut définir des restrictions.
3. Dans la partie gauche de la fenêtre, sélectionnez la section **Mots clés**.
4. Dans la partie droite de la fenêtre, cochez la case **Activer le contrôle**.
5. Composez la liste des mots clés contrôlés dans la correspondance et dans les données envoyées.
6. Cliquez sur le bouton **Appliquer** afin d'enregistrer les modifications introduites.

## CONSULTATION DES RAPPORTS SUR LES ACTIONS DE L'UTILISATEUR

Vous pouvez consulter les rapports sur les actions de chaque utilisateur pour lequel le Contrôle Parental a été configuré ainsi que pour chaque catégorie d'événement contrôlé.

*Pour consulter les rapports sur les actions de l'utilisateur contrôlé, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et dans la partie gauche de la fenêtre, sélectionnez la rubrique **Contrôle Parental**.
2. Dans la partie droite de la fenêtre, cliquez sur le groupe contenant le compte utilisateur dont vous souhaitez consulter le rapport.
3. Sélectionnez l'onglet **Rapports**.
4. Dans la partie gauche de la fenêtre, sélectionnez la rubrique portant le nom de la catégorie d'événements ou de contenu contrôlés, par exemple **Utilisation d'Internet** ou **Données personnelles**.

   La partie droite de la fenêtre affiche le rapport sur les actions contrôlées et le contenu.

# ZONE DE CONFIANCE

La *zone de confiance* est une liste d'objets composée par l'utilisateur. Ces objets seront ignorés par l'application. En d'autres termes, il s'agit d'un ensemble d'exclusions de la protection de Kaspersky Internet Security.

La zone de confiance est composée sur la base de la liste des applications de confiance (cf. section "Composition de la liste des applications de confiance" à la page 171) et des règles d'exclusion (cf. section "Création de règles d'exclusion" à la page 172) en fonction des particularités des objets avec lesquels vous travaillez et des applications installées sur l'ordinateur. Il faudra peut-être inclure des objets dans la zone de confiance si Kaspersky bloque l'accès à un objet ou à une application quelconque alors que vous êtes certain que cet objet ou cette application ne pose absolument aucun danger.

Par exemple, si vous estimez que les objets utilisés par l'application standard Bloc-Notes de Microsoft Windows ne posent aucun danger et ne doivent pas être analysés (vous faites confiance à cette application), ajoutez l'application Bloc-Notes à la liste des applications de confiance afin d'exclure de l'analyse les objets qui utilisent ce processus.

De plus, certaines actions jugées dangereuses peuvent être sans danger dans le cadre du fonctionnement de toute une série de programmes. Ainsi, l'interception des frappes au clavier est une action standard pour les programmes de permutation automatique de la disposition du clavier (par exemple, Punto Switcher). Afin de tenir compte des particularités de tels programmes et de désactiver le contrôle de leur activité, il est conseillé de les ajouter à la liste des applications de confiance.

Quand une application est ajoutée à la liste des applications de confiance, l'activité de fichier et de réseau de celle-ci ne sera pas contrôlée (même les activités suspectes), ni les requêtes adressées à la base de registres système. Le fichier exécutable et le processus de l'application de confiance seront toujours soumis à la recherche de virus. Pour exclure entièrement l'application de l'analyse, il faut recourir aux règles d'exclusion.

Le recours aux exclusions d'applications de confiance de l'analyse permet de résoudre les éventuels problèmes de compatibilité entre Kaspersky Internet Security et d'autres applications (par exemple, le problème de la double analyse du trafic de réseau d'un ordinateur tiers par Kaspersky Internet Security et une autre application antivirus) et d'augmenter les performances de l'ordinateur, ce qui est particulièrement important en cas d'utilisation d'applications de serveur.

Les règles des exclusions de la zone de confiance garantissent à leur tour la sécurité pendant l'utilisation d'application potentiellement dangereuse. Une application potentiellement dangereuse ne possède pas elle-même de fonctionnalité malveillante mais elle peut être exploitée en tant que composant auxiliaire par une application malveillante. Cette catégorie reprend les applications d'administration à distance, les clients IRC, les serveurs FTP, divers utilitaires de suspension ou d'arrêt de processus, les enregistreurs de frappe, les applications d'identification de mots de passe, les numéroteurs automatiques vers des sites web payants, etc. Kaspersky Internet Security peut bloquer de telles applications. Pour éviter le blocage, il est possible de créer des règles d'exclusion de l'analyse pour les applications utilisées.

La *règle d'exclusion* est un ensemble de conditions qui, si elles sont vérifiées, entraîne l'exclusion de l'objet de l'analyse réalisée par Kaspersky Internet Security. Dans tous les autres cas, l'analyse de l'objet en question sera réalisée par tous les composants de la protection conformément aux paramètres de protection définis pour ceux-ci.

Les règles d'exclusion de la zone de confiance peuvent être utilisées par plusieurs composants de la protection (par exemple, l'Antivirus Fichiers, l'Antivirus Courrier, l'Antivirus Internet (cf. section "Antivirus Internet" à la page 99)) ou lors de l'exécution de tâches d'analyse.

### DANS CETTE SECTION



## COMPOSITION DE LA LISTE DES APPLICATIONS DE CONFIANCE

Par défaut Kaspersky Internet Security analyse les objets ouverts, exécutés et enregistrés par n'importe quel processus logiciel et contrôle l'activité de toutes les activités (programme et réseau) qu'il génère. Quand une application est ajoutée à la liste des applications de confiance, Kaspersky Internet Security l'exclut de l'analyse.

*Pour ajouter une application à la liste des applications de confiance, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, choisissez la sous-rubrique **Menaces et exclusions** dans la rubrique **Paramètres avancés**.
3. Dans la rubrique **Exclusions**, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Applications de confiance**, ouvrez le menu de sélection de l'application à l'aide du lien **Ajouter**.
5. Dans le menu déroulant, choisissez l'application dans la liste **Applications** ou sélectionnez l'option **Parcourir** pour indiquer le chemin d'accès au fichier exécutable de l'application souhaitée.
6. Dans la fenêtre **Exclusions pour l'application** qui s'ouvre, cochez les cases ☑ en regard des types d'activité de l'application qu'il ne faut pas analyser.

Vous pouvez modifier l'application de confiance ou la supprimer de la liste à l'aide du lien du même nom dans la partie inférieure de la fenêtre. Pour exclure une application de la liste sans la supprimer, décochez la case ☑ en regard de l'application.

## CREATION DE REGLES D'EXCLUSION

Si vous utilisez des applications que Kaspersky Internet Security considère comme potentiellement dangereuses, vous pouvez configurer des règles d'exclusion pour celles-ci.

*Pour créer une règle d'exclusion, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, choisissez la sous-rubrique **Menaces et exclusions** dans la rubrique **Paramètres avancés**.
3. Dans la rubrique **Exclusions**, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Règles d'exclusion**, cliquez sur le lien **Ajouter**.
5. Dans la fenêtre **Règle d'exclusion** qui s'ouvre, définissez les paramètres de la règle d'exclusion.

# PERFORMANCES ET COMPATIBILITE AVEC D'AUTRES APPLICATIONS

Dans le contexte de Kaspersky Internet Security, les performances désignent le spectre des menaces détectées ainsi que la consommation d'énergie et l'utilisation des ressources de l'ordinateur.

Kaspersky Internet Security permet de configurer avec souplesse le spectre de la protection et de sélectionner diverses catégories de menaces (cf. section "Sélection des catégories de menaces identifiées" à la page 173) que l'application découvrira durant son fonctionnement.

Dans le cadre de l'utilisation d'un ordinateur portable, la consommation en énergie des applications est un élément particulièrement important. En particulier, la recherche d'éventuels virus sur l'ordinateur et la mise à jour des bases de Kaspersky Internet Security requièrent des ressources importantes. Le mode spécial de fonctionnement de Kaspersky Internet Security sur un ordinateur portable (à la page 175) permet de reporter automatiquement l'exécution des tâches d'analyse et de mise à jour programmées en cas d'alimentation via la batterie, ce qui permet d'économiser la charge de cette dernière, et le mode Analyse pendant les temps morts de l'ordinateur (cf. section "Lancement des tâches pendant les temps morts de l'ordinateur" à la page 174) permet de lancer les tâches à forte intensité de ressources quand l'ordinateur n'est pas utilisé.

L'utilisation des ressources de l'ordinateur par Kaspersky Internet Security peut avoir un effet sur les performances des autres applications. Pour résoudre les problèmes liés au fonctionnement simultané en cas d'augmentation de la charge du processeur et des sous-système de disque, Kaspersky Internet Security suspend l'exécution des tâches d'analyse et cède des ressources aux autres applications (cf. page 174) qui tournent sur l'ordinateur.

En Mode Jeux, l'affichage des notifications sur le fonctionnement de Kaspersky Internet Security est automatiquement désactivé quand les autres applications sont lancées en mode plein écran.

La procédure de désinfection avancée en cas d'infection active du système requiert le redémarrage de l'ordinateur, ce qui peut également avoir un effet sur le fonctionnement des autres applications. Le cas échéant, vous pouvez suspendre l'application de la technologie de réparation d'une infection active (cf. page 173) afin d'éviter le redémarrage inopportun de l'ordinateur.

**DANS CETTE SECTION**



# SELECTION DES CATEGORIES DE MENACES IDENTIFIEES

Les menaces qui peuvent être découvertes par Kaspersky Internet Security sont réparties en différentes catégories selon diverses caractéristiques. L'application détecte toujours les virus, les chevaux de Troie et les utilitaires malveillants. Il s'agit des programmes qui peuvent occasionner les dégâts les plus graves. Afin de garantir une protection plus étendue, vous pouvez agrandir la liste des menaces à découvrir en activant la recherche de divers programmes qui présentent un risque potentiel.

*Pour sélectionner les catégories de menaces à identifier, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, choisissez la sous-rubrique **Menaces et exclusions** dans la rubrique **Paramètres avancés**.
3. Dans la partie droite de la fenêtre, dans le groupe **Menaces**, cliquez sur **Configuration**.
4. Dans la fenêtre **Menaces** qui s'ouvre, cochez la case ☑ en regard de la catégorie de menace qu'il faut détecter.

# TECHNOLOGIE DE REPARATION DE L'INFECTION ACTIVE

Les programmes malveillants actuels peuvent s'introduire au niveau le plus bas du système d'exploitation, ce qui vous prive en pratique de la possibilité de les supprimer. En cas de découverte d'une action malveillante dans le système, Kaspersky Internet Security propose la réalisation d'une procédure élargie de réparation qui permet de neutraliser la menace ou de la supprimer de l'ordinateur.

L'ordinateur redémarrera à la fin de la procédure. Une fois que l'ordinateur a redémarré, il est conseillé de lancer une analyse complète (cf. section "Procédure d'exécution d'une analyse complète de l'ordinateur" à la page 59).

*Pour que Kaspersky Internet Security applique la procédure de réparation élargie, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, choisissez la sous-rubrique **Compatibilité** dans la rubrique **Paramètres avancés**.
3. Cochez la case ☑ **Appliquer la technologie de réparation de l'infection active**.

# REPARTITION DES RESSOURCES DE L'ORDINATEUR PENDANT LA RECHERCHE DE VIRUS

Afin de limiter la charge appliquée au processeur central et aux sous-systèmes du disque, vous pouvez reporter les tâches liées à la recherche de virus.

L'exécution des tâches d'analyse augmente la charge du processeur central et des sous-systèmes du disque, ce qui ralentit le fonctionnement d'autres programmes. Lorsqu'une telle situation se présente, Kaspersky Internet Security arrête par défaut l'exécution des tâches d'analyse et libère des ressources pour les applications de l'utilisateur.

Il existe cependant toute une série de programmes qui sont lancés lors de la libération des ressources du processeur et qui travaillent en arrière-plan. Pour que l'analyse ne dépende pas du fonctionnement de tels programmes, il ne faut pas leur céder des ressources.

Remarquez que ce paramètre peut être défini individuellement pour chaque tâche d'analyse. Dans ce cas, la configuration des paramètres pour une tâche particulière a une priorité supérieure.

*Pour que Kaspersky Internet Security reporte l'exécution des tâches d'analyse lorsque le fonctionnement des autres applications ralentit, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, choisissez la sous-rubrique **Compatibilité** dans la rubrique **Paramètres avancés**.
3. Cochez la case **Céder les ressources aux autres applications**.

# LANCEMENT DES TACHES PENDANT LES TEMPS MORTS DE L'ORDINATEUR

Ce mode spécial d'analyse pendant les temps morts de l'ordinateur est prévu pour optimiser la charge des ressources de l'ordinateur. Dans ce mode, toutes les tâches gourmandes en ressources seront réalisées uniquement lorsque vous n'utilisez pas l'ordinateur.

Lors du fonctionnement de l'ordinateur via la batterie, les tâches pendant les temps morts de l'ordinateur ne seront pas exécutées.

Les tâches suivantes peuvent être exécutées pendant les temps morts de l'ordinateur :

- la mise à jour automatique des bases antivirus et des modules d'application ;
- l'analyse de la mémoire système, de la section système et des objets de démarrage.

Les tâches d'analyse pendant les temps morts de l'ordinateur s'activent quand l'ordinateur est verrouillé par l'utilisateur ou si l'économiseur d'écran fonctionne pendant 5 minutes.

L'analyse de l'actualité des bases et des modules d'application est la première étape de l'Analyse en mode veille de l'ordinateur. Si une mise à jour est requise selon les résultats de l'analyse, la tâche de la mise à jour automatique se lance. La date et l'état de la dernière exécution de l'Analyse en mode veille de l'ordinateur est vérifié à la deuxième étape. Si l'Analyse en mode veille de l'ordinateur n'était pas lancée, exécutée 7 jours avant pour la dernière fois ou suspendue, alors la tâche d'analyse de la mémoire système, du registre de système et des objets de démarrage est lancée.

Quand l'utilisateur revient à son ordinateur, l'analyse pendant les temps morts est automatiquement interrompue. L'étape où l'analyse de l'ordinateur a été interrompue est mémorisée et la prochaine analyse reprendra à ce point.

Si l'exécution de tâches pendant les temps morts de l'ordinateur est interrompue pendant le téléchargement des mises à jour, la mise à jour reprendra à zéro la prochaine fois.

*Pour activer l'analyse pendant les temps morts de l'ordinateur, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la rubrique **Analyse de l'ordinateur**, choisissez la sous-rubrique **Paramètres généraux**.
3. Dans la partie droite de la fenêtre, cochez la case **Réaliser l'analyse en mode veille de l'ordinateur**.

## PARAMETRES DE L'APPLICATION EN CAS D'UTILISATION DU MODE PLEIN ECRAN. MODE JEUX

L'utilisation de certaines applications (principalement des jeux) en mode plein écran peut créer des problèmes avec certaines fonctionnalités de Kaspersky Internet Security : par exemple, les fenêtres de notification n'ont pas leur place dans ce mode. Bien souvent, ces applications requièrent également des ressources considérables du système et c'est la raison pour laquelle l'exécution de certaines tâches de Kaspersky Internet Security peut ralentir ces applications.

Pour ne pas devoir désactiver manuellement les notifications ou suspendre les tâches chaque fois que vous utilisez le mode plein écran, Kaspersky Internet Security permet de modifier temporairement les paramètres grâce au mode Jeux. Quand le Mode Jeux est utilisé, les paramètres de tous les composants sont automatiquement modifiés quand l'utilisateur passe en mode plein écran afin de garantir le fonctionnement optimal dans ce mode. Au moment de quitter le mode plein écran, les paramètres de l'application reprennent les valeurs en vigueur au moment de passer en mode plein écran.

*Pour activer le mode jeu, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, sélectionnez la sous-rubrique **Mode jeux** dans la rubrique **Paramètres avancés**.
3. Cochez la case **Utiliser le Mode Jeux** et dans le groupe **Paramètres du profil** en dessous, définissez les paramètres indispensables de l'exécution du Mode Jeux.

## ÉCONOMIE D'ENERGIE EN CAS D'ALIMENTATION VIA LA BATTERIE

Afin d'économiser les batteries des ordinateurs portables, vous pouvez reporter l'exécution des tâches d'analyse antivirus et de mises à jour programmées. Le cas échéant, il est possible d'actualiser Kaspersky Internet Security ou de lancer la recherche de virus manuellement.

*Pour activer le mode d'économie d'énergie en cas d'alimentation via la batterie, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, choisissez la sous-rubrique **Économie d'énergie** dans la rubrique **Paramètres avancés**.
3. Dans la partie droite de la fenêtre, cochez la case **Ne pas lancer l'analyse programmée en cas d'alimentation via la batterie**.

# AUTODEFENSE DE KASPERSKY INTERNET SECURITY

Dans la mesure où Kaspersky Internet Security protège les ordinateurs contre les programmes malveillants, ceux-ci tentent, une fois qu'ils se sont infiltrés dans l'ordinateur, de bloquer le fonctionnement de Kaspersky Internet Security, voire de supprimer l'application de l'ordinateur.

La stabilité du système de protection de l'ordinateur est garantie par des mécanismes d'autodéfense et de protection contre l'interaction à distance intégrés à Kaspersky Internet Security.

L'autodéfense de Kaspersky Internet Security empêche la modification et la suppression des fichiers de l'application sur le disque, des processus dans la mémoire et des enregistrements dans la base de registres. La protection contre l'interaction à distance permet de bloquer toutes les tentatives d'administration à distance des services de l'application.

Sous les systèmes d'exploitation 64 bits et sous Microsoft Windows Vista, seule l'administration du mécanisme d'autodéfense de Kaspersky Internet Security contre la modification et la suppression de ses propres fichiers sur le disque ou contre la modification ou la suppression des clés dans la base de registres est accessible.

### DANS CETTE SECTION



## ACTIVATION/DESACTIVATION DE L'AUTODEFENSE

L'autodéfense de Kaspersky Internet Security est activée par défaut. Le cas échéant, vous pouvez désactiver l'autodéfense.

*Pour désactiver l'autodéfense de Kaspersky Internet Security, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, choisissez la sous-rubrique **Autodéfense** dans la rubrique **Paramètres avancés**.
3. Dans la partie droite de la fenêtre, désélectionnez la case **Activer l'Autodéfense**.

## PROTECTION CONTRE L'ADMINISTRATION EXTERNE

La protection contre l'administration externe est activée par défaut. Le cas échéant, vous pouvez désactiver cette protection.

Il arrive parfois que le recours à la protection contre les interventions à distance entraîne l'impossibilité d'utiliser les programmes d'administration à distance (par exemple, RemoteAdmin). Pour garantir leur fonctionnement, il faut ajouter ces applications à la liste des applications de confiance (cf. section "Composition de la liste des applications de confiance" à la page 171) et activer le paramètre **Ne pas surveiller l'activité de l'application**.

*Pour désactiver la protection contre l'administration externe, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, choisissez la sous-rubrique **Autodéfense** dans la rubrique **Paramètres avancés**.

3. Dans le groupe **Administration externe**, cochez la case ☑ **Interdire l'administration externe du service système**.

# QUARANTAINE ET SAUVEGARDE

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 par des virus ou leur modification.

L'objet potentiellement infecté peut-être identifié et mis en quarantaine par l'Antivirus Fichiers, l'Antivirus Courrier, lors de l'analyse antivirus ou par la Défense Proactive.

Les objets sont placés en quarantaine dans les cas suivants :

- Le code de l'objet est semblable à celui d'une menace connue mais il a été partiellement modifié ou sa structure évoque celle d'un programme malveillant, mais ne figure pas dans la base. Dans ce cas, les objets sont placés en quarantaine suite à l'analyse heuristique pendant l'intervention de l'Antivirus Fichiers et de l'Antivirus Courrier, ainsi que pendant la recherche de virus. Le mécanisme d'analyse heuristique provoque rarement de faux positifs.

- La séquence d'actions réalisée par l'objet est suspecte. Dans ce cas, les objets sont placés en quarantaine suite à l'analyse de leur comportement par la Défense Proactive.

L'objet placé en quarantaine est déplacé et non pas copié : l'objet est supprimé du disque ou du message et il est enregistré dans le répertoire de quarantaine. Les fichiers mis en quarantaine sont convertis dans un format spécial et ne représentent aucun danger.

*Le dossier de sauvegarde* est conçu pour l'enregistrement des copies de sauvegarde des objets infectés impossibles à réparer au moment de leur détection.

Lors de la prochaine mise à jour des bases de l'application, il se peut que Kaspersky Internet Security puisse identifier la menace et la neutraliser. C'est pour cette raison que le logiciel analyse les objets en quarantaine après chaque mise à jour (cf. page 87).

### DANS CETTE SECTION



# CONSERVATION DES OBJETS DE LA QUARANTAINE ET DE LA SAUVEGARDE.

La durée maximale de conservation par défaut des objets est de 30 jours. Les objets sont supprimés à l'issue de cette période. Vous pouvez annuler la restriction sur la durée de conservation ou la modifier.

En outre, vous pouvez indiquer la taille maximale de la quarantaine et de la sauvegarde. Une fois que la taille maximale est atteinte, le contenu de la quarantaine et de la sauvegarde est remplacé par de nouveaux objets. Par défaut, il n'y a pas de limite sur la taille maximale.

➧ *Pour configurer la durée maximale de conservation des objets, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.

2. Dans la partie gauche de la fenêtre, dans la rubrique **Paramètres avancés**, sélectionnez la sous-rubrique **Rapports et stockages**.

3. Dans la partie droite de la fenêtre, dans le groupe **Conservation des objets de la quarantaine et de la sauvegarde**, cochez la case **Supprimer les objets après** et indiquez la durée maximale de conservation des objets en quarantaine.

*Pour configurer la taille maximale de la quarantaine ou de la sauvegarde, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.

2. Dans la partie gauche de la fenêtre, dans la rubrique **Paramètres avancés**, sélectionnez la sous-rubrique **Rapports et stockages**.

3. Dans la partie droite de la fenêtre, dans le groupe **Conservation des objets de la quarantaine et de la sauvegarde**, cochez la case **Taille maximale** et indiquez la taille maximale de la quarantaine et de la sauvegarde.

## MANIPULATION DES OBJETS EN QUARANTAINE

La quarantaine de Kaspersky Internet Security permet d'exécuter les opérations suivantes :

- Mettre en quarantaine les fichiers qui selon vous sont infectés par un virus ;
- Analyser et réparer tous les objets potentiellement infectés de la quarantaine à l'aide de la version actuelle des bases de Kaspersky Internet Security ;
- Restaurer les fichiers dans le dossier indiqué ou dans les dossiers où ils se trouvaient avant d'être placés en quarantaine (par défaut) ;
- Supprimer n'importe quel objet ou groupe d'objets de la quarantaine ;
- Envoyer les objets de la quarantaine à Kaspersky Lab pour étude.

Un objet peut être placé en quarantaine de deux manières :

- Via le lien **Placer en quarantaine** de la fenêtre **Etat de la protection** ;
- Via le menu contextuel de l'objet.

*Pour placer un objet en quarantaine depuis la fenêtre Etat de la protection, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.

2. Cliquez sur le lien **Quarantaine** situé dans la partie supérieure de la fenêtre principale pour ouvrir la fenêtre **Etat de la protection** à l'onglet **Menaces détectées**.

3. Cliquez sur le lien **Placer en quarantaine** situé au-dessus de la liste des menaces.

4. Dans la fenêtre qui s'ouvre, choisissez l'objet qu'il faut placer en quarantaine.

*Pour placer un objet en quarantaine à l'aide du menu contextuel, procédez comme suit :*

1. Ouvrez la fenêtre de l'Assistant de Microsoft Windows et accédez au dossier contenant l'objet à mettre en quarantaine.

2. Cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel de l'objet, puis choisissez l'option **Copier dans la quarantaine**.

*Pour analyser un objet en quarantaine, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.

2. Cliquez sur le lien **Quarantaine** dans la partie supérieure de la fenêtre afin d'ouvrir la fenêtre de la quarantaine.

3. Dans la fenêtre qui s'ouvre, sous l'onglet **Menaces détectées**, sélectionnez l'objet à analyser.

4. Cliquez sur le bouton droit de la souris afin d'ouvrir le menu contextuel pour les objets requis, puis choisissez l'option **Analyser**.

*Pour réparer tous les objets en quarantaine, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.

2. Cliquez sur le lien **Quarantaine** dans la partie supérieure de la fenêtre afin d'ouvrir la fenêtre de la quarantaine.

3. Dans la fenêtre qui s'ouvre, sous l'onglet **Menaces détectées**, cliquez sur le bouton **Réparer tous**.

*Pour restaurer un fichier depuis la quarantaine, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.

2. Cliquez sur le lien **Quarantaine** dans la partie supérieure de la fenêtre afin d'ouvrir la fenêtre de la quarantaine.

3. Dans la fenêtre qui s'ouvre, sous l'onglet **Menaces détectées**, sélectionnez l'objet à restaurer.

4. Cliquez sur le bouton droit de la souris afin d'ouvrir le menu contextuel pour les objets requis, puis choisissez l'option **Restaurer**.

*Pour supprimer un objet de la quarantaine, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.

2. Cliquez sur le lien **Quarantaine** dans la partie supérieure de la fenêtre afin d'ouvrir la fenêtre de la quarantaine.

3. Dans la fenêtre qui s'ouvre, sous l'onglet **Menaces détectées**, sélectionnez l'objet à supprimer.

4. Cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel, puis sélectionnez l'option **Supprimer de la liste**.

*Pour envoyer l'objet en quarantaine à Kaspersky Lab pour étude, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.

2. Cliquez sur le lien **Quarantaine** dans la partie supérieure de la fenêtre afin d'ouvrir la fenêtre de la quarantaine.

3. Dans la fenêtre qui s'ouvre, sous l'onglet **Menaces détectées**, sélectionnez l'objet à envoyer pour examen.

4. Cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel, puis sélectionnez l'option **Envoyer**.

# OUTILS DE PROTECTION COMPLEMENTAIRE

Afin d'exécuter des tâches spécifiques à la protection de l'ordinateur, Kaspersky Internet Security propose une série d'Assistants et d'outils.

- L'Assistant de création de disque de dépannage est prévu pour la création d'un disque de dépannage qui permettra de restaurer le système après une attaque de virus en lançant le système depuis un disque amovible. Le disque de dépannage intervient dans les cas d'infection qui rendent la réparation de l'ordinateur impossible à l'aide des logiciels antivirus ou des outils de réparation.

- L'Assistant de suppression des traces d'activité est prévu pour la recherche et la suppression des traces d'activité de l'utilisateur dans le système ainsi que des paramètres du système d'exploitation qui permettent d'accumuler des données sur l'activité de l'utilisateur.

- L'Assistant de restauration du système permet de supprimer les corruptions et les traces laissées par des objets malveillants dans le système.

- L'Assistant de Configuration du navigateur est prévu pour l'analyse et la configuration des paramètres de Microsoft Internet Explorer dans le but de supprimer les vulnérabilités potentielles.

- La Recherche de Vulnérabilités est prévue pour examiner le système d'exploitation et les applications dans le but d'identifier d'éventuelles vulnérabilités qui pourraient être exploitées par des individus malintentionnés.

Tous les problèmes découverts par les Assistants (sauf l'Assistant de création du disque de dépannage) sont regroupés en fonction du danger qu'ils représentent pour le système. Pour chaque groupe de problèmes, les experts de Kaspersky Lab proposent un ensemble d'actions dont l'exécution permettra de supprimer les vulnérabilités et les points problématiques du système. Il existe trois groupes de problèmes et par conséquent, trois groupes d'actions exécutées.

- *Les actions vivement recommandées* permettent de supprimer les problèmes qui constituent une menace sérieuse pour la sécurité. Il est conseillé d'exécuter dans les plus brefs délais toutes les actions de ce groupe pour supprimer la menace.

- *Les actions recommandées* visent à supprimer les problèmes qui peuvent présenter un danger potentiel. Il est également conseillé d'exécuter les actions de ce groupe pour garantir une protection optimale.

- *Les actions complémentaires* sont prévues pour supprimer les problèmes qui ne présentent actuellement aucun danger mais qui à l'avenir pourraient menacer la sécurité de l'ordinateur. L'exécution de ces actions garantit la protection totale de l'ordinateur mais peut, dans certains cas, entraîner la suppression de certains paramètres définis par l'utilisateur (par exemple, les cookies).

### DANS CETTE SECTION



# SUPPRESSION DES TRACES D'ACTIVITE

Lorsque vous utilisez votre ordinateur, vos activités sont enregistrées dans le système. Les données relatives aux recherches lancées par l'utilisateur et aux sites visités sont conservées, tout comme les données relatives à l'exécution d'applications et à l'ouverture et à l'enregistrement de fichiers, les entrées du journal système Microsoft Windows, les fichiers temporaires et bien d'autres encore.

Toutes ces sources d'informations sur l'activité de l'utilisateur peuvent contenir des données confidentielles (y compris des mots de passe) que les individus malintentionnés pourraient analyser. Bien souvent, l'utilisateur ne possède pas les connaissances suffisantes pour empêcher le vol d'informations depuis ces sources.

Kaspersky Internet Security propose un Assistant de suppression des traces d'activité. Cet Assistant recherche les traces d'activité de l'utilisateur dans le système ainsi que les paramètres du système d'exploitation qui permettent de récolter des informations sur cette activité.

Il ne faut pas oublier que des informations sur l'activité de l'utilisateur dans le système sont accumulées sans cesse. L'exécution du moindre fichier ou l'ouverture de n'importe quel document est enregistrée dans l'historique et le journal de Microsoft Windows enregistre une multitude d'événements qui surviennent dans le système. Ceci veut dire qu'une nouvelle exécution de l'Assistant de suppression des traces d'activité peut découvrir des traces supprimées lors de l'exécution antérieure de l'Assistant. Certains fichiers, par exemple le fichier de rapport de Microsoft Windows, peuvent être utilisés par le système au moment où les traces sont supprimées par l'Assistant. Afin de pouvoir supprimer ces fichiers, l'Assistant propose de redémarrer le système. Toutefois, ces fichiers peuvent être recréés lors du redémarrage, ce qui signifie qu'ils seront à nouveau découverts en tant que trace d'activité.

L'Assistant se compose d'une série de fenêtres (étapes) entre lesquelles vous pouvez naviguer grâce aux boutons **Précédent** et **Suivant**. Pour quitter l'Assistant, cliquez sur le bouton **Terminer**. Pour interrompre l'Assistant à n'importe quelle étape, cliquez sur le bouton **Annuler**.

*Pour lancer l'Assistant de suppression des traces d'activités, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et dans la partie gauche de la fenêtre, sélectionnez la rubrique **Outils**.

2. Dans la partie droite de la fenêtre, cliquez sur le bouton **Suppression des traces d'activité**.

Examinons en détails les étapes de l'Assistant.

### Etape 1. Début de l'utilisation de l'Assistant

Assurez-vous que l'option **Rechercher les Traces d'activité de l'utilisateur** a été sélectionnée, puis appuyez sur le bouton **Suivant** pour lancer l'Assistant.

### Etape 2. Recherche de traces d'activité

L'Assistant recherche les traces d'activité sur votre ordinateur. La recherche peut durer un certain temps. Une fois la recherche terminée, l'Assistant passe automatiquement à l'étape suivante.

### Etape 3. Sélection des actions pour la suppression des traces d'activité

À la fin de la recherche, l'Assistant indique les traces d'activité trouvées et les moyens proposés pour s'en débarrasser. Le rapport sur le fonctionnement de l'Assistant est présenté sous forme de la liste (cf. section "Outils de protection complémentaire" à la page 179).

Pour voir les actions reprises dans le groupe, cliquez sur le signe **+** situé à gauche du nom du groupe.

Pour que l'Assistant réalise une action, cochez la case à gauche du nom de l'action. Toutes les actions recommandées et vivement recommandées sont exécutées par défaut. Si vous ne souhaitez pas exécuter une action quelconque, désélectionnez la case en regard de celle-ci.

Il est vivement déconseillé de décocher les cases sélectionnées par défaut car vous pourriez mettre en danger la sécurité de l'ordinateur.

Une fois que vous aurez sélectionné les actions pour l'Assistant, cliquez sur **Suivant**.

### Etape 4. Suppression des traces d'activité

L'Assistant exécute les actions sélectionnées à l'étape précédente. La suppression des traces d'activité peut durer un certain temps. La suppression de certaines traces d'activité nécessitera peut-être le redémarrage de l'ordinateur. L'Assistant vous préviendra.

Une fois les traces d'activité supprimée, l'Assistant passe automatiquement à l'étape suivante.

### Etape 5. Fin de l'Assistant

Si vous souhaitez que la suppression des traces d'activité soit réalisée automatiquement à l'avenir au moment de quitter Kaspersky Internet Security, cochez la case **Supprimer les traces d'activité à chaque arrêt de Kaspersky Internet Security** à la dernière étape de l'Assistant. Si vous avez l'intention de supprimer vous-même les traces d'activité à l'aide de l'Assistant, sans cochez cette case.

Cliquez sur le bouton **Terminer** pour quitter l'Assistant.

# CONFIGURATION DU NAVIGATEUR

Dans certains cas, le navigateur Microsoft Internet Explorer requiert une analyse et une configuration spéciales des paramètres car certaines valeurs, définies par les utilisateurs ou présentes par défaut peuvent entraîner des problèmes au niveau de la sécurité.

Voici quelques exemples d'objets et de paramètres utilisés par le navigateur et qui constituent une menace potentielle pour la sécurité.

- **Cache de fonctionnement de Microsoft Internet Explorer**. Le cache conserve les données téléchargées depuis Internet, ce qui permet de ne pas les télécharger de nouveaux par la suite. Ceci diminue le temps de téléchargement des pages web et diminue le trafic Internet. Par ailleurs, le cache contient les données confidentielles et offre la possibilité de connaître les ressources visitées par l'utilisateur. Nombreux sont les objets malveillants qui, lors du balayage du disque, balaient également le cache, ce qui signifie que les individus malintentionnés peuvent obtenir, par exemple, les adresses de messagerie des utilisateurs. Pour augmenter la protection, il est recommandé de purger le cache après la fin du fonctionnement du navigateur.

- **Affichage de l'extension pour les fichiers de format connu**. Pour faciliter la modification des noms des fichiers, il est possible de ne pas afficher leurs extensions. Cependant, il est utile par fois pour l'utilisateur de voir l'extension réelle du fichier. Les noms de fichier de nombreux objets malveillants utilisent des combinaisons de caractères qui imitent une extension supplémentaire avant l'extension réelle (par exemple, ceciestunexemple.txt.com). Si l'extension réelle du fichier n'est pas affichée, l'utilisateur voit uniquement la partie du fichier avec l'imitation de l'extension et peut considérer l'objet malveillant comme un objet ne présentant aucun danger. Pour augmenter la protection, il est recommandé d'activer l'affichage des extensions pour les fichiers de formats connus.

- **Liste des sites de confiance**. Pour le fonctionnement correct de certains sites web, il faut les ajouter dans la liste de confiance. Par ailleurs, les objets malveillants peuvent ajouter à cette liste les liens sur les sites web créés par les malfaiteurs.

Il ne faut pas oublier que certaines valeurs des paramètres peuvent entraîner des problèmes d'affichage de certains sites web (par exemple, si ces sites utilisent des éléments ActiveX). Vous pouvez résoudre ce problème en ajoutant ces sites web à la zone de confiance.

L'analyse et la configuration du navigateur sont confiées à l'Assistant de configuration du navigateur. L'Assistant vérifie si les mises à jour les plus récentes du navigateur ont été installées et si les valeurs des paramètres définies ne rendent pas le système vulnérable aux actions des individus malintentionnés. Pour conclure, l'Assistant rédige un rapport qui peut être envoyé à Kaspersky Lab pour analyse.

L'Assistant se compose d'une série de fenêtres (étapes) entre lesquelles vous pouvez naviguer grâce aux boutons **Précédent** et **Suivant**. Pour quitter l'Assistant, cliquez sur le bouton **Terminer**. Pour interrompre l'Assistant à n'importe quelle étape, cliquez sur le bouton **Annuler**.

Avant de lancer le diagnostic, fermez toutes les fenêtres de Microsoft Internet Explorer.

*Pour lancer l'Assistant de configuration du navigateur, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et dans la partie gauche de la fenêtre, sélectionnez la rubrique **Outils**.

2. Dans la partie droite de la fenêtre, cliquez sur le bouton **Configuration du navigateur**.

Examinons en détails les étapes de l'Assistant.

## Etape 1. Début de l'utilisation de l'Assistant

Assurez-vous que l'option **Analyser Microsoft Internet Explorer** a été sélectionnée, puis appuyez sur le bouton **Suivant** pour lancer l'Assistant.

### Etape 2. Analyse des paramètres de Microsoft Internet Explorer

L'Assistant analyse les paramètres du navigateur Microsoft Internet Explorer. La recherche de problèmes dans les paramètres peut prendre un certain temps. Une fois la recherche terminée, l'Assistant passe automatiquement à l'étape suivante.

### Etape 3. Sélection des actions pour la configuration du navigateur

Tous les problèmes identifiés à l'étape antérieure sont regroupés selon le niveau de danger qu'ils présentent pour le système (cf. section "Outils de protection complémentaire" à la page 179).

Pour voir les actions reprises dans le groupe, cliquez sur le signe **+** situé à gauche du nom du groupe.

Pour que l'Assistant réalise une action, cochez la case à gauche du nom de l'action. Toutes les actions recommandées et vivement recommandées sont exécutées par défaut. Si vous ne souhaitez pas exécuter une action quelconque, désélectionnez la case en regard de celle-ci.

Il est vivement déconseillé de décocher les cases sélectionnées par défaut car vous pourriez mettre en danger la sécurité de l'ordinateur.

Une fois que vous aurez sélectionné les actions pour l'Assistant, cliquez sur **Suivant**.

### Etape 4. Configuration du navigateur

L'Assistant exécute les actions sélectionnées à l'étape précédente. La configuration du navigateur peut durer un certain temps. Une fois la configuration terminée, l'Assistant passe automatiquement à l'étape suivante.

### Etape 5. Fin de l'Assistant

Cliquez sur le bouton **Terminer** pour quitter l'Assistant.

## RETOUR A L'ETAT ANTERIEUR AUX MODIFICATIONS INTRODUITES PAR LES ASSISTANTS

Il est possible d'annuler certaines modifications introduites par l'Assistant de suppression des traces d'activité (cf. section "Suppression des traces d'activité" à la page 180), l'Assistant de restauration du système (cf. section "Que faire si vous pensez que votre ordinateur est infecté" à la page 64), l'Assistant de Configuration du navigateur (cf. section "Configuration du navigateur" à la page 182).

*Pour revenir à l'état antérieur aux modifications, lancez l'Assistant correspondant de la manière suivante :*

1. Ouvrez la fenêtre principale de l'application et dans la partie gauche de la fenêtre, sélectionnez la rubrique **Outils**.
2. Dans la partie droite de la fenêtre, cliquez sur un des boutons suivants :
   - **Suppression des traces d'activité** : lancement de l'Assistant de suppression des traces d'activité ;
   - **Restauration du système** : lancement de l'Assistant de restauration du système ;
   - **Configuration du navigateur** : lancement de l'Assistant de configuration du navigateur.

Examinons en détail les étapes des Assistants pour revenir à l'état antérieur aux modifications.

### Etape 1. Début de l'utilisation de l'Assistant

Choisissez l'option **Annuler les modifications**, puis cliquez sur le bouton **Suivant**.

### Etape 2. Recherche des modifications

L'Assistant recherche les modifications qu'il a introduit et qui peuvent être annulées. Une fois la recherche terminée, l'Assistant passe automatiquement à l'étape suivante.

### Etape 3. Sélection des modifications à annuler

Au cours de cette étape, l'Assistant propose un rapport sur les modifications découvertes. Le rapport se présente sous la forme d'une liste reprenant les modifications introduites par l'Assistant et dont les effets peuvent être annulés.

Pour qu'un Assistant annule les effets d'une action exécutée, cochez la case à gauche du nom de l'action.

Une fois que vous aurez sélectionné les actions à annuler, cliquez sur **Suivant**.

### Etape 4. Retour à l'état antérieur aux modifications

L'Assistant revient à l'état antérieur aux modifications sélectionnées à l'étape antérieure. Une fois l'annulation des modifications terminée, l'Assistant passe automatiquement à l'étape suivante.

### Etape 5. Fin de l'Assistant

Cliquez sur le bouton **Terminer** pour quitter l'Assistant.

# RAPPORTS

Les événements survenus pendant le fonctionnement des composants de la protection ou lors de l'exécution des tâches de Kaspersky Internet Security sont consignés dans des rapports. Vous pouvez composer un rapport détaillé pour chaque composant de la protection ou chaque tâche et configurer l'affichage des données (cf. section "Gestion de la représentation des données à l'écran" à la page 185) dans une mise en page pratique. De plus, vous pouvez filtrer les données (cf. section "Filtrage des données" à la page 186) et lancer une recherche (cf. section "Recherche d'événements" à la page 187) sur tous les événements du rapport.

Le cas échéant, vous pouvez enregistrer les données du rapport (cf. section "Enregistrement du rapport dans un fichier" à la page 188) dans un fichier texte. Vous pouvez également purger les rapports (cf. section "Purge des rapports" à la page 188) contenant des données qui ne vous sont plus nécessaires et configurer les paramètres de composition (cf. section "Entrées relatives aux événements non critiques" à la page 189) et de conservation (cf. section "Conservation des rapports" à la page 188) des rapports.

**DANS CETTE SECTION**



# COMPOSITION DU RAPPORT POUR LE COMPOSANT SELECTIONNE

Vous pouvez obtenir un rapport détaillé sur les événements survenus pendant le fonctionnement de chaque composant ou de chaque tâche de Kaspersky Internet Security.

*Pour obtenir un rapport pour le composant ou la tâche, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Cliquez sur le lien **Rapports** dans la partie supérieure de la fenêtre afin d'ouvrir la fenêtre des rapports.
3. Dans la fenêtre qui s'ouvre, sous l'onglet **Rapport**, cliquez sur le bouton **Rapport détaillé**.
4. Dans la partie gauche de la fenêtre **Rapport détaillé** qui s'ouvre, sélectionnez le composant ou la tâche pour lequel vous souhaitez créer un rapport. Si vous choisissez l'option **Protection**, le rapport sera produit pour tous les composants de la protection.

# GESTION DE LA REPRESENTATION DES DONNEES A L'ECRAN

Pour le confort d'utilisation des rapports, vous pouvez gérer la représentation des données à l'écran : regrouper les événements selon divers paramètres, sélectionner la période couverte par le rapport, trier les événements dans chaque colonne ou selon l'importance et masquer des colonnes du tableau.

*Pour définir la période couverte par le rapport, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Cliquez sur le lien **Rapports** dans la partie supérieure de la fenêtre afin d'ouvrir la fenêtre des rapports.
3. Dans la fenêtre qui s'ouvre, sous l'onglet **Rapport**, cliquez sur le bouton **Rapport détaillé**.
4. Dans la partie droite de la fenêtre **Rapport détaillé** qui s'ouvre, dans la liste déroulante **Période**, choisissez la longueur de la période couverte par le rapport.
5. Cliquez sur le bouton  pour sélectionner la période couverte par le rapport souhaitée.

- *Pour regrouper les événements, procédez comme suit :*

  1. Ouvrez la fenêtre principale de l'application.
  2. Cliquez sur le lien **Rapports** dans la partie supérieure de la fenêtre afin d'ouvrir la fenêtre des rapports.
  3. Dans la fenêtre qui s'ouvre, sous l'onglet **Rapport**, cliquez sur le bouton **Rapport détaillé**.
  4. Dans la partie droite de la fenêtre **Rapport détaillé** qui s'ouvre, cliquez sur le bouton **Apparence** et sélectionnez le mode de regroupement dans la liste déroulante.

- *Pour trier les événements selon l'importance, procédez comme suit :*

  1. Ouvrez la fenêtre principale de l'application.
  2. Cliquez sur le lien **Rapports** dans la partie supérieure de la fenêtre afin d'ouvrir la fenêtre des rapports.
  3. Dans la fenêtre qui s'ouvre, sous l'onglet **Rapport**, cliquez sur le bouton **Rapport détaillé**.
  4. Dans la partie droite de la fenêtre **Rapport détaillé** qui s'ouvre, cliquez sur l'icône du type d'événement (  ) afin d'afficher ou de dissimuler les événements de ce type.

- *Pour trier les événements selon la valeur d'une colonne quelconque du tableau, procédez comme suit :*

  1. Ouvrez la fenêtre principale de l'application.
  2. Cliquez sur le lien **Rapports** dans la partie supérieure de la fenêtre afin d'ouvrir la fenêtre des rapports.
  3. Dans la fenêtre qui s'ouvre, sous l'onglet **Rapport**, cliquez sur le bouton **Rapport détaillé**.
  4. Dans la partie droite de la fenêtre **Rapport détaillé** qui s'ouvre, cliquez sur le bouton droit de la souris afin d'ouvrir le menu contextuel de l'en-tête de la colonne requise, puis choisissez l'option **Classer en ordre décroissant** ou **Classer en ordre croissant**.

     Une flèche indiquant l'ordre du classement apparaît dans l'en-tête de la colonne.

- *Pour afficher/dissimuler des colonnes du tableau, procédez comme suit :*

  1. Ouvrez la fenêtre principale de l'application.
  2. Cliquez sur le lien **Rapports** dans la partie supérieure de la fenêtre afin d'ouvrir la fenêtre des rapports.
  3. Dans la fenêtre qui s'ouvre, sous l'onglet **Rapport**, cliquez sur le bouton **Rapport détaillé**.
  4. Dans la partie droite de la fenêtre **Rapport détaillé** qui s'ouvre, cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel de l'en-tête du tableau. Pour masquer des colonnes du tableau, décochez la case en regard du nom de la colonne en question dans le menu contextuel.

## FILTRAGE DES DONNEES

Les rapports de Kaspersky Internet Security permettent de filtrer les événements selon une ou plusieurs valeurs dans les colonnes du tableau, voire de définir des conditions de filtrage complexe.

- *Pour filtrer les événements selon des valeurs, procédez comme suit :*

  1. Ouvrez la fenêtre principale de l'application.
  2. Cliquez sur le lien **Rapports** dans la partie supérieure de la fenêtre afin d'ouvrir la fenêtre des rapports.
  3. Dans la fenêtre qui s'ouvre, sous l'onglet **Rapport**, cliquez sur le bouton **Rapport détaillé**.

4. Dans la partie droite de la fenêtre **Rapport détaillé**, placez le curseur sur le coin supérieur gauche de l'en-tête de la colonne, puis ouvrez le menu du filtre en cliquant sur le bouton gauche de la souris.

5. Dans le menu du filtre, choisissez la valeur à utiliser pour filtrer les données.

6. Le cas échéant, répétez la procédure pour une autre colonne du tableau.

*Pour définir des conditions de filtrage complexe, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.

2. Cliquez sur le lien **Rapports** dans la partie supérieure de la fenêtre afin d'ouvrir la fenêtre des rapports.

3. Dans la fenêtre qui s'ouvre, sous l'onglet **Rapport**, cliquez sur le bouton **Rapport détaillé**.

4. Dans la partie droite de la fenêtre **Rapport détaillé** qui s'ouvre, cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel de la colonne du rapport requise, puis choisissez l'option **Filtre**.

5. Dans la fenêtre **Filtre complexe**, définissez les conditions nécessaires du filtrage.

   a. Dans la partie droite de la fenêtre, définissez la limite de la sélection.

   b. Dans la partie gauche de la fenêtre, dans la liste déroulante **Condition**, choisissez la condition de sélection (par exemple, supérieure à ou inférieure à, égale à ou différente de la valeur indiquée en tant que limite de la sélection).

   c. Le cas échéant, ajoutez une deuxième valeur à l'aide d'un opérateur logique de conjonction (ET) ou de disjonction (OU). Si vous souhaitez que la sélection des données vérifie les deux conditions définies, sélectionnez **ET**. Si une condition minimum suffit, sélectionnez **OU**.

## RECHERCHE D'EVENEMENTS

Vous pouvez rechercher l'événement souhaité dans le rapport à l'aide d'un mot clé via la barre de recherche ou à l'aide d'une fenêtre de recherche spéciale.

*Pour trouver un événement à l'aide de la barre de recherche, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.

2. Cliquez sur le lien **Rapports** dans la partie supérieure de la fenêtre afin d'ouvrir la fenêtre des rapports.

3. Dans la fenêtre qui s'ouvre, sous l'onglet **Rapport**, cliquez sur le bouton **Rapport détaillé**.

4. Dans la partie droite de la fenêtre **Rapport détaillé** qui s'ouvre, saisissez le mot clé dans la barre de recherche.

*Pour trouver un événement à l'aide de la fenêtre de recherche, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.

2. Cliquez sur le lien **Rapports** dans la partie supérieure de la fenêtre afin d'ouvrir la fenêtre des rapports.

3. Dans la fenêtre qui s'ouvre, sous l'onglet **Rapport**, cliquez sur le bouton **Rapport détaillé**.

4. Dans la partie droite de la fenêtre **Rapport détaillé** qui s'ouvre, cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel de la colonne du rapport requise, puis choisissez l'option **Recherche**.

5. Dans la fenêtre **Recherche** qui s'ouvre, définissez les critères de la recherche.

   a. Dans le champ **Ligne**, saisissez le mot clé pour la recherche.

b. Dans la liste déroulante **Colonne**, sélectionnez le nom de la colonne dans laquelle il faudra rechercher le mot clé saisi.

c. Le cas échéant, cochez les cases ☑ pour des paramètres de recherche complémentaires.

6. Cliquez sur le bouton **Recherche avancée**.

## ENREGISTREMENT DU RAPPORT DANS UN FICHIER

Le rapport obtenu peut être enregistré dans un fichier texte.

*Pour enregistrer le rapport dans un fichier, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Cliquez sur le lien **Rapports** dans la partie supérieure de la fenêtre afin d'ouvrir la fenêtre des rapports.
3. Dans la fenêtre qui s'ouvre, sous l'onglet **Rapport**, cliquez sur le bouton **Rapport détaillé**.
4. Dans la fenêtre **Rapport détaillé** qui s'ouvre, rédigez le rapport requis, puis cliquez sur le bouton **Enregistrer**.
5. Dans la fenêtre qui s'ouvre, désignez le répertoire dans lequel il faut enregistrer le fichier du rapport et saisissez le nom du fichier.

## CONSERVATION DES RAPPORTS

La durée maximale de conservation des rapports sur les événements est limitée à 30 jours. Les données sont supprimées à l'issue de cette période. Vous pouvez annuler la restriction sur la durée de conservation ou la modifier.

De plus, vous pouvez également indiquer la taille maximale du fichier du rapport. Par défaut, la taille maximale est limitée à 1 024 Mo. Une fois que la taille maximale est atteinte, le contenu du fichier est remplacé par de nouveaux enregistrements. Vous pouvez supprimer les restrictions sur la taille du rapport ou attribuer une autre valeur.

*Pour configurer la durée maximale de conservation des rapports, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la rubrique **Paramètres avancés**, sélectionnez la sous-rubrique **Rapports et stockages**.
3. Dans la partie droite de la fenêtre, dans le groupe **Conservation des rapports**, cochez la case ☑ **Supprimer les rapports après** et indiquez la durée maximale de la conservation des rapports.

*Pour configurer la taille maximale du fichier de rapport, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la rubrique **Paramètres avancés**, sélectionnez la sous-rubrique **Rapports et stockages**.
3. Dans la partie droite de la fenêtre, dans le groupe **Conservation des rapports**, cochez la case ☑ **Taille maximale de fichier** et indiquez la taille maximale du fichier de rapport.

## PURGE DES RAPPORTS

Vous pouvez purger les rapports dont les données ne vous sont plus utiles.

*Pour purger* les rapports*, procédez comme suit* :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la rubrique **Paramètres avancés**, sélectionnez la sous-rubrique **Rapports et stockages**.
3. Dans la partie droite de la fenêtre, dans le groupe **Purge des rapports**, cliquez sur **Purger**.
4. Dans la fenêtre **Suppression des informations des rapports** qui s'ouvre, cochez les cases en regard des rapports que vous souhaitez purger.

## ENTREES RELATIVES AUX EVENEMENTS NON CRITIQUES

Par défaut, les entrées relatives aux événements non critiques, aux événements du registre ou aux événements du système de fichiers ne sont pas ajoutées. Vous pouvez inclure ces entrées dans les rapports sur la protection.

*Pour ajouter au rapport des entrées relatives aux événements non critiques, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la rubrique **Paramètres avancés**, sélectionnez la sous-rubrique **Rapports et stockages**.
3. Dans la partie droite de la fenêtre, cochez la case **Ajouter les enregistrements des événements non critiques**.

## CONFIGURATION DE LA NOTIFICATION SUR LA DISPONIBILITE DU RAPPORT

Vous pouvez programmer la fréquence selon laquelle Kaspersky Internet Security vous rappellera la disponibilité des rapports.

Pour réaliser la programmation, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Cliquez sur le lien **Rapports** dans la partie supérieure de la fenêtre afin d'ouvrir la fenêtre des rapports.
3. Dans la fenêtre qui s'ouvre, sous l'onglet **Rapport**, cochez la case **Rappeler le rapport** et ouvrez la fenêtre de configuration de la programmation en cliquant sur le temps indiqué.
4. Dans la fenêtre **Rapport : programmation** qui s'ouvre, définissez les paramètres de la programmation.

# APPARENCE DE L'APPLICATION

Vous pouvez modifier l'aspect de Kaspersky Internet Security à l'aide de skins. Il est également possible de configurer l'utilisation d'éléments actifs de l'interface (icône de l'application dans la zone de notification de la barre des tâches de Microsoft Windows et fenêtres contextuelles).

**DANS CETTE SECTION**



# GRAPHISME DE KASPERSKY INTERNET SECURITY

Tous les couleurs, les caractères, les icônes et les textes utilisés dans l'interface de Kaspersky Internet Security peuvent être modifiés. Vous pouvez créer votre propre environnement graphique pour le logiciel et localiser l'interface de l'application dans la langue de votre choix.

*Pour utilisez un autre skin, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Paramètres avancés**, sélectionnez la sous-section **Apparence**.
3. Dans le groupe **Skins**, cochez la case **Utiliser un skin personnalisé** pour activer un skin. Dans le champ de saisie, indiquez le catalogue avec les paramètres des skins et cliquez sur le bouton **Parcourir** pour trouver ce catalogue.

# ELEMENTS ACTIFS DE L'INTERFACE

Vous pouvez configurer l'affichage des éléments actifs de l'interface : par exemple, la fenêtre des notifications, l'icône Kaspersky Internet Security de la barre des tâches.

*Pour configurer les éléments actifs de l'interface, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Paramètres avancés**, sélectionnez la sous-section **Apparence**.
3. Dans le groupe **Icône de la barre des tâches**, cochez ou décochez les cases correspondantes.

# KIOSQUE D'INFORMATIONS

Grâce au *kiosque d'informations*, Kaspersky Lab vous maintient au courant des événements importants qui concernent Kaspersky Internet Security en particulier et la protection contre les menaces informatiques en général.

L'application vous signalera l'existence de nouvelles informations par le biais d'une fenêtre contextuelle dans la zone de notification de la barre des tâches. L'aspect de l'icône de l'application changera (cf. ci-dessous). Les informations sur le nombre d'informations non lues apparaissent également dans la fenêtre principale de l'application. L'option **Infos** apparaît dans le menu contextuel de l'icône de l'application, tandis que l'icône des informations apparaît dans le gadget de Kaspersky Internet Security.

Si vous ne souhaitez pas obtenir des infos, vous pouvez désactiver la réception de celles-ci d'une des manières suivantes :

- Au départ de la fenêtre du kiosque d'informations (uniquement lorsqu'il y a des informations non lues) ;
- Au départ de la fenêtre de configuration de l'application.

*Pour lire les informations, ouvrez la fenêtre du kiosque d'informations d'une des manières suivantes :*

- Cliquez sur l'icône dans la zone de notification de la barre des tâches ;
- Sélectionnez le point **Infos** dans le menu contextuel de l'icône de l'application ;
- Cliquez sur le lien **Lire les nouvelles** dans la fenêtre contextuelle présentant l'information ;
- Cliquez sur le lien **Infos** dans la fenêtre principale de l'application ;
- Cliquez sur l'icône qui apparaît au milieu du gadget quand une info est disponible (uniquement pour les systèmes d'exploitation Microsoft Windows Vista et Microsoft Windows 7).

Les méthodes citées pour ouvrir le kiosque d'informations sont disponibles uniquement lorsqu'il y a des informations non lues.

*Pour désactiver la réception des informations depuis la fenêtre du kiosque des informations, procédez comme suit :*

1. Ouvrez la fenêtre du kiosque d'informations (cf. instructions ci-dessus).
2. Décochez la case **Je souhaite recevoir des informations de Kaspersky Lab**.

*Pour désactiver la réception des informations depuis la fenêtre de configuration de l'application, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Paramètres avancés**, sélectionnez la sous-section **Apparence**.
3. Dans le groupe **Icône de la barre des tâches**, décochez la case **M'avertir des informations de Kaspersky Lab**.

# NOTIFICATIONS

Par défaut, lorsqu'un événement se produit pendant l'utilisation de Kaspersky Internet Security, vous verrez apparaître un message spécial. En fonction de la gravité de l'événement pour la sécurité de l'ordinateur, les notifications peuvent appartenir aux catégories suivantes :

- Critiques : signalent des événements d'une importance capitale du point de vue de la sécurité de l'ordinateur (par exemple : découverte d'un objet malveillant ou d'une activité dangereuse dans le système). Quand un tel message apparaît, il faut impérativement décider de la suite des événements. La fenêtre de ce genre de notification est rouge.
- Importantes : signalent des événements potentiellement importants du point de vue de la sécurité de l'ordinateur (par exemple : découverte d'un objet potentiellement infecté ou d'une activité suspecte dans le système). Quand un tel message apparaît, il faut décider du danger que représente l'objet ou le processus découvert et décider de la suite des événements. La fenêtre de ce genre de notification est orange.
- Informatives : signalent des événements qui n'ont pas une importance capitale. La fenêtre de ce genre de notification est verte.

Les notifications contiennent les informations suivantes :

- Une brève description de l'événement (activité suspecte, nouveau réseau, alerte, virus, etc.) ou le composant qui a découvert l'événement, apparaît dans le titre de la notification.

- Le corps de la description de l'événement reprend des informations détaillées sur les origines de la notification (nom de l'application à l'origine de la notification, nom de la menace découverte, paramètres de la connexion de réseau détectée, etc.).

- Les options proposées dépendent du type d'événement, par exemple : **Réparer**, **Supprimer**, **Ignorer** en cas de découverte d'un virus, **Autoriser**, **Interdire** lorsque l'application demande des privilèges pour exécuter des actions présentant un danger potentiel.

Vous pouvez sélectionner les modes de notification (cf. section "Configuration des modes de notification" à la page 192) sur les événements, ainsi que désactiver les notifications (cf. section "Activation et désactivation des notifications" à la page 192).

La liste complète des notifications figure dans les Annexes du présent document.

### DANS CETTE SECTION



## ACTIVATION ET DESACTIVATION DES NOTIFICATIONS

Kaspersky Internet Security affiche par défaut les notifications relatives aux événements. Vous pouvez désactiver l'affichage des notifications.

Même si l'affichage de la notification est désactivé, les informations relatives aux événements qui surviennent pendant l'utilisation de Kaspersky Internet Security seront consignées dans le rapport sur l'activité de l'application.

*Pour désactiver la remise des notifications, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, choisissez la sous-rubrique **Notifications** dans la rubrique **Paramètres avancés**.
3. Dans la partie droite de la fenêtre, décochez la case **Activer les notifications**.

## CONFIGURATION DES MODES DE NOTIFICATION

Les notifications relatives aux événements peuvent prendre diverses formes :

- Messages contextuels dans la zone de notification ;
- Notification sonore ;
- Messages électroniques.

Par défaut, toutes les notifications sont sonorisées. Les notifications sonores utilisent la gamme de sons de Microsoft Windows. Vous pouvez changer la gamme de sons ou désactiver la notification sonore.

Si vous choisissez de recevoir les notifications par courrier électronique, il faudra définir les paramètres de livraison.

*Pour désactiver l'accompagnement sonore, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.

2. Dans la partie gauche de la fenêtre, choisissez la sous-rubrique **Notifications** dans la rubrique **Paramètres avancés**.

3. Dans la partie droite de la fenêtre, décochez la case **Activer les sons**.

*Pour modifier la gamme de sons des notifications, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.

2. Dans la partie gauche de la fenêtre, choisissez la sous-rubrique **Notifications** dans la rubrique **Paramètres avancés**.

3. Dans la partie droite de la fenêtre, cochez la case **Utiliser les sons standard de Windows par défaut** et modifiez la gamme de sons utilisée du système d'exploitation.

   Si la case est décochée, c'est la sélection de sons de la version antérieure de l'application qui sera utilisée.

*Pour configurer les paramètres du courrier électronique pour l'envoi des notifications, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.

2. Dans la partie gauche de la fenêtre, choisissez la sous-rubrique **Notifications** dans la rubrique **Paramètres avancés**.

3. Dans la partie droite de la fenêtre, cochez la case **Activer les notifications par courriers**, puis cliquez sur le bouton **Configuration**.

4. Dans la fenêtre **Configuration des notifications par courrier** qui s'ouvre, définissez les paramètres de livraison.

# PARTICIPATION AU KASPERSKY SECURITY NETWORK

Chaque jour dans le monde, une multitude de nouveaux virus apparaît. Afin de contribuer à la collecte efficace de données sur les types et les sources des nouvelles menaces et dans le but d'accélérer le développement de moyens de neutralisation, vous pouvez participer au Kaspersky Security Network.

Kaspersky Security Network (KSN) est un ensemble de services en ligne qui permet d'accéder à la base de connaissances de Kaspersky Lab sur la réputation des fichiers, des sites et des applications. L'utilisation des données de Kaspersky Security Network permet à l'application de réagir plus rapidement aux nouvelles formes de menace, améliore l'efficacité de certains composants de la protection et réduit la probabilité de faux positifs.

La participation au Kaspersky Security Network signifie que certaines statistiques obtenues pendant l'utilisation de Kaspersky Internet Security sur votre ordinateur sont envoyées automatiquement à Kaspersky Lab.

Les données relatives à l'utilisateur ne sont ni recueillies, ni traitées, ni enregistrées.

La participation au Kaspersky Security Network est volontaire. Vous prenez cette décision pendant l'installation de Kaspersky Internet Security, mais vous pouvez la changer à tout moment.

*Pour activer l'utilisation de Kaspersky Security Network, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.

2. Dans la partie gauche de la fenêtre, choisissez la sous-rubrique **Retour d'informations** dans la rubrique **Paramètres avancés**.

3. Dans la partie droite de la fenêtre, cochez la case **J'accepte de rejoindre le Kaspersky Security Network**.

# VERIFICATION DE L'EXACTITUDE DE LA CONFIGURATION DE KASPERSKY INTERNET SECURITY

Une fois que Kaspersky Internet Security a été installé et configuré, vous pouvez vérifier si la configuration est correcte à l'aide d'un virus d'essai et de ses modifications. La vérification doit être réalisée séparément pour chaque composant de la protection/protocole.

### DANS CETTE SECTION



## VIRUS D'ESSAI EICAR ET SES MODIFICATIONS

Ce "virus" d'essai a été développé spécialement par l'organisation EICAR (The European Institute for Computer Antivirus Research) afin de tester les logiciels antivirus.

Le "virus" d'essai N'EST PAS un programme malveillant et il ne contient pas de code qui pourrait nuire à votre ordinateur. Toutefois, la majorité des logiciels antivirus considère EICAR comme un virus.

N'utilisez jamais d'authentiques virus pour vérifier le fonctionnement de votre antivirus !

Vous pouvez télécharger le "virus" d'essai depuis le site officiel de l'organisation EICAR : http://www.eicar.org/anti_virus_test_file.htm.

Avant de lancer le téléchargement, il faut suspendre la protection antivirus (cf. section "Suspension et lancement de la protection" à la page 52), puisque le "virus" d'essai, chargé depuis la page anti_virus_test_file.htm, sera identifié et traité par l'application en tant qu'objet infecté transmis par le protocole HTTP.

L'application identifie le fichier téléchargé depuis le site de la société EICAR comme un objet infecté par un virus qui ne peut être réparé et exécute l'action définie pour ce genre d'objet.

Vous pouvez également utiliser une modification du virus d'essai standard afin de vérifier le bon fonctionnement de l'application. Pour ce faire, il faut modifier le contenu du virus d'essai standard en ajoutant un des préfixes présentés dans le tableau ci-après. Pour créer une modification du virus d'essai, vous pouvez utiliser n'importe quel éditeur de fichier texte ou éditeur hypertexte tel que le Bloc-Notes de Microsoft ou UltraEdit32.

La première colonne du tableau (cf. ci-dessous) contient les préfixes qu'il faut ajouter en tête de la ligne du "virus" d'essai traditionnel afin de pouvoir créer sa modification. La deuxième colonne reprend toute les valeurs possibles de l'état attribué par application à la fin de l'analyse. La troisième colonne contient les informations relatives au traitement

que réservera l'application aux objets de l'état indiqué. N'oubliez pas que les actions à réaliser sur les objets sont définies par les paramètres de l'application.

Après avoir ajouté le préfixe au "virus" d'essai, enregistrez le fichier obtenu sous le nom présentant la modification du virus : par exemple, si vous avez ajouté le préfixe DELE-, enregistrez le fichier obtenu sous le nom eicar_dele.com.

N'oubliez pas de restaurer la protection antivirus dès que le téléchargement du "virus" d'essai et la création de sa modification seront terminés.

*Tableau 2. Modifications du virus d'essai*

| Préfixe | Etat de l'objet | Informations relatives au traitement de l'objet |
|---|---|---|
| Pas de préfixe, "virus" d'essai standard. | **Infecté**.<br>L'objet contient le code d'un virus connu. Réparation impossible. | L'application identifie l'objet en tant que virus qui ne peut être réparé.<br>Une erreur se produit en cas de tentative de réparation de l'objet ; l'action définie pour les objets qui ne peuvent être réparés est appliquée. |
| CORR- | **Corrompu**. | L'application a pu accéder à l'objet mais n'a pas pu l'analyser car l'objet est corrompu (par exemple, sa structure est endommagée ou le format du fichier est invalide). Les informations relatives au traitement de l'objet figurent dans le rapport sur le fonctionnement de l'application. |
| WARN- | **Suspect**.<br>L'objet contient le code d'un virus inconnu. Réparation impossible. | L'objet est considéré comme suspect. Au moment de la découverte, les bases de l'application ne contenaient pas la description de la réparation de cet objet. Vous serez averti de la découverte d'un tel objet. |
| SUSP- | **Suspect**.<br>L'objet contient le code modifié d'un virus connu. Réparation impossible. | L'application a découvert une équivalence partielle entre un extrait du code de l'objet et un extrait du code d'un virus connu. Au moment de la découverte, les bases de l'application ne contenaient pas la description de la réparation de cet objet. Vous serez averti de la découverte d'un tel objet. |
| ERRO- | **Erreur d'analyse**. | Une erreur s'est produite lors de l'analyse de l'objet. L'application ne peut accéder à l'objet car l'intégrité de celui-ci a été violée (par exemple : il n'y a pas de fin à une archive multivolume) ou il n'y a pas de lien vers l'objet (lorsque l'objet se trouve sur une ressource de réseau). Les informations relatives au traitement de l'objet figurent dans le rapport sur le fonctionnement de l'application. |
| CURE- | **Infecté**.<br>L'objet contient le code d'un virus connu. Réparable. | L'objet contient un virus qui peut être réparé. L'application répare l'objet et le texte du corps du virus est remplacé par CURE. Vous serez averti de la découverte d'un tel objet. |
| DELE- | **Infecté**.<br>L'objet contient le code d'un virus connu. Réparation impossible. | L'application identifie l'objet en tant que virus qui ne peut être réparé.<br>Une erreur se produit en cas de tentative de réparation de l'objet ; l'action définie pour les objets qui ne peuvent être réparés est appliquée.<br>Vous serez averti de la découverte d'un tel objet. |

# TEST DE LA PROTECTION DU TRAFIC HTTP

➡ *Pour tester l'identification de virus dans le flux de données transmises par le protocole HTTP :*

essayez de télécharger le "virus" d'essai depuis le site officiel de l'organisation **EICAR** : http://www.eicar.org/anti_virus_test_file.htm.

Lors de la tentative de téléchargement du virus d'essai, Kaspersky Internet Security découvre l'objet, l'identifie comme étant infecté et ne pouvant être réparé, puis exécute l'action définie dans les paramètres d'analyse du trafic HTTP pour ce type d'objet. Par défaut, la connexion avec le site est coupée à la moindre tentative de téléchargement du virus d'essai et un message indiquera dans le navigateur que l'objet en question est infecté par le virus EICAR-Test-File.

# TEST DE LA PROTECTION DU TRAFIC SMTP

Pour tester l'identification des virus dans le flux de données transmises via le protocole SMTP, vous pouvez utiliser le système de messagerie qui exploite ce protocole pour le transfert des données.

Il est conseillé de tester la détection de virus dans les différentes parties du courrier sortant : aussi bien sur le corps des messages que les pièces jointes. Pour le test, utilisez le fichier du virus d'essai EICAR (cf. section "Virus d'essai EICAR et ses modifications" à la page 194).

*Pour tester la détection de virus dans le flux de données envoyées par le protocole SMTP, procédez comme suit :*

1. Composez le message au format "Texte normal" à l'aide du client de messagerie installé sur l'ordinateur.

   Les messages contenant le "virus" d'essai dans le corps et rédigés au format RTF ou HTML ne seront pas analysés !

2. En fonction de la partie du message où l'application doit détecter un virus, procédez comme suit :

   - Pour détecter le virus dans le corps du message, placez le texte du "virus" d'essai standard ou modifié EICAR au début du message ;
   - Pour détecter le virus dans les pièces jointes, ajoutez au message le fichier contenant le "virus" d'essai EICAR.

3. Envoyez ce message à l'adresse de l'administrateur.

L'application découvre l'objet, l'identifie en tant qu'objet infecté et bloque l'envoi du message.

# VERIFICATION DE L'EXACTITUDE DE LA CONFIGURATION DE L'ANTIVIRUS FICHIERS

*Pour vérifier l'exactitude de la configuration de l'Antivirus Fichiers, procédez comme suit :*

1. Créez un dossier sur le disque, copiez-y le virus d'essai récupéré sur le site officiel de l'organisation **EICAR** (http://www.eicar.org/anti_virus_test_file.htm) ainsi que les modifications de ce virus que vous avez créées.
2. Autorisez la consignation de tous les événements afin que le rapport reprenne les données sur les objets corrompus ou les objets qui n'ont pas été analysés suite à un échec.
3. Exécutez le fichier du virus d'essai ou une de ses modifications.

L'Antivirus Fichiers intercepte la requête adressée au fichier, la vérifie et exécute l'action définie dans les paramètres. En sélectionnant diverses actions à réaliser sur l'objet infecté, vous pouvez vérifier le fonctionnement du composant dans son ensemble.

Les informations complètes sur les résultats du fonctionnement de l'Antivirus Fichiers sont consultables dans le rapport sur l'utilisation du composant.

# VERIFICATION DE L'EXACTITUDE DE LA CONFIGURATION DE LA TACHE D'ANALYSE ANTIVIRUS

*Pour vérifier l'exactitude de la configuration de la tâche d'analyse, procédez comme suit :*

1. Créez un dossier sur le disque, copiez-y le virus d'essai récupéré sur le site officiel de l'organisation **EICAR** (http://www.eicar.org/anti_virus_test_file.htm) ainsi que les modifications de ce virus que vous avez créées.

2. Créez une nouvelle tâche d'analyse antivirus et en guise d'objet à analyser, sélectionnez le dossier contenant la sélection de virus d'essai.

3. Autorisez la consignation de tous les événements dans le rapport afin de conserver les données relatives aux objets corrompus ou aux objets qui n'ont pas été analysés suite à l'échec.

4. Lancez la tâche d'analyse antivirus.

Lors de l'analyse, les actions définies dans les paramètres de la tâche seront exécutées au fur et à mesure que des objets suspects ou infectés sont découverts. En sélectionnant diverses actions à réaliser sur l'objet infecté, vous pouvez vérifier le fonctionnement du composant dans son ensemble.

Toutes les informations relatives aux résultats de l'exécution de la tâche d'analyse sont consultables dans le rapport de fonctionnement du composant.

# VERIFICATION DE L'EXACTITUDE DE LA CONFIGURATION DE LA PROTECTION CONTRE LE COURRIER INDESIRABLE

Pour vérifier la protection contre le courrier indésirable, vous pouvez utiliser un message d'essai qui sera considéré comme indésirable par l'application.

Le corps du message d'essai doit contenir la ligne suivante :

```
Spam is bad do not send it
```

Une fois que ce message est arrivée sur l'ordinateur, Kaspersky Internet Security l'analyse, lui attribue l'état de courrier indésirable et exécute l'action définie pour les objets de ce type.

# CONTACTER LE SUPPORT TECHNIQUE

En cas de problème d'utilisation de Kaspersky Internet Security, vérifiez d'abord si la solution n'est pas expliquée dans la documentation, dans l'aide, dans la banque de solutions du service d'assistance technique de Kaspersky Lab ou dans le forum des utilisateurs.

Si vous ne trouvez pas la réponse à votre question, vous pouvez contacter le service d'assistance technique de Kaspersky Lab d'une des manières suivantes :

- Envoyez une demande depuis Mon Espace Personnel sur le site Web du service d'assistance technique ;
- Appelez par téléphone.

Les experts du service d'assistance technique répondront à vos questions sur l'installation, l'activation et l'utilisation de l'application. En cas d'infection de votre ordinateur, ils vous aideront à supprimer les conséquences de l'action des programmes malveillants.

Avant de contacter le service d'assistance technique, veuillez prendre connaissance des règles d'assistance (http://support.kaspersky.com/fr/support/rules).

Si vous contactez les experts du Service d'assistance technique, ceux-ci peuvent vous demander de générer un rapport sur l'état du système et un fichier de trace et de les envoyer au support technique. Après l'analyse des données envoyées, les experts du Service d'assistance technique pourront créer le script AVZ et vous l'envoyer. Celui-ci vous aidera à supprimer les problèmes rencontrés.

### DANS CETTE SECTION



## MON ESPACE PERSONNEL

Comme son nom l'indique, *Mon Espace Personnel* est un espace qui vous est réservé sur le site du support technique. Vous pouvez y réaliser les opérations suivantes :

- Envoyer des demandes au service d'assistance technique et au laboratoire d'étude des virus ;
- Communiquer avec le service d'assistance technique sans devoir envoyer des messages électroniques ;
- Suivre le statut de vos demandes en temps réel ;
- Consulter l'historique complet de votre interaction avec le support technique.

*Pour accéder à la page d'accueil de Mon Espace Personnel, réalisez une des opérations suivantes :*

- Cliquez sur le lien **Mon Espace Personnel** dans la fenêtre principale de Kaspersky Internet Security ;

- Saisissez l'URL https://my.kaspersky.com/en/index.html?LANG=fr dans la barre d'adresse du navigateur.

Si vous n'êtes pas enregistré dans Mon Espace Personnel, vous pouvez réaliser la procédure d'enregistrement à la page d'enregistrement https://my.kaspersky.com/ru/registration?LANG=fr. Vous devrez saisir votre adresse de messagerie et un mot de passe d'accès à Mon Espace Personnel. L'envoi de questions sur l'utilisation de Kaspersky Internet Security requiert le code d'activation.

N'oubliez pas que certaines demandes doivent être envoyées non pas au service d'assistance technique mais au laboratoire d'étude des virus. Il s'agit des demandes du type suivant :

- Programme malveillant inconnu. Vous pensez qu'un objet quelconque est malveillant mais Kaspersky Internet Security ne confirme pas vos soupçons ;
- Faux positif du logiciel antivirus. Kaspersky Internet Security considère un certain fichier comme un virus mais vous êtes convaincu que ce n'est pas le cas ;
- Demande de description d'un programme malveillant. Vous souhaitez obtenir la description d'un virus quelconque.

L'envoi de demandes au laboratoire d'étude des virus ne requiert pas le code d'activation.

Vous pouvez également envoyer des demandes au laboratoire d'étude des virus sans vous enregistrer dans Mon Espace Personnel. Utilisez pour ce faire le formulaire de demande en ligne (http://support.kaspersky.ru/virlab/helpdesk.html?LANG=fr).

# ASSISTANCE TECHNIQUE PAR TELEPHONE

Si le problème est urgent, vous pouvez téléphoner au service d'assistance technique dans votre ville. Si vous contactez l'assistance technique russe (http://support.kaspersky.com/fr/support/support_local) ou internationale (http://support.kaspersky.com/fr/support/international) veuillez fournir l'information (http://support.kaspersky.com/fr/support/details Nos experts pourront ainsi vous venir en aide plus rapidement.

# CREATION D'UN RAPPORT SUR L'ETAT DU SYSTEME

Afin de pouvoir résoudre vos problèmes, il se peut que les experts du Service d'assistance technique de Kaspersky Lab aient besoin d'un rapport sur l'état du système. Ce rapport contient des informations détaillées sur les processus exécutés, les modules et les pilotes chargés, les modules externes de Microsoft Internet Explorer et de l'Assistant Microsoft Windows, les ports ouverts, les objets suspects décelés, etc.

Aucune donnée personnelle relative à l'utilisateur n'est recueillie durant la création du rapport.

*Pour créer un rapport sur l'état du système, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application (cf. section "Fenêtre principale de Kaspersky Internet Security" à la page 42).
2. Cliquez sur le lien **Assistance technique** dans la partie inférieure de la fenêtre principale pour ouvrir la fenêtre **Assistance technique** dans laquelle vous cliquerez sur le lien **Outils d'assistance**.
3. Dans la fenêtre **Informations pour le service d'assistance technique**, cliquez sur le bouton **Créer le rapport sur l'état du système**.

Le rapport sur l'état du système est généré au format HTML et XML et il est enregistré dans l'archive sysinfo.zip. Une fois que la collecte des informations sur le système est terminée, vous pouvez consulter le rapport.

*Pour consulter le rapport, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application (cf. section "Fenêtre principale de Kaspersky Internet Security" à la page 42).
2. Cliquez sur le lien **Assistance technique** dans la partie inférieure de la fenêtre principale pour ouvrir la fenêtre **Assistance technique** dans laquelle vous cliquerez sur le lien **Outils d'assistance**.
3. Dans la fenêtre **Informations pour le service d'assistance technique** qui s'ouvre, cliquez sur le bouton **Voir**.
4. Ouvrez l'archive sysinfo.zip contenant le fichier du rapport.

# CREATION D'UN FICHIER DE TRACE

Le système d'exploitation et certaines applications peuvent connaître des échecs après l'installation de Kaspersky Internet Security. Dans ce cas, il s'agit généralement d'un conflit entre Kaspersky Internet Security et des applications installées ou des pilotes sur l'ordinateur. Afin de résoudre ce problème, les experts du Service d'assistance technique de Kaspersky Lab pourraient vous demander de créer un fichier de trace.

*Afin de créer le fichier de trace, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application (cf. section "Fenêtre principale de Kaspersky Internet Security" à la page 42).
2. Cliquez sur le lien **Assistance technique** dans la partie inférieure de la fenêtre principale pour ouvrir la fenêtre **Assistance technique** dans laquelle vous cliquerez sur le lien **Outils d'assistance**.
3. Dans la fenêtre **Informations pour le service d'assistance technique** qui s'ouvre, dans le groupe **Traçages** sélectionnez le niveau du traçage dans la liste déroulante.

   Il est recommandé de demander au spécialiste du Service d'assistance technique le niveau du traçage requis. Faute d'indication du Service d'assistance technique, il est conseillé d'établir le niveau du traçage à **500**.
4. Afin de lancer le traçage, cliquez sur le bouton **Activer**.
5. Reproduisez la situation où le problème apparaît.
6. Pour arrêter le traçage, cliquez sur le bouton **Désactiver**.

Vous pouvez passer au transfert des résultats du traçage (cf. section "Envoi des fichiers de données" à la page 200) sur le serveur de Kaspersky Lab.

# ENVOI DES RAPPORTS

Une fois que les fichiers de traçage et le rapport sur l'état du système ont été créés, il faut les envoyer aux experts du Service d'assistance technique de Kaspersky Lab.

Pour charger les fichiers de données sur le serveur du Service d'assistance technique, il faut obtenir un numéro de requête. Ce numéro est accessible dans Mon Espace Personnel sur le site web du Service d'assistance technique lorsque des requêtes actives sont présentes.

*Pour télécharger les fichiers de données sur le serveur du Service d'assistance technique, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application (cf. section "Fenêtre principale de Kaspersky Internet Security" à la page 42).
2. Cliquez sur le lien **Assistance technique** dans la partie inférieure de la fenêtre principale pour ouvrir la fenêtre **Assistance technique** dans laquelle vous cliquerez sur le lien **Outils d'assistance**.

3. Dans la fenêtre **Informations pour le service d'assistance technique** qui s'ouvre, dans le groupe **Actions**, cliquez sur le bouton **Envoyer les informations au service d'assistance technique**.

   La fenêtre **Chargement des informations pour l'assistance sur le serveur** s'ouvre.

4. Cochez les cases en regard des fichiers que vous souhaitez envoyer au Service d'assistance technique, puis cliquez sur **Envoyer**.

   La fenêtre **Numéro de requête** s'ouvre.

5. Indiquez le numéro attribué à votre demande lors de l'appel au Service d'assistance technique via Mon Espace Personnel et cliquez sur le bouton **OK**.

Les fichiers de données sélectionnés seront compactés et envoyés sur le serveur du Support technique.

S'il n'est pas possible pour une raison quelconque de contacter le Service d'assistance technique, vous pouvez enregistrer les fichiers de données sur votre ordinateur et les envoyer plus tard depuis Mon Espace Personnel.

*Pour enregistrer les fichiers de données sur le disque, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application (cf. section "Fenêtre principale de Kaspersky Internet Security" à la page 42).

2. Cliquez sur le lien **Assistance technique** dans la partie inférieure de la fenêtre principale pour ouvrir la fenêtre **Assistance technique** dans laquelle vous cliquerez sur le lien **Outils d'assistance**.

3. Dans la fenêtre **Informations pour le service d'assistance technique** qui s'ouvre, dans le groupe **Actions**, cliquez sur le bouton **Envoyer les informations au service d'assistance technique**.

   La fenêtre **Chargement des informations pour l'assistance sur le serveur** s'ouvre.

4. Cochez les cases en regard des fichiers que vous souhaitez envoyer au Service d'assistance technique, puis cliquez sur **Envoyer**.

   La fenêtre **Saisir le numéro de requête (numéro SRF)** s'ouvre.

5. Cliquez sur le bouton **Annuler**, et dans la fenêtre qui s'ouvre confirmez l'enregistrement des fichiers sur le disque, en cliquant sur le bouton **Oui**.

   La fenêtre d'enregistrement des archives s'ouvre.

6. Saisissez le nom de l'archive et confirmez l'enregistrement.

Vous pouvez envoyer l'archive créée au Service d'assistance technique via Mon Espace Personnel.

# EXECUTION DU SCRIPT AVZ

Les experts de Kaspersky Lab analysent votre problème sur la base des fichiers de trace et du rapport sur l'état du système. Cette analyse débouche sur une séquence d'actions à exécuter pour supprimer les problèmes identifiés. Le nombre de ces actions peut être très élevé.

Pour simplifier la procédure de résolution des problèmes, des scripts AVZ sont utilisés. Le script AVZ est un ensemble d'instructions qui permettent de modifier les clés du registre, de mettre des fichiers en quarantaine, de lancer des recherches de catégories avec possibilité de mise en quarantaine des fichiers connexes, de bloquer les intercepteurs UserMode et KernelMode, etc.

Pour exécuter les scripts inclus dans l'application, utilisez *l'Assistant d'exécution des scripts AVZ*.

L'Assistant se compose d'une série de fenêtres (étapes) entre lesquelles vous pouvez naviguer grâce aux boutons **Précédent** et **Suivant**. Pour quitter l'Assistant, cliquez sur le bouton **Terminer**. Pour interrompre l'Assistant à n'importe quelle étape, cliquez sur le bouton **Annuler**.

Il est déconseillé de modifier le texte du script envoyé par les experts de Kaspersky Lab. En cas de problème lors de l'exécution du script, contactez le Support technique.

*Pour lancer l'Assistant, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application (cf. section "Fenêtre principale de Kaspersky Internet Security" à la page 42).

2. Cliquez sur le lien **Assistance technique** dans la partie inférieure de la fenêtre principale pour ouvrir la fenêtre **Assistance technique** dans laquelle vous cliquerez sur le lien **Outils d'assistance**.

3. Dans la fenêtre **Informations pour le service d'assistance technique** qui s'ouvre, cliquez sur le bouton **Exécuter le script AVZ**.

Si l'exécution du script réussi, l'Assistant termine. Si un échec se produit durant l'exécution du script, l'Assistant affiche le message correspondant.

# ANNEXES

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

### DANS CETTE SECTION



# ETATS DE L'ABONNEMENT

L'état de l'abonnement se caractérise par un des états suivants :

- *En cours*. La demande sur l'abonnement n'a pas encore été traitée (pour traiter la demande sur le serveur, un certain temps est requis). Kaspersky Internet Security est totalement opérationnel. Si à l'expiration d'une certaine période la demande sur l'abonnement n'a pas été traitée, vous recevez une notification que la mise à jour de l'état de l'abonnement n'a pas été exécutée. Les bases de l'application ne seront plus actualisées (pour les licences avec abonnement pour la mise à jour) et l'ordinateur ne sera plus protégé (pour les licences avec abonnement pour la mise à jour et la protection).

- *Activé*. L'abonnement a été activé pour une durée indéterminée ou non (la date de fin de validité est alors précisée).

- *Renouvelé*. L'abonnement a été renouvelé pour une durée indéterminée ou non.

- *Erreur*. Lors de la mise à jour de l'état de l'abonnement, une erreur s'est produite.

- *Expiré. Période de grâce.* La durée de validité de l'abonnement ou la durée pour la mise à jour de l'état a expiré. Si la durée de validité pour la mise à jour de l'état a expiré, actualisez l'état de l'abonnement à la main. Si la durée de validité de l'abonnement a expiré, vous pouvez renouveler l'abonnement en contactant la boutique en ligne où vous avez acheté Kaspersky Internet Security. Avant de pouvoir utiliser un autre code d'activation, il faut d'abord supprimer le fichier de licence pour l'abonnement utilisé.

- *Expiré. Période de grâce expirée.* La durée de validité de l'abonnement ou la période de grâce pour le renouvellement de la licence est écoulée. Contactez votre fournisseur de l'abonnement pour obtenir un nouvel abonnement ou renouveler l'abonnement actuel.

  Si la durée de validité de l'abonnement est écoulée ainsi que la période complémentaire durant laquelle le renouvellement est possible (état *Expiré*), Kaspersky Internet Security vous le signale et cesse de tenter d'obtenir le renouvellement depuis le serveur. Dans le cas des licences avec abonnement pour la mise à jour, les fonctions de l'application sont préservées à l'exception de la mise à jour des bases de l'application. Dans le cas d'une licence avec abonnement pour la mise à jour et la protection, les bases de l'application ne seront plus actualisées, l'ordinateur ne sera plus protégé et les analyses ne seront plus exécutées.

- *Refus de l'abonnement*. Vous avez refusé l'abonnement pour renouveler automatiquement la licence.

- *Mise à jour requise*. L'état de l'abonnement n'a pas été actualisé à temps pour une raison quelconque.

  Si l'abonnement n'a pas été renouvelé à temps (par exemple, l'ordinateur n'était pas allumé pendant la période où le renouvellement de la licence était possible), vous pouvez actualiser son état manuellement dans la fenêtre de Gestionnaire de licences (cf. section "Consultation des informations sur la licence" à la page 39). Avant le renouvellement de l'abonnement, Kaspersky Internet Security n'actualise plus les bases de l'application (pour

les licences avec abonnement pour la mise à jour) et cesse de protéger l'ordinateur et de lancer l'analyse (pour les licences commerciales avec abonnement pour la mise à jour et la protection).

- *Suspendu*. L'abonnement pour renouveler la licence est suspendu.
- *Restauré*. L'abonnement est restauré.

# Liste des notifications de Kaspersky Internet Security

Cette rubrique reprend la liste des notifications qui peuvent être affichées pendant l'utilisation de Kaspersky Internet Security.

### Dans cette section



## Notifications dans n'importe quel mode de protection

Cette rubrique reprend les notifications qui apparaissent durant l'utilisation de l'application aussi bien en mode automatique, qu'en mode de protection interactif (cf. section "Sélection du mode de protection" à la page 74). Si vous souhaitez voir toutes les notifications possibles, passez en mode de protection interactif. Dans ce cas, les notifications décrites dans cette rubrique ainsi que celles qui apparaissent uniquement en mode interactif (cf. section "Notifications dans le mode de protection interactif" à la page 211) seront visibles.

### Dans cette section



### Une procedure speciale de reparation est requise

Suite à la découverte d'une menace active en ce moment dans le système (par exemple, un processus malveillant dans la mémoire vive ou dans les objets de démarrage), un message vous invitant à lancer la procédure de réparation élargie s'affiche.

Le message reprend les informations suivantes :

- La description de la menace.
- Le type de la menace et le nom de l'objet malveillant tel que repris dans l'Encyclopédie des virus de Kaspersky Lab.

  L'icône s'affiche à côté du nom de l'objet malveillant. Cliquez sur cette icône pour ouvrir la fenêtre contenant les informations sur l'objet. Le lien //www.viruslist.com/fr dans la fenêtre permet d'accéder au site Web de l'Encyclopédie des virus et d'obtenir des informations plus précises sur une menace.
- Le nom du fichier de l'objet malveillant, y compris son chemin d'accès.

Vous aurez le choix entre les actions suivantes :

- **Oui, réparer et redémarrer** : exécute une procédure spéciale de réparation.

  Les experts de Kaspersky Lab recommandent vivement de sélectionner cette option. Cependant, n'oubliez pas qu'à la fin de la procédure de réparation, le système d'exploitation sera redémarré. C'est pourquoi, il est conseillé d'enregistrer tous les travaux en cours et de quitter toutes les applications avant de lancer la procédure. Lors de la procédure de réparation, il est interdit de lancer les clients de messagerie ou de modifier les bases de registres système du système d'exploitation. Une fois que l'ordinateur a redémarré, il est conseillé de lancer une analyse complète.
- **Ne pas exécuter** : l'objet ou le processus trouvé sera traité conformément aux actions sélectionnées précédemment.

Pour que l'action sélectionnée soit toujours appliquée ultérieurement dans une situation similaire, cochez la case **Appliquer à tous les objets**.

## CHARGEMENT DISSIMULE D'UN PILOTE

Certains programmes malveillants téléchargent les pilotes sur l'ordinateur de l'utilisateur d'une manière cachée. Après cela, il n'est pas possible de contrôler l'activité du programme malveillant à l'aide de Kaspersky Internet Security. Les applications utiles utilisent rarement ce mode de téléchargement des pilotes.

Quand le Contrôle des Applications détecte une tentative de téléchargement d'un pilote d'une manière cachée, une notification apparaît.

Le message reprend les informations suivantes :

- La description de la menace.
- Le nom du fichier du pilote, y compris son chemin d'accès.

  L'icône s'affiche à côté du nom du fichier. Cliquez sur cette icône pour ouvrir la fenêtre contenant les informations sur le pilote.

Choisissez l'une des options suivantes :

- **Autoriser maintenant** : autorise le téléchargement du pilote et ajoute le pilote à la liste des exclusions.
- **Interdire maintenant** : interdit le téléchargement du pilote.
- **Quarantaine** : interdit le téléchargement du pilote et place le fichier du pilote en quarantaine.

## UNE APPLICATION POTENTIELLEMENT DANGEREUSE SANS SIGNATURE NUMERIQUE EST LANCEE

Quand le Contrôle des Applications détecte une application lancée sur l'ordinateur sans signature numérique et figurant dans le haut du classement du danger (selon l'analyse heuristique), une notification apparaît.

Le message reprend les informations suivantes :

- La description de la menace.
- Le nom de l'application lancée.

  L'icône s'affiche à côté du nom de l'application. Cliquez sur cette icône pour ouvrir la fenêtre contenant les informations sur l'application.
- Informations sur le nombre d'utilisateurs qui utilisent l'application et lui font confiance.

Vous pouvez indiquer si vous faites confiance ou non à l'application en sélectionnant une des actions suivantes :

- **Oui, je fais confiance** : autorise le lancement et l'exécution de l'application sans restrictions.
- **Restreindre l'application** : autorise le lancement de l'application, mais interdit l'exécution des opérations dangereuses.
- **Bloquer** : interdit le lancement et l'exécution de l'application maintenant et ultérieurement.

## UN DISQUE AMOVIBLE A ETE CONNECTE

Une notification apparaît lors de la connexion d'un disque amovible à l'ordinateur. Vous aurez le choix entre les actions suivantes :

- **Analyse rapide** : analyse uniquement les fichiers sur le disque amovible qui peuvent être potentiellement dangereux.
- **Analyse complète** : analyse tous les fichiers sur le disque amovible.
- **Ne pas analyser** : n'analyse pas le disque amovible.

Pour appliquer ultérieurement l'action sélectionnée à tous les disques amovibles à connecter, cochez la case ☑ **Appliquer à tous les cas similaires**.

## UN NOUVEAU RESEAU A ETE DECOUVERT

Chaque fois que l'ordinateur se connecte à une nouvelle zone (réseau), un message s'affiche.

La partie supérieure de la notification reprend des informations sur le réseau :

- L'adaptateur de réseau utilisé pour la connexion au réseau ;
- Le type de réseau (par exemple, "sans fil") ;
- Le nom du réseau.

La partie inférieure de la fenêtre vous propose d'attribuer un état à la nouvelle zone. Cet état permettra d'autoriser ou non telle ou telle activité de réseau.

- **Oui, ce réseau est fiable**. Cet état doit être réservé aux zones qui, d'après vous, ne présentent aucun danger car l'ordinateur ne risque pas d'être attaqué ou victime d'un accès non autorisé.

- **Réseau local**. Cet état est recommandé pour les zones présentant un risque moyen (par exemple, le réseau interne d'une entreprise).

- **Non, c'est un réseau public**. Ce réseau présente un très grand risque car une fois que l'ordinateur y est connecté, il est exposé à toutes les menaces possibles et imaginables. Cet état doit être sélectionné pour les réseaux qui ne sont protégés par aucun logiciel antivirus, pare-feu, filtre, etc. Ce choix offre la protection maximale de l'ordinateur dans cet environnement.

## UN CERTIFICAT DOUTEUX A ETE DECOUVERT

L'analyse de la sécurité de la connexion via le protocole SSL aura lieu à l'aide du certificat installé. En cas de tentative de connexion au serveur avec un certificat incorrect (par exemple, en cas de substitution par les individus malintentionnés), un message spécial s'affiche.

Le message reprend les informations suivantes :

- La description de la menace ;

- Le lien pour consulter le certificat ;

- Les causes possibles de l'erreur ;

- L'URL de la ressource.

Vous êtes invité à de prendre une décision sur la nécessité de la connexion dans les conditions d'utilisation d'un certificat douteux :

- **Oui, accepter le certificat douteux** : poursuit la connexion à une ressource en ligne.

- **Rejeter le certificat** : arrête la connexion à une ressource en ligne.

## DEMANDE D'AUTORISATION DE CONNEXION A UN SITE DU DOMAINE REGIONAL

Lors de la tentative d'ouverture d'un site appartenant à un domaine régional pour lequel aucune décision n'a été prise sur l'octroi ou le refus de l'accès, une notification apparaît.

Le message reprend les informations suivantes :

- La description de la raison du blocage de la connexion au site ;

- Le nom de la région à laquelle le site appartient ;

- Le domaine et les caractéristiques du niveau d'infection des sites Web dans ce domaine ;

- L'adresse du site Web ;

- Le nom de l'application qui se connecte au site Web.

Choisissez l'une des options suivantes :

- **Oui, autoriser la consultation** : charge le site Web.

- **Non, interdire la consultation** : refuse le chargement du site Web.

Pour que l'action sélectionnée soit appliquée ultérieurement à tous les sites Web de ce domaine régional, cochez la case **Enregistrer pour cette région**.

## DECOUVERTE D'UNE APPLICATION POTENTIELLEMENT DANGEREUSE

Quand la Surveillance du système découvre une application dont le comportement est semblable à celui des programmes malveillants, une notification apparaît.

Le message reprend les informations suivantes :

- La description de la menace.
- Le type de programme potentiellement malveillant et son nom.

  L'icône s'affiche à côté du nom de l'application. Cliquez sur cette icône pour ouvrir la fenêtre contenant les informations sur l'application.
- L'identificateur du processus et le nom du fichier de l'application, y compris le chemin d'accès.
- Le lien vers la fenêtre avec l'historique d'apparition de l'application.

Choisissez l'une des options suivantes :

- **Quarantaine** : quitte l'application ; place le fichier de l'application en quarantaine où il ne constituera pas de menace pour la sécurité de votre ordinateur.

  Lors des analyses suivantes de la quarantaine, l'état de l'objet peut se modifier. Par exemple, l'objet peut être identifié comme étant infecté et traité à l'aide de bases actualisées ou il peut recevoir l'état *sain* et dans ce cas, il pourra être restauré.

  En cas de mise en quarantaine manuelle d'un fichier qui lors de l'analyse suivante ne sera pas considéré comme infecté, son état deviendra *ok* uniquement si le fichier est analysé dans les trois jours maximum après la mise en quarantaine.
- **Terminer** : interrompt l'exécution de l'application.
- **Autoriser** : autorise l'exécution de l'application.
- **Ajouter aux exclusions** : autorise l'application à exécuter toujours de telles actions.

## UNE NOUVELLE VERSION DE L'APPLICATION EST DISPONIBLE

Quand une nouvelle version de Kaspersky Internet Security est disponible sur les serveurs de Kaspersky Lab, une notification apparaît.

Le message reprend les informations suivantes :

- Le lien vers les informations détaillées sur la nouvelle version de l'application ;
- La taille de la distribution.

Vous aurez le choix entre les actions suivantes :

- **Oui, télécharger** : télécharge la distribution de la nouvelle version de l'application dans le dossier indiqué.
- **Non** : refuse de télécharger la distribution.

Pour que les notifications relatives aux nouvelles versions de l'application ne soient plus affichées, cochez la case **Ne pas m'informer de cette mise à jour**.

## UNE MISE A JOUR TECHNIQUE A ETE DIFFUSEE

Quand une mise à jour technique de Kaspersky Internet Security est disponible sur les serveurs de Kaspersky Lab, une notification apparaît.

Le message reprend les informations suivantes :

- Le nouveau de la version de l'application installée sur l'ordinateur ;
- Le numéro de version de l'application après la mise à jour technique proposée ;
- Le lien vers les informations détaillées sur la mise à jour technique ;
- La taille du fichier de la mise à jour.

Vous aurez le choix entre les actions suivantes :

- **Oui, télécharger** : charge le fichier de la mise à jour dans le dossier indiqué.
- **Non** : refuse de télécharger la mise à jour. Cette option est disponible si la case **Ne pas m'informer de cette mise à jour** a été cochée (cf. ci-après).
- **Non, me rappeler plus tard** : ne télécharge pas la mise à jour maintenant et envoi un rappel plus tard. Cette option est disponible si la case **Ne pas m'informer de cette mise à jour** a été décochée (cf. ci-après).

Pour que les notifications relatives à la mise à jour ne soient plus affichées, cochez la case **Ne pas m'informer de cette mise à jour**.

## UNE MISE A JOUR TECHNIQUE A ETE TELECHARGEE

À l'issue du téléchargement de la mise à jour technique de Kaspersky Internet Security depuis les serveurs de Kaspersky Lab, une notification apparaît.

Le message reprend les informations suivantes :

- Le numéro de version de l'application après la mise à jour technique ;
- Le lien vers le fichier de la mise à jour.

Vous aurez le choix entre les actions suivantes :

- **Oui, installer** : installe la mise à jour.

  Après l'installation de la mise à jour, il faut redémarrer le système d'exploitation.

- **Reporter l'installation** : reporte l'installation.

## LA MISE A JOUR TECHNIQUE TELECHARGEE N'A PAS ETE INSTALLEE

Si une mise à jour technique de Kaspersky Internet Security a été téléchargée, mais pas encore installée, une notification apparaît.

Le message reprend les informations suivantes :

- Le numéro de version de l'application après la mise à jour technique ;
- Le lien vers le fichier de la mise à jour.

Vous aurez le choix entre les actions suivantes :

- **Oui, installer** : installe la mise à jour.

  Après l'installation de la mise à jour, il faut redémarrer le système d'exploitation.

- **Reporter l'installation** : reporte l'installation.

Pour que les notifications sur cette mise à jour n'affichent plus, cochez la case ☑ **Ne pas demander jusqu'à l'apparition de la nouvelle version**.

## NOTIFICATIONS DANS LE MODE DE PROTECTION INTERACTIF

Cette rubrique reprend les notifications qui apparaissent uniquement pendant l'utilisation de l'application en mode de protection interactif (cf. section "Sélection du mode de protection" à la page 74). Si vous ne souhaitez pas que ces notifications apparaissent, passez en mode de protection automatique. Dans ce cas, seules les notifications dont l'affichage est prévu dans n'importe quel mode de protection (cf. section "Notifications dans n'importe quel mode de protection" à la page 205) apparaîtront.

### DANS CETTE SECTION



## UNE ACTIVITE RESEAU DE L'APPLICATION A ETE DECOUVERTE

Lors de la détection de l'activité de réseau de l'application (par défaut, pour les applications incluses dans le groupe **Restrictions faibles** ou **Restrictions élevées**) une notification apparaîtra sur votre écran.

La notification s'affichera, si Kaspersky Internet Security fonctionne en mode interactif (cf. section "Sélection du mode de protection" à la page 74), et si aucune règle pour les paquets (cf. page 125) n'a été créée pour l'application dont l'activité de réseau a été détectée.

La notification contient les informations suivantes :

- Nom de l'application et brève description de la connexion qu'elle établit ;
- Informations sur la connexion (type de connexion, port distant et local, adresse à partir d'où la connexion est établie) ;
- Séquence de lancement de l'application.

Vous aurez le choix entre les actions suivantes :

- **Autoriser maintenant**.
- **Interdire maintenant**.
- **Créer une règle**. Le choix de cette option entraîne l'ouverture de la fenêtre **Pare-feu** qui permet de créer une règle qui régit l'activité de réseau de l'application (cf. section "Création de règles pour l'application" à la page 125).

Vous pouvez interdire ou autoriser l'activité de réseau de l'application d'une des manières suivantes :

- Exécuter l'action une seule fois. Pour ce faire, sélectionnez l'action **Autoriser maintenant** ou **Interdire maintenant**.
- Enregistrer l'action pour la session de l'application qui manifeste une activité de réseau. Pour ce faire, sélectionnez **Autoriser maintenant** ou **Interdire maintenant** et cochez la case **Enregistrer pour la session de l'application**.
- Enregistrer pour toujours l'action sélectionnée pour l'application. Pour ce faire, sélectionnez l'action **Autoriser maintenant** ou **Interdire maintenant** et cochez la case **Enregistrer pour toujours**.
- Créer une règle pour régir l'activité de réseau de l'application. Pour ce faire, sélectionnez l'action **Créer une règle**.

## UN OBJET MALVEILLANT A ETE IDENTIFIE

Lorsque l'Antivirus Fichiers, l'Antivirus Courrier ou une tâche d'analyse découvre un objet malveillant, un message apparaît.

Le message reprend les informations suivantes :

- La description de la menace.
- Le type de la menace et le nom de l'objet malveillant tel que repris dans l'Encyclopédie des virus de Kaspersky Lab.

  L'icône s'affiche à côté du nom de l'objet malveillant. Cliquez sur cette icône pour ouvrir la fenêtre contenant les informations sur l'objet. Le lien //www.viruslist.com/fr dans la fenêtre permet d'accéder au site Web de l'Encyclopédie des virus et d'obtenir des informations plus précises sur une menace.
- Le nom du fichier de l'objet malveillant, y compris son chemin d'accès.

Vous aurez le choix entre les actions suivantes :

- **Réparer** : tentative de réparation de l'objet malveillant. Une copie de sauvegarde est créée avant la réparation au cas où il faudrait restaurer l'objet ou le scénario de l'infection.
- **Supprimer** : supprime l'objet malveillant. Une copie de sauvegarde de l'objet est créée avant la suppression au cas où il faudrait le restaurer ou reproduire le scénario de l'infection.
- **Ignorer/Bloquer** : bloque l'accès à l'objet mais n'exécute aucune action sur ce dernier. L'application se contente de consigner les informations relatives à l'objet dans le rapport.

  Vous pourrez revenir au traitement des objets malveillants ignorés au départ de la fenêtre du rapport (le traitement différé d'un objet n'est pas possible lorsque l'objet découvert est joint à un message électronique).

Pour appliquer l'action sélectionnée à tous les objets portant le même état découverts dans la session en cours du composant de la protection ou de la tâche, cochez la case **Appliquer à tous les objets**. Par session en cours, il faut entendre la durée de fonctionnement du composant depuis son lancement jusqu'à son arrêt ou jusqu'au redémarrage de l'application ainsi que la durée de l'exécution de la tâche de recherche de virus depuis son lancement jusque sa fin.

## UNE VULNERABILITE A ETE DECOUVERTE

En cas de découverte d'une vulnérabilité au cours de l'exécution de la tâche de recherche de virus, une notification apparaît.

Elle contient les informations suivantes :

- La description de la vulnérabilité.
- Le nom de la vulnérabilité, tel qu'il figure dans l'Encyclopédie des virus de Kaspersky Lab.

  L'icône s'affiche à côté du nom. Cliquez sur cette icône pour ouvrir la fenêtre contenant les informations sur la vulnérabilité. Le lien //www.viruslist.com/fr dans la fenêtre permet d'accéder au site Web de l'Encyclopédie des virus et d'obtenir des informations plus précises sur une vulnérabilité.
- Le nom du fichier de l'objet vulnérable, y compris son chemin d'accès.

Vous aurez le choix entre les actions suivantes :

- **Oui, corriger** : supprime la vulnérabilité.
- **Ignorer** : n'exécute aucune action sur l'objet vulnérable.

## DEMANDE D'AUTORISATION DES ACTIONS DE L'APPLICATION

Quand une application tente d'exécuter une action quelconque dont le danger ou la nécessité est inconnue de Kaspersky Internet Security, une notification apparaît.

Le message reprend les informations suivantes :

- Le nom de l'application et icône . Cliquez sur cette icône pour ouvrir la fenêtre contenant les informations sur l'application.
- La description des actions de l'application.
- L'emplacement du fichier de l'application.
- La séquence de lancement de l'application.

Vous pouvez autoriser ou interdire l'exécution de l'application en choisissant une des options suivantes:

- **Rendre fiable** : place l'application dans le groupe des applications de confiance pour que son exécution soit toujours autorisée.
- **Autoriser maintenant** : autorise une fois l'exécution de l'application.
- **Interdire maintenant** : interdit une fois l'exécution de l'application.
- **Terminer l'application et appliquer l'état douteux** : place l'application dans le groupe des applications douteuses afin de toujours interdire son exécution.

## UNE ACTIVITE DANGEREUSE A ETE DECOUVERTE DANS LE SYSTEME

Lorsque la Défense Proactive découvre une activité dangereuse en provenance d'une application quelconque du système, un message spécial apparaît.

La notification contient les informations suivantes :

- La description de la menace.

- Le type de la menace et le nom de l'objet malveillant tel que repris dans l'Encyclopédie des virus de Kaspersky Lab.

  L'icône s'affiche à côté du nom de l'objet malveillant. Cliquez sur cette icône pour ouvrir la fenêtre contenant les informations sur l'objet. Le lien //www.viruslist.com/fr dans la fenêtre permet d'accéder au site Web de l'Encyclopédie des virus et d'obtenir des informations plus précises sur une menace.

- L'identificateur du processus et le nom du fichier de l'application, y compris le chemin d'accès.

Choisissez l'une des options suivantes :

- **Quarantaine** : quitte l'application ; place le fichier de l'application en quarantaine où il ne constituera pas de menace pour la sécurité de votre ordinateur.

  Lors des analyses suivantes de la quarantaine, l'état de l'objet peut se modifier. Par exemple, l'objet peut être identifié comme étant infecté et traité à l'aide de bases actualisées ou il peut recevoir l'état *sain* et dans ce cas, il pourra être restauré.

  En cas de mise en quarantaine manuelle d'un fichier qui lors de l'analyse suivante ne sera pas considéré comme infecté, son état deviendra *ok* uniquement si le fichier est analysé dans les trois jours maximum après la mise en quarantaine.

- **Terminer** : interrompt l'exécution de l'application.

- **Autoriser** : autorise l'exécution de l'application.

Pour appliquer l'action sélectionnée à tous les objets portant le même état découverts dans la session en cours de la Défense Proactive, cochez la case **Appliquer à tous les cas identiques**. La session de fonctionnement en cours d'un composant désigne la période entre le moment où il a été lancé et le moment où il est arrêté ou redémarré.

Si vous êtes convaincu que l'application découverte ne représente aucun danger, il est conseillé de l'ajouter à la zone de confiance pour éviter un nouveau déclenchement de Kaspersky Internet Security.

## REMISE A L'ETAT ANTERIEUR AUX MODIFICATIONS INTRODUITES PAR L'APPLICATION DANGEREUSE

Quand l'exécution de l'application potentiellement dangereuse se termine, il est conseillé de revenir à l'état antérieur aux modifications introduites dans le système (annuler les modifications). Dans ce cas, une notification de la demande de retour à l'état antérieur aux modifications apparaît.

Le message reprend les informations suivantes :

- La demande de retour à l'état antérieur aux modifications exécutées par l'application potentiellement dangereuse.

- Le type d'application et son nom.

  L'icône s'affiche à côté du nom de l'application. Cliquez sur cette icône pour ouvrir la fenêtre contenant les informations sur l'application.

- L'identificateur du processus et le nom du fichier de l'application, y compris le chemin d'accès.

Choisissez l'une des options suivantes :

- **Oui, restaurer** : tente d'annuler les modifications introduites par l'application.

- **Ignorer** : n'annule pas les modifications.

## UN PROGRAMME MALVEILLANT A ETE DECOUVERT

Quand la Surveillance du système découvre une application dont le comportement correspond parfaitement à celui d'un programme malveillant, une notification apparaît.

Le message reprend les informations suivantes :

- La description de la menace.
- Le type de programme malveillant et son nom.

  L'icône s'affiche à côté du nom de l'application. Cliquez sur cette icône pour ouvrir la fenêtre contenant les informations sur l'application.
- L'identificateur du processus et le nom du fichier de l'application, y compris le chemin d'accès.
- Le lien vers la fenêtre avec l'historique d'apparition de l'application.

Choisissez l'une des options suivantes :

- **Quarantaine** : quitte l'application ; place le fichier de l'application en quarantaine où il ne constituera pas de menace pour la sécurité de votre ordinateur.

  Lors des analyses suivantes de la quarantaine, l'état de l'objet peut se modifier. Par exemple, l'objet peut être identifié comme étant infecté et traité à l'aide de bases actualisées ou il peut recevoir l'état *sain* et dans ce cas, il pourra être restauré.

  En cas de mise en quarantaine manuelle d'un fichier qui lors de l'analyse suivante ne sera pas considéré comme infecté, son état deviendra *ok* uniquement si le fichier est analysé dans les trois jours maximum après la mise en quarantaine.
- **Terminer** : interrompt l'exécution de l'application.
- **Autoriser** : autorise l'exécution de l'application.

## UN LIEN SUSPECT/MALVEILLANT A ETE DECOUVERT

Quand Kaspersky Internet Security détecte une tentative d'ouverture d'un site Web au contenu malveillant ou suspect, une notification spéciale s'affiche sur l'écran.

Le message reprend les informations suivantes :

- La description de la menace ;
- Le nom de l'application (du navigateur) à l'aide de laquelle le chargement du site Web est exécuté ;
- L'adresse du site ou de la page au contenu malveillant ou suspect.

Choisissez l'une des options suivantes :

- **Autoriser** : poursuit le chargement du site Web.
- **Interdire** : bloque le chargement du site Web.

Pour appliquer l'action sélectionnée à tous les sites Web portant le même état découverts dans la session en cours du composant de la protection, cochez la case **Appliquer à tous les objets**. La session de fonctionnement en cours d'un composant désigne la période entre le moment où il a été lancé et le moment où il est arrêté ou redémarré.

## UN OBJET DANGEREUX A ETE DECOUVERT DANS LE TRAFIC

Lorsque l'Antivirus Internet découvre un objet dangereux dans le trafic, un message spécial s'affiche.

La notification contient les informations suivantes :

- La description de la menace ou des actions exécutées par l'application.
- Le nom de l'application en action.
- Le type de la menace et le nom de l'objet malveillant tel que repris dans l'Encyclopédie des virus de Kaspersky Lab.

  L'icône s'affiche à côté du nom de l'objet malveillant. Cliquez sur cette icône pour ouvrir la fenêtre contenant les informations sur l'objet. Le lien //www.viruslist.com/fr dans la fenêtre permet d'accéder au site Web de l'Encyclopédie des virus et d'obtenir des informations plus précises sur une menace.
- Emplacement de l'objet (adresse URL).

Vous aurez le choix entre les actions suivantes :

- **Autoriser** : continue à télécharger l'objet.
- **Interdire** : bloque le téléchargement de l'objet depuis le site Internet.

Pour appliquer l'action sélectionnée à tous les objets portant le même état découverts dans la session en cours du composant de la protection ou de la tâche, cochez la case **Appliquer à tous les objets**. Par session en cours, il faut entendre la durée de fonctionnement du composant depuis son lancement jusqu'à son arrêt ou jusqu'au redémarrage de l'application ainsi que la durée de l'exécution de la tâche de recherche de virus depuis son lancement jusque sa fin.

## UNE TENTATIVE DE CONNEXION A UN SITE DE PHISHING A ETE DECOUVERTE

Quand Kaspersky Internet Security détecte une tentative de connexion à un site qui est un site de phishing confirmé ou potentiel, une notification apparaît.

Le message reprend les informations suivantes :

- La description de la menace ;
- L'adresse du site Web.

Vous aurez le choix entre les actions suivantes :

- **Autoriser** : poursuit le chargement du site Web.
- **Interdire** : bloque le chargement du site Web.

Pour appliquer l'action sélectionnée à tous les sites Web portant le même état découverts dans la session en cours de Kaspersky Internet Security, cochez la case **Appliquer à tous les objets**. La session de fonctionnement en cours d'un composant désigne la période entre le moment où il a été lancé et le moment où il est arrêté ou redémarré.

## UNE TENTATIVE D'ACCES A LA BASE DE REGISTRES SYSTEME A ETE DECOUVERTE

Quand la Défense Proactive découvre une tentative d'accès aux clés de la base de registres système, une notification apparaît.

Le message reprend les informations suivantes :

- La clé du registre victime de la tentative d'accès ;
- Le nom du fichier ou du processus à l'origine de la tentative d'accès à la base de registres, y compris le chemin d'accès à celui-ci.

Vous aurez le choix entre les actions suivantes :

- **Autoriser** : autorise une fois l'exécution de l'action dangereuse ;
- **Interdire** : bloque une fois l'exécution de l'action dangereuse.

Pour que l'action que vous choisissez soit exécutée automatiquement chaque fois que cette activité sera lancée sur l'ordinateur, cochez la case **Créer une règle**.

Si vous estimez que l'activité de l'application qui a envoyé une requête aux clés de la base de registre système n'est pas dangereuse, ajoutez-la à la liste des applications de confiance.

## OBJET SUSPECT DETECTE

Quand l'Antivirus Fichiers, l'Antivirus Courrier ou une tâche d'analyse d'un objet découvre le code d'un virus inconnu ou le code modifié d'un virus connu, une notification apparaît.

Le message reprend les informations suivantes :

- La description de la menace.
- Le type de la menace et le nom de l'objet malveillant tel que repris dans l'Encyclopédie des virus de Kaspersky Lab.

  L'icône s'affiche à côté du nom de l'objet malveillant. Cliquez sur cette icône pour ouvrir la fenêtre contenant les informations sur l'objet. Le lien //www.viruslist.com/fr dans la fenêtre permet d'accéder au site Web de l'Encyclopédie des virus et d'obtenir des informations plus précises sur une menace.
- Le nom du fichier de l'objet malveillant, y compris son chemin d'accès.

Vous aurez le choix entre les actions suivantes :

- **Quarantaine** : place l'objet en quarantaine où il ne constituera plus un danger pour votre ordinateur.

  Lors des analyses suivantes de la quarantaine, l'état de l'objet peut se modifier. Par exemple, l'objet peut être identifié comme étant infecté et traité à l'aide de bases actualisées ou il peut recevoir l'état *sain* et dans ce cas, il pourra être restauré.

  > En cas de mise en quarantaine manuelle d'un fichier qui lors de l'analyse suivante ne sera pas considéré comme infecté, son état deviendra *ok* uniquement si le fichier est analysé dans les trois jours maximum après la mise en quarantaine.
- **Supprimer** : supprime l'objet malveillant. Une copie de sauvegarde de l'objet est créée avant la suppression au cas où il faudrait le restaurer ou reproduire le scénario de l'infection.
- **Ignorer/Bloquer** : bloque l'accès à l'objet mais n'exécute aucune action sur ce dernier. L'application se contente de consigner les informations relatives à l'objet dans le rapport.

  Vous pourrez revenir au traitement des objets malveillants ignorés au départ de la fenêtre du rapport (le traitement différé d'un objet n'est pas possible lorsque l'objet découvert est joint à un message électronique).

Pour appliquer l'action sélectionnée à tous les objets portant le même état découverts dans la session en cours du composant de la protection ou de la tâche, cochez la case **Appliquer à tous les objets**. Par session en cours, il faut

entendre la durée de fonctionnement du composant depuis son lancement jusqu'à son arrêt ou jusqu'au redémarrage de l'application ainsi que la durée de l'exécution de la tâche de recherche de virus depuis son lancement jusque sa fin.

Si vous êtes convaincu que l'objet découvert n'est pas malveillant, il est conseillé de l'ajouté à la zone de confiance afin d'éviter une nouvelle réaction de l'application.

## LA REPARATION DE L'OBJET EST IMPOSSIBLE

Dans certains cas, il est impossible de réparer l'objet malveillant : par exemple, si le fichier est endommagé à un tel point qu'il est impossible d'en supprimer le code malveillant ou de le restaurer complètement. De plus, il existe certains types d'objets malveillants comme les chevaux de Troie qui ne peuvent pas être réparés. Dans ce cas, une notification apparaît.

Le message reprend les informations suivantes :

- La description de la menace.
- Le type de la menace et le nom de l'objet malveillant tel que repris dans l'Encyclopédie des virus de Kaspersky Lab.

  L'icône s'affiche à côté du nom de l'objet malveillant. Cliquez sur cette icône pour ouvrir la fenêtre contenant les informations sur l'objet. Le lien //www.viruslist.com/fr dans la fenêtre permet d'accéder au site Web de l'Encyclopédie des virus et d'obtenir des informations plus précises sur une menace.
- Le nom du fichier de l'objet malveillant, y compris son chemin d'accès.

Vous aurez le choix entre les actions suivantes :

- **Supprimer** : supprime l'objet malveillant. Une copie de sauvegarde de l'objet est créée avant la suppression au cas où il faudrait le restaurer ou reproduire le scénario de l'infection.
- **Ignorer/Bloquer** : bloque l'accès à l'objet mais n'exécute aucune action sur ce dernier. L'application se contente de consigner les informations relatives à l'objet dans le rapport.

  Vous pourrez revenir au traitement des objets malveillants ignorés au départ de la fenêtre du rapport (le traitement différé d'un objet n'est pas possible lorsque l'objet découvert est joint à un message électronique).

Pour appliquer l'action sélectionnée à tous les objets portant le même état découverts dans la session en cours du composant de la protection ou de la tâche, cochez la case **Appliquer à tous les objets**. Par session en cours, il faut entendre la durée de fonctionnement du composant depuis son lancement jusqu'à son arrêt ou jusqu'au redémarrage de l'application ainsi que la durée de l'exécution de la tâche de recherche de virus depuis son lancement jusque sa fin.

## DETECTION DE PROCESSUS CACHES

Quand la Défense Proactive découvre un processus caché dans le système, une notification apparaît.

Le message reprend les informations suivantes :

- La description de la menace.
- Le type de la menace et le nom de l'objet malveillant tel que repris dans l'Encyclopédie des virus de Kaspersky Lab.

  L'icône s'affiche à côté du nom. Cliquez sur cette icône pour ouvrir la fenêtre contenant les informations sur la menace. Le lien //www.viruslist.com/fr dans la fenêtre permet d'accéder au site Web de l'Encyclopédie des virus et d'obtenir des informations plus précises sur la menace.
- Le nom du fichier du pilote, y compris son chemin d'accès.

Vous aurez le choix entre les actions suivantes :

- **Quarantaine** : quitte l'application ; place le fichier du processus en quarantaine où il ne constituera pas de menace pour la sécurité de votre ordinateur.

  Lors des analyses suivantes de la quarantaine, l'état de l'objet peut se modifier. Par exemple, l'objet peut être identifié comme étant infecté et traité à l'aide de bases actualisées ou il peut recevoir l'état *sain* et dans ce cas, il pourra être restauré.

  En cas de mise en quarantaine manuelle d'un fichier qui lors de l'analyse suivante ne sera pas considéré comme infecté, son état deviendra *ok* uniquement si le fichier est analysé dans les trois jours maximum après la mise en quarantaine.

- **Terminer** : interrompt le processus.

- **Autoriser** : autorise l'exécution du processus.

Pour appliquer l'action sélectionnée à tous les processus cachés portant le même état découverts dans la session en cours de la Défense Proactive, cochez la case **Appliquer à tous les cas identiques**. La session de fonctionnement en cours d'un composant désigne la période entre le moment où il a été lancé et le moment où il est arrêté ou redémarré.

Si vous êtes convaincu que le processus découvert ne représente aucun danger, il est conseillé de l'ajouter à la zone de confiance pour éviter un nouveau déclenchement de Kaspersky Internet Security.

## LE FILTRAGE PAR GEO LOCALISATION A BLOQUE LA DEMANDE D'ACCES AU SITE

La connexion au site Web peut être interdite par l'Antivirus Internet puisque ce site appartient au domaine régional. Le domaine est considéré comme interdit dans les cas suivants :

- L'utilisateur a interdit la consultation du domaine dans la configuration de l'Antivirus Internet ;

- La dernière connexion à un site de cette région à été interdite par l'utilisateur.

Quand le filtrage par géo localisation (le module de l'Antivirus Internet) détecte une tentative d'ouverture d'un site Web appartenant à une région interdite, une notification s'affiche dans la fenêtre du navigateur.

Le message reprend les informations suivantes :

- La description de la raison du blocage de la connexion au site ;

- Le nom de la région à laquelle le site appartient ;

- Le domaine et les caractéristiques du niveau d'infection des sites Web dans ce domaine ;

- L'adresse du site Web.

Choisissez l'une des options suivantes :

- **Revenir à la page précédente** : ouvre la page précédente.

- **Ouvrir le site** : charge le site appartenant au domaine interdit.

- **Ouvrir la configuration du Filtrage par géo localisation** : ouvre la fenêtre de configuration de l'Antivirus Internet sous l'onglet **Filtrage par géo localisation**.

## LA NAVIGATION SECURISEE A BLOQUE LE CHARGEMENT DU SITE

Quand la navigation sécurisée (le module de l'Antivirus Internet) détecte une tentative d'ouverture d'un site dangereux, une notification s'affiche dans la fenêtre du navigateur.

Le message reprend les informations suivantes :

- La description de la raison du blocage de la connexion au site ;
- L'adresse du site Web.

Choisissez l'une des options suivantes :

- **Revenir à la page précédente** : ouvre la page précédente.
- **Ouvrir malgré tout** : charge le site, malgré le danger qu'il représente.

## LA NAVIGATION SECURISEE A SUSPENDU LE CHARGEMENT DU SITE

Quand la navigation sécurisée (le module de l'Antivirus Internet) détecte une tentative de connexion à un site dont la sécurité n'est pas certaine, une notification apparaît.

Le message reprend les informations suivantes :

- La description de la raison de la suspension de la connexion au site ;
- L'adresse du site Web.

Choisissez l'une des options suivantes :

- **Oui, ouvrir le site** : charge le site.
- **Ouvrir et ajouter aux adresses de confiance** : charge le site et son adresse est ajoutée à la liste des adresses de confiance pour que la navigation sécurisée ne suspende plus son chargement à l'avenir.
- **Ouvrir dans le Navigateur protégé** : charge le site web dans le Navigateur protégé (uniquement pour les navigateurs Microsoft Internet Explorer, Mozilla Firefox et Google Chrome). Lors du téléchargement dans le Navigateur protégé, les objets malveillants (s'ils sont présents dans les pages à télécharger) ne présenteront aucun danger pour la sécurité de l'ordinateur.
- **Non et revenir à la page précédente** : ne télécharge pas le site Web, mais ouvre la page précédente.

## IL EST CONSEILLE DE PASSER A LA NAVIGATION DANS L'ENVIRONNEMENT PROTEGE

L'utilisateur qui emploie des services de transactions bancaires en ligne a besoin d'une protection particulière car dans ce cas-ci, la fuite d'informations confidentielles peut entraîner des pertes financières. C'est pourquoi, pour l'utilisation des services de transactions bancaires en ligne, Kaspersky Lab recommande d'utiliser le mode du navigateur protégé qui garantit une protection élevée de vos données personnelles.

Lors de la tentative de la connexion au site web des services de transactions bancaires en ligne, l'Antivirus Internet affiche une notification dans la fenêtre du navigateur.

Le message reprend les informations suivantes :

- La recommandation de passer au mode de la navigation sur les sites Web en mode protégé ;
- L'adresse de la ressource des services de transactions bancaires en ligne.

Vous aurez le choix entre les actions suivantes :

- **Navigation sur les sites web en mode protégé** : ouvre le site web en utilisant le mode du navigateur protégé (uniquement pour les navigateurs Microsoft Internet Explorer, Mozilla Firefox et Google Chrome).
- **Ouvrir le site** : ouvre le site web en mode normal.
- **Revenir à la page précédente** : ouvre la page précédente en mode normal.

### IL EST CONSEILLE DE QUITTER LA NAVIGATION DANS L'ENVIRONNEMENT PROTEGE

Quand vous utilisez un site web de transactions bancaires en ligne en mode du navigateur protégé et que vous passez à un autre site web sans rapport avec les transactions bancaires en ligne, il est conseillé de quitter le mode du navigateur protégé. L'utilisation du site web ordinaire en mode du navigateur protégé peut affaiblir la protection de vos données personnelles.

Lors de la tentative de connexion à un autre site web depuis le site web de transactions bancaires en ligne en mode du navigateur protégé, l'Antivirus Internet affiche une notification dans la fenêtre du navigateur.

Le message reprend les informations suivantes :

- La recommandation de quitter le mode du navigateur protégé ;
- L'adresse du site web auquel vous vous connectez depuis le site web de transactions bancaires en ligne.

Vous aurez le choix entre les actions suivantes :

- **Ouvrir le site dans le navigateur normal** : quitte le mode du navigateur protégé et ouvre le site web, sans rapport avec les transactions bancaires en ligne, en mode normal.
- **Poursuivre en mode du navigateur protégé** : ouvre le site web, sans rapport avec les transactions bancaires en ligne, en mode du navigateur protégé.
- **Revenir à la page précédente** : ouvre la page précédente en mode du navigateur protégé.

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

Vous pouvez utiliser Kaspersky Internet Security à l'aide de la ligne de commande. Ce mode vous permet d'exécuter les opérations suivantes :

- Activation de l'application ;
- Lancement et arrêt de l'application ;
- Lancement et arrêt des composants de l'application ;
- Lancement et arrêt des tâches ;
- Obtention d'informations relatives à l'état actuel des composants et aux tâches et à leur statistiques ;
- lancement et arrêt de l'exécution des tâches d'analyse antivirus ;
- Analyse des objets sélectionnés ;
- Mise à jour des bases et des modules de l'application, retour à l'état antérieur à la mise à jour ;

- Exportation et importation des paramètres de la protection ;
- Affichage de l'aide sur la syntaxe de la ligne de commande pour l'ensemble des instructions ou pour des instructions individuelles.

Syntaxe de la ligne de commande :

```
avp.com <instruction> [paramètres]
```

La requête adressée à l'application via la ligne de commande doit être réalisée depuis le répertoire d'installation du logiciel ou en indiquant le chemin d'accès complet à avp.com.

La liste des instructions utilisées pour l'administration de l'application et de ses composants est reprise dans le tableau ci-dessous.

| | |
|---|---|
| **START** | Lancement du composant ou de la tâche |
| **STOP** | Arrêt du composant ou de la tâche (l'exécution de l'instruction est possible uniquement après saisie du mot de passe défini via l'interface de Kaspersky Internet Security) |
| **STATUS** | Affichage de l'état actuel du composant ou de la tâche |
| **STATISTICS** | Affichage des statistiques du composant ou de la tâche |
| **HELP** | Affichage de la liste des instructions et des informations sur la syntaxe de l'instruction |
| **SCAN** | Recherche d'éventuels virus dans les objets |
| **UPDATE** | Lancement de la mise à jour de l'application |
| **ROLLBACK** | annulation de la dernière mise à jour réalisée (l'exécution de l'instruction est possible uniquement après saisie du mot de passe défini via l'interface de Kaspersky Internet Security) |
| **EXIT** | Arrêt du logiciel (l'exécution de l'instruction est possible uniquement avec la saisie du mode passe défini via l'interface de l'application) |
| **IMPORT** | Importation des paramètres de protection de Kaspersky Internet Security (l'exécution de l'instruction est possible uniquement après saisie du mot de passe défini via l'interface de l'application) |
| **EXPORT** | Exportation des paramètres de la protection de l'application |

Chaque instruction possède ses propres paramètres, propres à chaque composant de l'application.

**DANS CETTE SECTION**



# ACTIVATION DE L'APPLICATION

Kaspersky Internet Security peut être activé à l'aide du fichier de licence.

Syntaxe de l'instruction :

```
avp.com ADDKEY <nom_du_fichier>
```

La description des paramètres d'exécution de l'instruction est reprise dans le tableau ci-dessous.

| | |
|---|---|
| **<nom_du_fichier>** | Nom du fichier de licence avec l'extension *.key |

**Exemple :**

```
avp.com ADDKEY 1AA111A1.key
```

# LANCEMENT DE L'APPLICATION

Syntaxe de l'instruction :

```
avp.com
```

# ARRET DE L'APPLICATION

Syntaxe de l'instruction :

```
avp.com EXIT /password=<votre_mot_de_passe>
```

La description des paramètres est reprise dans le tableau ci-dessous.

| | |
|---|---|
| **<votre_mot_de_passe>** | Mot de passe d'accès à l'application, défini dans l'interface |

N'oubliez pas que l'instruction ne s'exécutera pas sans la saisie du mot de passe.

## ADMINISTRATION DES COMPOSANTS DE L'APPLICATION ET DES TACHES

Syntaxe de l'instruction :

```
avp.com <instruction> <profil|nom_de_la_tâche> [/R[A]:<fichier_de_rapport>]
avp.com STOP <profil|nom_de_la_tâche> /password=<votre_mot_de_passe>
[/R[A]:<fichier_de_rapport>]
```

Les instructions et les paramètres sont décrits dans le tableau ci-après.

| | |
|---|---|
| **<instruction>** | L'administration des composants et des tâches de Kaspersky Internet Security via la ligne de commande s'opère à l'aide des instructions suivantes :<br>START : lancement du composant de la protection en temps réel ou d'une tâche.<br>STOP : arrêt du composant de la protection en temps réel ou d'une tâche.<br>STATUS : affichage de l'état actuel du composant de la protection ou d'une tâche.<br>STATISTICS : affichage des statistiques du composant de la protection ou d'une tâche.<br>N'oubliez pas que l'instruction STOP ne peut être exécutée sans la saisie préalable du mot de passe. |
| **<profil\|nom_de_la_tâche>** | En guise de valeur pour le paramètre **<profil>**, vous pouvez indiquer n'importe quel composant de la protection en temps réel de Kaspersky Internet Security ainsi que les modules qui sont repris dans les composants des tâches d'analyse à la demande ou de mise à jour composées (les valeurs standard utilisées par l'application sont reprises dans le tableau ci-après).<br><br>En guise de valeur pour le paramètre **<nom_de_la_tâche>**, vous pouvez indiquer le nom de n'importe quelle tâche d'analyse à la demande ou de mise à jour configurée par l'utilisateur. |
| **<votre_mot_de_passe>** | Mot de passe d'accès à l'application, défini dans l'interface. |
| **/R[A]:<fichier_de_rapport>** | **/R:<fichier_de_rapport>** : consigner dans le rapport uniquement les événements importants.<br>**/RA:<fichier_de_rapport>** : consigner tous les événements dans le rapport.<br>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. |

Le paramètre **<profil>** prend une des valeurs du tableau ci-après.

| | |
|---|---|
| **RTP** | Tous les composants de la protection.<br>L'instruction **avp.com START RTP** lance tous les composants de la protection, si la protection avait été arrêtée.<br>Si le composant a été arrêté via l'instruction **STOP** de la ligne de commande, il ne pourra être redémarré via l'instruction **avp.com START RTP**. Pour ce faire, il faut exécuter la commande **avp.com START <profil>** où le paramètre **<profil>** représente un composant concret de la protection, par exemple **avp.com START FM**. |
| **FW** | Pare-feu. |
| **HIPS** | Contrôle des Applications. |
| **pdm** | Défense Proactive. |

| | |
|---|---|
| **FM** | Antivirus Fichiers. |
| **EM** | Antivirus Courrier. |
| **WM** | Antivirus Internet.<br>Valeurs pour les sous-composants de l'Antivirus Internet :<br>**httpscan (HTTP)** : analyse du trafic HTTP ;<br>**sc** : analyse des scripts. |
| **IM** | Antivirus IM ("Chat"). |
| **AB** | Anti-bannière. |
| **AS** | Anti-Spam. |
| **PC** | Contrôle Parental. |
| **AP** | Anti-Phishing. |
| **ids** | Prévention des intrusions. |
| **Updater** | Mise à jour. |
| **Rollback** | Annulation de la dernière mise à jour. |
| **Scan_My_Computer** | Analyse de l'ordinateur. |
| **Scan_Objects** | Analyse des objets. |
| **Scan_Quarantine** | Analyse de la quarantaine. |
| **Scan_Startup (STARTUP)** | Analyse des objets de démarrage. |
| **Scan_Vulnerabilities (SECURITY)** | Recherche de vulnérabilités. |

Les composants et les tâches lancés via la ligne de commande sont exécutés selon les paramètres définis dans l'interface du logiciel.

**Exemples** :

- *Pour activer l'Antivirus Fichiers, saisissez l'instruction :*

```
avp.com START FM
```

- *Pour arrêter l'analyse de l'ordinateur, saisissez l'instruction :*

```
avp.com STOP Scan_My_Computer /password=<votre_mot_de_passe>
```

# RECHERCHE DE VIRUS

La ligne de commande utilisée pour lancer l'analyse antivirus d'un secteur quelconque et pour lancer le traitement des objets malveillants découverts ressemble à ceci :

```
avp.com SCAN [<objet à analyser>] [<action>] [<types de fichiers>] [<exclusions>]
[<fichier de configuration>] [<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. Dans ce cas, la tâche sera réalisée selon les paramètres définis dans l'interface de Kaspersky Internet Security.

La description des paramètres est reprise dans le tableau ci-dessous.

| | |
|---|---|
| **<objet à analyser>** : ce paramètre définit la liste des objets qui seront soumis à la recherche de code malveillant.<br>Il peut contenir plusieurs des valeurs de la liste ci-après, séparées par un espace. | |
| **<files>** | Liste des chemins d'accès aux fichiers et aux répertoires à analyser.<br><br>La saisie d'un chemin relatif ou absolu est autorisée. Les éléments de la liste doivent être séparés par un espace.<br><br>Remarques :<br>• Mettre le nom de l'objet entre guillemets s'il contient un espace ;<br>• Lorsqu'un répertoire particulier a été défini, l'analyse porte sur tous les fichiers qu'il contient. |
| **/MEMORY** | Objets de la mémoire vive. |
| **/STARTUP** | Objets de démarrage. |
| **/MAIL** | Boîtes aux lettres. |
| **/REMDRIVES** | Tous les disques amovibles. |
| **/FIXDRIVES** | Tous les disques locaux. |
| **/NETDRIVES** | Tous les disques de réseau. |
| **/QUARANTINE** | Objets en quarantaine. |
| **/ALL** | Analyse complète de l'ordinateur. |
| **/@:<filelist.lst>** | Chemin d'accès au fichier de la liste des objets et répertoires inclus dans l'analyse. La saisie d'un chemin d'accès relatif ou absolu au fichier est autorisée. Le chemin doit être saisi sans guillemets, même s'il contient un espace.<br><br>Le fichier contenant la liste des objets doit être au format texte. Chaque objet à analyser doit se trouver sur une nouvelle ligne.<br><br>Il est conseillé de saisir dans le fichier les chemins d'accès absolu aux objets à analyser. Si un chemin d'accès relatif est saisi, le chemin est indiqué par rapport au fichier exécutable de l'application et non pas par rapport au fichier contenant la liste des objets à analyser. |
| **<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**.<br>Si vous travaillez en mode automatique, alors Kaspersky Internet Security appliquera automatiquement l'action recommandée par les experts de Kaspersky Lab en cas de découverte d'objets dangereux. L'action définie par la valeur du paramètre **<action>** sera ignorée. | |
| **/i0** | Aucune action n'est exécutée, 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, supprimer les objets simples; ne pas supprimer les objets infectés au sein d'un conteneur (fichiers composés); supprimer les conteneurs avec un en-tête exécutable (archive fx). |

| | |
|---|---|
| **/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. |
| **/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. | |
| **/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.<br>Il peut contenir plusieurs des valeurs de la liste ci-après, séparées 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 plain text. |
| **-e:<filemask>** | Ne pas analyser les objets en fonction d'un masque. |
| **-e:<secondes>** | Ignorer les objets dont l'analyse dure plus que la valeur attribuée au paramètre **<secondes>**. |
| **-es:<taille>** | Ignorer les objets dont la taille (en Mo) est supérieure à la valeur définie par le paramètre **<taille>**.<br><br>Le paramètre s'applique uniquement aux fichiers composés (par exemple, aux archives). |
| Le paramètre **<fichier de configuration>** définit le chemin d'accès au fichier de configuration qui contient les paramètres utilisés par l'application pour l'analyse.<br>Le fichier de configuration est un fichier au format texte qui contient l'ensemble des paramètres de la ligne de commande pour l'analyse antivirus.<br>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. | |
| **/C:<nom_du_fichier>** | Utiliser les valeurs des paramètres définies dans le fichier de configuration **<nom_du_fichier>**. |
| Le paramètre **<paramètres du rapport>** définit le format du rapport sur les résultats de l'analyse.<br>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:<fichier_de_rapport>** | Consigner uniquement les événements importants dans le fichier indiqué. |
| **/RA:<fichier_de_rapport>** | Consigner tous les événements dans le fichier de rapport indiqué. |
| **<paramètres complémentaires>** : paramètres qui définissent l'utilisation de technologies de recherche de virus. | |
| **/iChecker=<on\|off>** | Active/désactive l'utilisation de la technologie iChecker. |
| **/iSwift=<on\|off>** | Active/désactive l'utilisation de la technologie iSwift. |

**Exemples** :

- *Lancer l'analyse de la mémoire vive, des objets de démarrage automatique, des boîtes aux lettres et des*

*répertoires My Documents, Program Files et du fichier test.exe :*

```
avp.com SCAN /MEMORY /STARTUP /MAIL "C:\Documents and Settings\All Users\My
Documents" "C:\Program Files" "C:\Downloads\test.exe"
```

- *Analyser les objets dont la liste est reprise dans le fichier object2scan.txt. Utiliser le fichier de configuration scan_setting.txt. À la fin de l'analyse, rédiger un rapport qui reprendra tous les événements :*

```
avp.com SCAN /MEMORY /@:objects2scan.txt /C:scan_settings.txt /RA:scan.log
```

Exemple de fichier de configuration :

```
/MEMORY /@:objects2scan.txt /C:scan_settings.txt /RA:scan.log
```

# MISE A JOUR DE L'APPLICATION

L'instruction pour la mise à jour des modules de Kaspersky Internet Security et des bases de l'application possède la syntaxe suivante :

```
avp.com UPDATE [<source_de_la_mise_à_jour>] [/R[A]:<fichier_de_rapport>]
[/C:<nom_du_fichier>]
```

La description des paramètres est reprise dans le tableau ci-dessous.

| | |
|---|---|
| **<source_de_la_mise_à_jour>** | Serveur HTTP, serveur FTP pou répertoire de réseau pour le chargement de la mise à jour. Ce paramètre accepte en tant que valeur le chemin d'accès complet à la source des mises à jour ou une URL. 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. |
| **/R[A]:<fichier_de_rapport>** | **/R:<fichier_de_rapport>** : consigner dans le rapport uniquement les événements importants.<br><br>**/RA:<fichier_de_rapport>** : consigner tous les événements dans le rapport.<br><br>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 ; portent sur tous les événements. |
| **/C:<nom_du_fichier>** | Chemin d'accès au fichier de configuration contenant les paramètres de fonctionnement de Kaspersky Internet Security pour la mise à jour.<br><br>Le fichier de configuration est un fichier au format texte qui contient l'ensemble des paramètres de la ligne de commande pour la mise à jour de l'application.<br><br>La saisie d'un chemin relatif ou absolu est autorisée. Si ce paramètre n'est pas défini, ce sont les valeurs des paramètres définies dans l'interface de l'application qui seront utilisées. |

**Exemples** :

- *Mettre à jour les bases de l'application et consigner tous les éléments dans le rapport :*

```
avp.com UPDATE /RA:avbases_upd.txt
```

- *Mettre à jour les modules de Kaspersky Internet Security en utilisant les paramètres du fichier de configuration updateapp.ini :*

```
avp.com UPDATE /C:updateapp.ini
```

Exemple de fichier de configuration :

```
"ftp://my_server/kav updates" /RA:avbases_upd.txt
```

# ANNULATION DE LA DERNIERE MISE A JOUR

Syntaxe de l'instruction :

```
avp.com ROLLBACK [/R[A]:<fichier_de_rapport>][/password=<votre_mot_de_passe>]
```

La description des paramètres est reprise dans le tableau ci-dessous.

| | |
|---|---|
| **/R[A]:<fichier_de_rapport>** | **/R:<fichier_de_rapport>** : consigner dans le rapport uniquement les événements importants.<br>**/RA:<fichier_de_rapport>** : consigner tous les événements dans le rapport.<br>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 ; portent sur tous les événements. |
| **<votre_mot_de_passe>** | Mot de passe d'accès à l'application, défini dans l'interface. |

N'oubliez pas que l'instruction ne s'exécutera pas sans la saisie du mot de passe.

**Exemple :**

```
avp.com ROLLBACK /RA:rollback.txt/password=<votre mot de passe>
```

# EXPORTATION DES PARAMETRES DE PROTECTION

Syntaxe de l'instruction :

```
avp.com EXPORT <profil> <nom_du_fichier>
```

La description des paramètres d'exécution de l'instruction est reprise dans le tableau ci-dessous.

| | |
|---|---|
| **<profil>** | Composant ou tâche dont les paramètres sont exportés.<br>Le paramètre **<profil>** peut prendre n'importe quelle des valeurs indiquées au point "Administration des composants de l'application et des tâches". |
| **<nom_du_fichier>** | Chemin d'accès au fichier vers lequel sont exportés les paramètres de Kaspersky Internet Security. Vous pouvez indiquer un chemin relatif ou absolu.<br>Le fichier de configuration est enregistré au format binaire (dat), si aucun autre format n'est indiqué ou si le format n'est pas précisé, et il peut être ensuite utilisé pour transférer les paramètres de l'application vers d'autres ordinateurs. De plus, vous pouvez enregistrer le fichier de configuration au format texte. Dans ce cas, ajoutez l'extension txt. N'oubliez pas que l'importation de paramètres de la protection depuis un fichier texte n'est pas prise en charge. Ce fichier peut être utilisé uniquement pour consulter les paramètres de fonctionnement principaux de Kaspersky Internet Security. |

**Exemple :**

```
avp.com EXPORT RTP c:\settings.dat
```

# IMPORTATION DES PARAMETRES DE PROTECTION

Syntaxe de l'instruction :

```
avp.com IMPORT <nom_du_fichier > [/password=< votre_mot_de_passe >
```

La description des paramètres d'exécution de l'instruction est reprise dans le tableau ci-dessous.

| | |
|---|---|
| **<nom_du_fichier>** | Chemin d'accès au fichier d'où sont importés les paramètres de Kaspersky Internet Security. Vous pouvez indiquer un chemin relatif ou absolu. |
| **<votre_mot_de_passe>** | Mot de passe pour Kaspersky Internet Security défini via l'interface de l'application. L'importation des paramètres de la protection est possible uniquement depuis un fichier au format binaire. |

N'oubliez pas que l'instruction ne s'exécutera pas sans la saisie du mot de passe.

**Exemple :**

```
avp.com IMPORT c:\settings.dat /password=<mot de passe>
```

## OBTENTION DU FICHIER DE TRACE

La création du fichier de trace s'impose parfois lorsque des problèmes se présentent dans le fonctionnement de Kaspersky Internet Security. Cela aidera les spécialistes du Service d'assistance technique à détecter plus précisément les problèmes.

Il est conseillé d'activer la création de ces fichiers uniquement pour le diagnostic d'un problème particulier. L'activation permanente de cette fonction peut entraîner une réduction des performances de l'ordinateur et un débordement du disque dur.

Syntaxe de l'instruction :

```
avp.com TRACE [file] [on|off] [<niveau_de_trace>]
```

La description des paramètres est reprise dans le tableau ci-dessous.

| | |
|---|---|
| **[on\|off]** | Active/désactive la création d'un fichier de trace. |
| **[file]** | Réception de la trace dans un fichier. |
| **<niveau_de_trace>** | Pour ce paramètre, il est possible de saisir un chiffre compris entre 0 (niveau minimum, uniquement les événements critiques) et 700 (niveau maximum, tous les messages).<br>Lorsque vous contactez le service d'assistance technique, l'expert doit vous préciser le niveau qu'il souhaite. Si le niveau n'a pas été indiqué, il est conseillé d'utiliser la valeur 500. |

**Exemples** :

- *Désactiver la constitution de fichiers de trace :*

```
avp.com TRACE file off
```

- *Créer un fichier de trace avec le niveau maximum de détails défini à 500 en vue d'un envoi à l'assistance technique :*

```
avp.com TRACE file on 500
```

## CONSULTATION DE L'AIDE

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

```
avp.com [ /? | HELP ]
```

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

```
avp.com <instruction> /?
avp.com HELP <instruction>
```

## CODES DE RETOUR DE LA LIGNE DE COMMANDE

Cette section décrit les codes de retour de la ligne de commande (dans le tableau ci-dessous). Les codes généraux peuvent être renvoyés par n'importe quelle instruction de la ligne de 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 GENERAUX | |
|---|---|
| **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 TACHES D'ANALYSE ANTIVIRUS** | |
| **101** | Tous les objets dangereux ont été traités |
| **102** | Des objets dangereux ont été découverts |

# GLOSSAIRE

## A

### Activation de l'application

La procédure d'activation de l'application consiste à saisir le code d'activation suite à la réception de la licence, ce qui permettra à l'application de définir les privilèges d'utilisation et la durée de validité de la licence.

### Analyse du trafic

Analyse en temps réel des objets transitant par tous les protocoles (exemple : HTTP, FTP etc.), à l'aide de la dernière version des bases.

### Analyseur heuristique

Technologie d'identification des menaces non reconnues par les bases de Kaspersky Anti-Virus. 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.

### Application incompatible

Application antivirus d'un autre éditeur ou application de Kaspersky Lab qui ne peut être administrée via Kaspersky Anti-Virus.

### Archive

Fichier qui contient un ou plusieurs autres objets qui peuvent être des archives.

### Attaque virale

Tentatives multiples d'infection d'un ordinateur par un virus.

## B

### Base des URL de phishing

Liste des URL de sites identifiés par les experts de Kaspersky Lab comme des sites de phishing. La base est actualisée régulièrement et elle est livrée avec l'application de Kaspersky Lab.

### Base des URL suspectes

Liste des URL de sites dont le contenu pourrait constituer une menace. La liste est composée par les experts de Kaspersky Lab. Elle est actualisée régulièrement et est livrée avec l'application de Kaspersky Lab.

### 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. Pour améliorer la qualité de la découverte de menaces, nous vous conseillons de télécharger fréquemment les mises à jour des bases depuis les serveurs de mise à jour de Kaspersky Lab.

### Bases de donnees de messagerie

Bases contenant les messages stockés sur votre ordinateur et possédant un format spécifique. Chaque message entrant/sortant est inscrit dans la base de données de messagerie après sa réception/son envoi. Ces bases sont analysées lors de l'analyse complète de l'ordinateur.

Si la protection en temps réel est activée, les messages entrants/sortants sont directement analysés lors de leur réception/envoi.

### BLOCAGE D'UN OBJET

Interdiction de l'accès d'applications tiers à l'objet. L'objet bloqué ne peut être lu, exécuté, modifié ou supprimé.

## C

### CERTIFICAT DU SERVEUR D'ADMINISTRATION

Certificat qui intervient dans l'authentification du serveur d'administration lors de la connexion à celui-ci de la console d'administration et de l'échange de données avec les postes client. Le certificat du serveur d'administration est créé lors de l'installation du serveur d'administration et il est enregistré dans le sous-répertoire Cert du répertoire d'installation.

### CLASSEMENT DU DANGER

Indicateur du danger de l'application pour le système d'exploitation. Le classement est constitué à l'aide de l'analyse heuristique et permet d'identifier les comportements typiques des programmes malveillants. Plus le classement est bas, plus le nombre d'actions autorisées pour l'application est élevé.

### COMPTEUR D'EPIDEMIE DE VIRUS

Modèle qui sert à prévenir les utilisateurs en cas de menace d'épidémie de virus. Le compteur d'épidémie de virus renferme un ensemble de paramètres qui déterminent un seuil d'activité de virus, les modes de diffusions et le texte des messages.

### COURRIER INDESIRABLE

Envoi massif non autorisé de messages électroniques, le plus souvent à caractère publicitaire.

## D

### DEGRE D'IMPORTANCE DE L'EVENEMENT

Caractéristique de l'événement consigné dans le fonctionnement de l'application de Kaspersky Lab. Il existe 4 degrés d'importance:

Evénement critique.

Refus de fonctionnement.

Avertissement.

Information.

Les événements d'un même type peuvent avoir différents degrés de gravité, en fonction du moment où l'événement s'est produit.

### DUREE DE VALIDITE DE LA LICENCE

Durée pendant laquelle vous pouvez utiliser toutes les fonctions de l'application de Kaspersky Lab. Généralement, la durée de validité d'une licence est d'une année calendrier à partir de la date d'installation. Une fois que la durée de validité est écoulée, les fonctions de l'application sont bloquées : vous ne pourrez plus actualiser les bases de l'application.

## E

### EN-TETE

Informations contenues dans le début du fichier ou du message et qui offrent des données de faibles niveaux sur l'état et le traitement du fichier (message). En particulier, l'en-tête du courrier électronique contient des renseignements tels que les données de l'expéditeur, du destinataire et la date.

### ÉTAT DE LA PROTECTION

État actuel de la protection qui définit le niveau de protection 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 POSITIF

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.

### FICHIER DE LICENCE

Fichier portant l'extension .key et qui est votre "clé" personnelle, indispensable au fonctionnement de l'application de Kaspersky Lab. Ce fichier sera inclus dans la boîte si vous avez achetez le logiciel chez un distributeur Kaspersky Lab. En revanche, il vous sera envoyé par email si le produit provient d'une boutique Internet.

### FICHIERS COMPACTE

Fichier d'archivage contenant un programme de décompactage ainsi que des instructions du système d'exploitation nécessaires à son exécution.

### FLUX NTFS ALTERNATIFS

Flux de données du système de fichiers NTFS (alternate data streams) prévus pour contenir des attributs complémentaires ou des informations relatives au fichier.

Chaque fichier dans le système de fichiers NTFS présente un ensemble de flux (streams). Un des flux renferme le contenu du fichier que nous pouvons voir une fois que le fichier a été ouvert. Les autres flux (alternatifs) sont prévus pour les méta-informations et garantissent, par exemple, la compatibilité du système NTFS avec d'autres systèmes tels que l'ancien système de fichiers Macintosh – Hierarchical File System (HFS). Les flux peuvent être créés, supprimés, enregistrés séparément, renommer ou lancer comme processus.

Les flux alternatifs peuvent être exploités par des individus mal intentionnés dans le but de dissimuler l'envoi ou la réception de données de l'ordinateur.

## I

### INSTALLATION A L'AIDE D'UN SCRIPT DE LANCEMENT

Méthode d'installation à distance des applications de Kaspersky Lab qui permet d'associer le lancement d'une tâche d'installation à distance à un compte utilisateur particulier (ou à plusieurs comptes). Lorsque l'utilisateur s'enregistre dans le domaine, une tentative d'installation de l'application sur le poste client d'où s'est connecté l'utilisateur est lancée. Cette méthode est conseillée pour l'installation d'applications sur des ordinateurs fonctionnant sous Microsoft Windows 98/Me.

### INTERCEPTEUR

Sous-composant de l'application chargé de l'analyse de certains types de messages électroniques. La sélection d'intercepteurs installés dépend du rôle ou de la combinaison de rôles de l'application.

## K

### KASPERSKY SECURITY NETWORK

Kaspersky Security Network (KSN) est un ensemble de services en ligne qui permet d'accéder à la base de connaissances de Kaspersky Lab sur la réputation des fichiers, des sites et des applications. L'utilisation des données

de Kaspersky Security Network permet à l'application de réagir plus rapidement aux nouvelles formes de menace, améliore l'efficacité de certains composants de la protection et réduit la probabilité de faux positifs.

## L

### 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 parvient à échéance.

### LISTE DES EXPEDITEURS AUTORISES

(également liste blanche des adresses)

Liste des adresses électroniques des messages du courrier entrant qui ne seront pas analysés par l'application de Kaspersky Lab.

### LISTE DES EXPEDITEURS INTERDITS

(également liste noire des adresses)

Liste des adresses de messagerie électronique bloquées par l'application de Kaspersky Lab, quel que soit le contenu des messages.

### LISTE DES URL ANALYSEES

Liste des masques et des URL soumises obligatoirement à la recherche d'objets malveillants par l'application de Kaspersky Lab.

### LISTE DES URL AUTORISEES

Liste des masques et des URL dont l'accès n'est pas bloqué par l'application de Kaspersky Lab. La liste des adresses est composée par les utilisateurs lors de la configuration de l'application.

### LISTE DES URL INTERDITES

Liste des masques et des URL dont l'accès est bloqué par l'application de Kaspersky Lab. La liste des adresses est composée par les utilisateurs lors de la configuration de l'application.

### LISTE NOIRE DES LICENCES

Base de données contenant des informations relatives aux clés de licence Kaspersky Lab bloquées. Le contenu du fichier de la liste noire est mis à jour en même temps que les bases.

## 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 caractères et ? représente un caractère unique). À 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.

### MASQUE DE SOUS-RESEAU

Le masque de sous-réseau et l'adresse réseau permettent d'identifier un ordinateur au sein d'un réseau informatique.

### MESSAGE INDECENT

Message électronique contenant un vocabulaire vulgaire

### MESSAGE SUSPECT

Message qui ne peut être considéré comme indésirable de manière certaine mais dont l'analyse donne lieu à des soupçons (par exemple, certains types d'envois et de messages publicitaires).

### MISE A JOUR

Procédure de remplacement/d'ajout de nouveaux fichiers (bases ou modules logiciels), récupérés sur les 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.

### MISE A JOUR DISPONIBLE

Ensemble de mises à jour des modules de l'application de Kaspersky Lab qui reprend les mises à jour urgentes rassemblées au cours d'un intervalle de temps défini ainsi que les modifications de l'architecture de l'application.

### MISE A JOUR URGENTE

Mise à jour critique des modules de l'application de Kaspersky Lab.

### MISE EN QUARANTAINE D'OBJETS

Mode de traitement d'un objet potentiellement infecté empêchant tout accès à celui-ci et engendrant son déplacement vers le dossier de quarantaine où il est conservé de manière cryptée afin de prévenir toute action malveillante.

### MODELE DE NOTIFICATION

Modèle utilisé pour signaler la découverte d'objets infectés lors de l'analyse. Le modèle de notification contient un ensemble de paramètres qui définissent l'ordre des notifications, les moyens de diffusion et le texte du message.

### MODULES LOGICIELS

Fichiers faisant partie de la distribution de l'application de Kaspersky Lab et responsables de ses principales tâches. Chaque type de tâche réalisée par l'application (Protection en temps réel, Analyse à la demande, Mise à jour) possède son propre module exécutable. En lançant l'analyse complète depuis la fenêtre principale, vous démarrez le module lié à cette tâche.

## N

### NIVEAU DE PROTECTION

Le niveau de protection est l'ensemble de paramètres prédéfinis de fonctionnement du composant.

### 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 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 CONTROLE

Fichier transmis via le protocole HTTP, FTP ou SMTP par le pare-feu et envoyé à l'application de Kaspersky Lab pour analyse.

### 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 INFECTE POTENTIELLEMENT

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 POTENTIELLEMENT INFECTE

Objet qui, en raison de son format ou de sa structure, peut être utilisé par un individu malintentionné 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 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.

### OBJETS DE DEMARRAGE

Série de programmes indispensables au lancement et au bon fonctionnement du système d'exploitation et des applications installés sur votre ordinateur. Ces objets sont exécutés à chaque démarrage du système d'exploitation. Il existe des virus qui s'attaquent en particulier à ces objets, ce qui peut par exemple provoquer le blocage du système d'exploitation.

## P

### PAQUET DE MISE A JOUR

Ensemble de fichiers copié depuis Internet et installés sur votre ordinateur afin de mettre à jour une application.

### PARAMETRES DE L'APPLICATION

Paramètres de fonctionnement de l'application communs à tous les types de tâche, responsables du fonctionnement de l'application dans son ensemble, par exemple les paramètres de performance de l'application, les paramètres de création des rapports, les paramètres de la sauvegarde.

### PARAMETRES DE LA TACHE

Paramètres de fonctionnement de l'application propres à chaque type de tâche.

### PASSERELLE A DEUX CANAUX

Ordinateur doté de deux cartes de réseau, chacune d'entre elles connectée à un réseau différent et transmettant les informations d'un réseau à l'autre.

### PHISHING

Type d'escroquerie sur Internet qui consiste à envoyer aux victimes potentielles des messages électroniques, prétendument envoyés en général par une banque, dans le but d'obtenir des informations confidentielles.

### 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.

### PORT ENTREE-SORTIE

Utilisé dans les microprocesseurs (par exemple Intel) lors de l'échange de données avec les périphériques. Le port entrée-sortie est comparé à l'un ou l'autre périphérique et permet aux applications de le contacter pour l'échange de données.

### PORT MATERIEL

Connexion pour un périphérique matériel quelconque via un câble ou une fiche (port LPT, port série, USB).

### PROCESSUS DE CONFIANCE

Processus d'une application dont les opérations sur les fichiers ne sont pas contrôlées par l'application de Kaspersky Lab dans le cadre de la protection en temps réel. Les objets lancés, ouverts ou conservés par un processus de confiance ne sont pas analysés.

### PROTECTION EN TEMPS REEL

Mode de fonctionnement pendant lequel l'application recherche en temps réel la présence éventuelle 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).

### PROTOCOLE

Ensemble de règles clairement définies et standardisées, régulant l'interaction entre un client et un serveur. Parmi les protocoles les plus connus et les services liés à ceux-ci, on peut noter : HTTP (WWW), FTP et NNTP (news).

### PROTOCOLE INTERNET (IP)

Protocole de base du réseau Internet, inchangé depuis son lancement en 1974. Il exécute les opérations principales liées au transfert de données d'un ordinateur à un autre et est à la base de protocoles de plus haut niveau tels que TCP et UDP. Il gère la connexion ainsi que la correction d'erreurs. Grâce à des technologies tels que le NAT et le masquerading, il est possible de dissimuler d'importants réseaux privés derrière quelques adresses IP (parfois même derrière une seule adresse). Cela permet de satisfaire la demande sans cesse croissante d'adresses IP alors que la plage IPv4 est relativement limitée.

## 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

### 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.

### REPARATION D'OBJETS LORS DU REDEMARRAGE

Mode de traitement des objets infectés utilisés par d'autres applications au moment de la réparation. Il consiste à créer une copie de l'objet infecté, à réparer cette copie et à remplacer l'objet original infecté par cette copie lors du redémarrage suivant de l'ordinateur.

### 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.

## S

### SOCKS

Protocole de serveur proxy permettant une connexion à deux points entre des ordinateurs du réseau interne et des ordinateurs de réseaux externes.

### SCRIPT

Petit programme informatique ou partie indépendante d'un programme (fonction) écrit, en règle générale, pour exécuter une petite tâche particulière. Ils interviennent le plus souvent lors de l'exécution de programmes intégrés à de l'hypertexte. Les scripts sont exécutés, par exemple, lorsque vous ouvrez certains sites Web.

Si la protection en temps réel est activée, l'application surveille l'exécution des scripts, les intercepte et vérifie s'ils contiennent des virus. En fonction des résultats de l'analyse, vous pourrez autoriser ou bloquer l'exécution du script.

### SECTEUR D'AMORÇAGE DU DISQUE

Le secteur d'amorçage est un secteur particulier du disque dur de l'ordinateur, d'une disquette ou d'un autre support de stockage informatique. Il contient des informations relatives au système de fichiers du disque ainsi qu'un programme de démarrage s'exécutant au lancement du système d'exploitation.

Certains virus, appelés virus de boot ou virus de secteur d'amorçage, s'attaquent aux secteurs d'amorçage des disques. L'application de Kaspersky Lab permet d'analyser les secteurs d'amorçage afin de voir s'ils contiennent des virus et des les réparer en cas d'infection.

### SERVEUR PROXY

Service dans les réseaux informatiques qui permet aux clients de réaliser des requêtes indirectes vers d'autres ressources du réseau. Le client se connecte d'abord au serveur proxy et envoi une requête vers une ressource quelconque (par exemple, un fichier) situé sur un autre serveur. Ensuite, le serveur proxy se connecte au serveur indiqué et obtient la ressource demandée ou récupère la ressource dans son cache (si le serveur proxy possède son propre cache). Dans certains cas, la requête du client ou la réponse du serveur peut être modifiée par le serveur proxy à des fins déterminées.

### 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.

### SERVICE DE NOMS DE DOMAINE (DNS)

Système distribué de traduction du nom d'hôte (ordinateur ou autre périphérique de réseau) en adresse IP. DNS fonctionne dans les réseaux TCP/IP. Dans certains cas particuliers, DNS peut enregistrer et traiter les requêtes de retour et définir le nom de l'hôte sur la base de son IP (enregistrement PTR). La résolution du nom DNS est généralement l'œuvre d'applications de réseau et non pas des utilisateurs.

### SEUIL D'ACTIVITE VIRALE

Nombre d'événements d'un type donné et générés dans un intervalle de temps déterminé qui, une fois dépassé, permettra à l'application de considérer qu'il y a augmentation de l'activité virale et développement d'un risque d'attaque virale. Ce paramètre est d'une importance capitale en cas d'épidémie de virus car il permet à l'administrateur d'anticiper l'attaque.

### SUPPRESSION D'UN MESSAGE

Mode de traitement d'un message électronique considéré comme indésirable. Il se caractérise par la suppression physique du message. Cette méthode est recommandée lorsqu'il ne fait aucun doute que le message est indésirable. Une copie du message supprimé est conservée dans le dossier de sauvegarde (pour autant que cette fonctionnalité ne soit pas désactivée).

### SUPPRESSION D'UN OBJET

Mode de traitement de l'objet qui entraîne sa suppression physique de l'endroit où il a été découvert par l'application (disque dur, répertoire, ressource de réseau). Ce mode de traitement est recommandé pour les objets dangereux dont la réparation est impossible pour une raison quelconque.

## T

### TACHE

Fonctions exécutées par l'application de Kaspersky Lab sous la forme d'une tâche, par exemple : Protection en temps réel des fichiers, Analyse complète de l'ordinateur, Mise à jour des bases.

### TECHNOLOGIE ICHECKER

Technologie qui permet d'accélérer l'analyse antivirus en excluant les objets qui n'ont pas été modifiés depuis l'analyse antérieure pour autant que les paramètres de l'analyse (bases antivirus et paramètres) n'aient pas été modifiés. Ces informations sont conservées dans une base spéciale. La technologie est appliquée aussi bien pendant la protection en temps réel que dans les analyses à la demande.

Admettons que vous possédez une archive qui a été analysée par une application de Kaspersky Lab et qui a reçu l'état sain. Lors de la prochaine analyse, cet objet sera exclu pour autant qu'aucune modification n'ait été apportée au fichier en question ou aux paramètres de l'analyse. Si vous avez modifié le contenu de l'archive (ajout d'un nouvel objet), si vous avez modifié les paramètres de l'analyse ou procédé à la mise à jour des bases antivirus, l'archive sera analysée à nouveau.

Limitations technologiques d'iChecker :

La technologie ne fonctionne pas avec les fichiers de grande taille car dans ce cas il est plus rapide d'analyser tout le fichier que de vérifier s'il a été modifié depuis la dernière analyse ;

La technologie est compatible avec un nombre restreint de formats (exe, dll, lnk, ttf, inf, sys, com, chm, zip, rar).

## V

### VIRUS DE BOOT (AMORÇAGE)

Virus affectant les secteurs d'amorçage du disque de l'ordinateur. Au redémarrage du système, le virus force le système à inscrire en mémoire et à exécuter du code malveillant au lieu du code d'amorçage original.

### VIRUS INCONNU

Nouveau virus au sujet duquel 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

Fondée en 1997, Kaspersky Lab est devenue un leader reconnu en technologies de sécurité de l'information. Elle produit un large éventail de logiciels de sécurité des données et distribue des solutions techniquement avancées et complètes afin de protéger les ordinateurs et les réseaux contre tous types de programmes malveillants, contre le courrier indésirable et contre les tentatives d'intrusion.

Kaspersky Lab est une compagnie internationale. Son siège principal se trouve en Fédération de Russie et la société possède des bureaux régionaux au Royaume Uni, en France, en Allemagne, au Japon, aux Etats-Unis (Californie), dans les pays du Benelux, en Chine, en Pologne et en Roumanie. Un nouveau service de la compagnie, le centre européen de recherches antivirus, a été récemment ouvert en France. Le réseau de partenaires de Kaspersky Lab compte plus de 500 entreprises à travers le monde.

Aujourd'hui, Kaspersky Lab emploie plus de 1 000 spécialistes hautement qualifiés : 10 d'entre eux possèdent un M.B.A et 16 autres, un doctorat. Les principaux experts de Kaspersky Lab sont membres de la prestigieuse Computer Anti-virus Researcher's Organization (organisation pour la recherche antivirus en informatique, CARO).

Kaspersky Lab offre les meilleures solutions de sécurité qui reposent sur une expérience unique et un savoir-faire accumulé pendant plus de 14 années de combat contre les virus informatiques. Grâce à l'analyse en continu de l'activité virale, nous pouvons prévoir les tendances dans le développement des programmes malveillants et fournir à temps à nos utilisateurs une protection optimale contre les nouveaux types d'attaques. Cet avantage est à la base des produits et des services proposés par Kaspersky Lab. Nous avons toujours une longueur d'avance sur la concurrence et nous fournissons à nos clients la meilleure protection possible.

Grâce à des années de travail assidu, la société est devenue leader en développement de systèmes de protection contre les virus. Kaspersky Lab fut l'une des premières entreprises à mettre au point les normes de protection contre les virus en vigueur aujourd'hui. Le produit vitrine de la société est Kaspersky Antivirus® : il assure la protection de tous les objets qui peuvent être pris pour cible par les virus, à savoir les postes de travail, les serveurs de fichiers, les systèmes de messagerie, les pare-feu et passerelles Internet, ainsi que les ordinateurs portables. La convivialité de l'administration permet aux utilisateurs d'automatiser au maximum la protection des ordinateurs et des réseaux de l'entreprise. De nombreux fabricants reconnus utilisent le noyau Kaspersky Anti-Virus : Nokia ICG (Etats-Unis), Aladdin (Israël), Sybari (Etats-Unis), G Data (Allemagne), Deerfield (Etats-Unis), Alt-N (Etats-Unis), Microworld (Inde) et BorderWare (Canada).

Les clients de Kaspersky Lab bénéficient d'un large éventail de services qui garantissent le fonctionnement ininterrompu des logiciels et qui sont parfaitement ajustés aux besoins spécifiques des activités professionnelles. Nous élaborons, mettons en œuvre et accompagnons les dispositifs de protection contre les virus pour entreprise. Les bases antivirus de Kaspersky Lab sont mises à jour toutes les heures. Nous offrons à nos clients une assistance technique en plusieurs langues.

Si vous avez des questions, vous pouvez les adresser au revendeur ou directement à Kaspersky Lab. Vous bénéficierez toujours de consultations détaillées par téléphone ou courrier électronique. Vous recevrez une réponse complète à vos questions.

| | |
|---|---|
| Site de Kaspersky Lab : | http://www.kaspersky.com/fr |
| Encyclopédie des virus : | http://www.viruslist.ru |
| Laboratoire d'étude des virus : | newvirus@kaspersky.com<br>(envoi uniquement d'objets suspects sous forme d'archive)<br>http://support.kaspersky.ru/virlab/helpdesk.html?LANG=fr<br>(pour les questions aux experts antivirus) |
| 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 d'application développé par des éditeurs tiers a été utilisé pour créer l'application.

## DANS CETTE SECTION

# AGG 2.4

**Copyright (C) 2002-2005 Maxim Shemanarev (McSeem)**

Anti-Grain Geometry has dual licensing model. The Modified BSD License was first added in version v2.4 just for convenience. It is a simple, permissive non-copyleft free software license, compatible with the GNU GPL. It's well proven and recognizable. See http://www.fsf.org/licensing/licenses/index_html#ModifiedBSD for details.

Note that the Modified BSD license DOES NOT restrict your rights if you choose the Anti-Grain Geometry Public License.

Anti-Grain Geometry Public License

Anti-Grain Geometry – Version 2.4

Copyright (C) 2002-2005 Maxim Shemanarev (McSeem)

Permission to copy, use, modify, sell and distribute this software is granted provided this copyright notice appears in all copies. This software is provided "as is" without express or implied warranty, and with no claim as to its suitability for any purpose.

Modified BSD License

Anti-Grain Geometry – Version 2.4

Copyright (C) 2002-2005 Maxim Shemanarev (McSeem)

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. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR 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.

# ADOBE ABI-SAFE CONTAINERS 1.0

**Copyright (C) 2005, Adobe Systems Incorporated**

---

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 EVEN SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

# BOOST 1.39.0

**Copyright (C) 2008, Beman Dawes**

---

Boost Software License - Version 1.0 - August 17th, 2003

Permission is hereby granted, free of charge, to any person or organization obtaining a copy of the software and accompanying documentation covered by this license (the "Software") to use, reproduce, display, distribute, execute, and transmit the Software, and to prepare derivative works of the Software, and to permit third-parties to whom the Software is furnished to do so, all subject to the following:

The copyright notices in the Software and this entire statement, including the above license grant, this restriction and the following disclaimer, must be included in all copies of the Software, in whole or in part, and all derivative works of the Software, unless such copies or derivative works are solely in the form of machine-executable object code generated by a source language processor.

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, TITLE AND NON-INFRINGEMENT. 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.

# BZIP2/LIBBZIP2 1.0.5

**Copyright (C) 1996-2007, Julian R Seward**

---

This program, "bzip2", the associated library "libbzip2", and all documentation, are copyright (C) 1996-2007 Julian R Seward. All rights reserved a été utilisée dans le développement de l'application.

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. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

3. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

4. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR 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.

Julian Seward, jseward@bzip.org

bzip2/libbzip2 version 1.0.5 of 10 December 2007

# CONVERTUTF

**Copyright (C) 2001-2004, Unicode, Inc**

---

Disclaimer

This source code is provided as is by Unicode, Inc. No claims are made as to fitness for any particular purpose. No warranties of any kind are expressed or implied. The recipient agrees to determine applicability of information provided. If this file has been purchased on magnetic or optical media from Unicode, Inc., the sole remedy for any claim will be exchange of defective media within 90 days of receipt.

Limitations on Rights to Redistribute This Code Unicode, Inc. hereby grants the right to freely use the information supplied in this file in the creation of products supporting the Unicode Standard, and to make copies of this file in any form for internal or external distribution as long as this notice remains attached.

# CURL 7.19.4

**Copyright (C) 1996-2009, Daniel Stenberg**

---

COPYRIGHT AND PERMISSION NOTICE

Copyright (c) 1996 - 2009, Daniel Stenberg, <daniel@haxx.se>.

All rights reserved a été utilisée dans le développement de l'application.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

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 OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

# DEELX - REGULAR EXPRESSION ENGINE 1.2

**Copyright (C) 2006, RegExLab.com**

http://www.regexlab.com/deelx/

---

# EXPAT 1.2, 2.0.1

**Copyright (C) 1998, 1999, 2000, Thai Open Source Software Center Ltd and Clark Cooper**

**Copyright (C) 2001, 2002, 2003, 2004, 2005, 2006, Expat maintainers**

---

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 AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

# FASTSCRIPT 1.90

**Copyright (C) Fast Reports Inc**

---

# FDLIBM 5.3

**Copyright (C) 2004, Sun Microsystems, Inc**

---

Permission to use, copy, modify, and distribute this software is freely granted, provided that this notice is preserved.

# FLEX: THE FAST LEXICAL ANALYZER 2.5.4

**Copyright (C) 1990, The Regents of the University of California**

---

This code is derived from software contributed to Berkeley by Vern Paxson.

The United States Government has rights in this work pursuant to contract no. DE-AC03-76SF00098 between the United States Department of Energy and the University of California.

Redistribution and use in source and binary forms with or without modification are permitted provided that: (1) source distributions retain this entire copyright notice and comment, and (2) distributions including binaries display the following acknowledgement: "This product includes software developed by the University of California, Berkeley and its contributors" in the documentation or other materials provided with the distribution and in all advertising materials mentioning features or use of this software. Neither the name of the University 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 "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

# 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.

# GDTOA

**Copyright (C) 1998-2002, Lucent Technologies**

**Copyright (C) 2004, 2005, 2009, David M. Gay**

---

Copyright (C) 1998-2002, Lucent Technologies

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that the copyright notice and this permission notice and warranty disclaimer appear in supporting documentation, and that the name of Lucent or any of its entities not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission.

LUCENT DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL LUCENT OR ANY OF ITS ENTITIES BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Copyright (C) 2004, 2005, 2009 David M. Gay

Permission to use, copy, modify, and distribute this software and its

documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that the copyright notice and this permission notice and warranty disclaimer appear in supporting documentation, and that the name of the author or any of his current or former employers not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission.

THE AUTHOR DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR OR ANY OF HIS CURRENT OR FORMER EMPLOYERS BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

# GECKO SDK 1.8, 1.9, 1.9.1

**Copyright (C) Mozilla Foundation**

---

Mozilla Public License Version 1.1

1. Definitions.

1.0.1. "Commercial Use" means distribution or otherwise making the Covered Code available to a third party.

1.1. "Contributor" means each entity that creates or contributes to the creation of Modifications.

1.2. "Contributor Version" means the combination of the Original Code, prior Modifications used by a Contributor, and the Modifications made by that particular Contributor.

1.3. "Covered Code" means the Original Code or Modifications or the combination of the Original Code and Modifications, in each case including portions thereof.

1.4. "Electronic Distribution Mechanism" means a mechanism generally accepted in the software development community for the electronic transfer of data.

1.5. "Executable" means Covered Code in any form other than Source Code.

1.6. "Initial Developer" means the individual or entity identified as the Initial Developer in the Source Code notice required by Exhibit A.

1.7. "Larger Work" means a work which combines Covered Code or portions thereof with code not governed by the terms of this License.

1.8. "License" means this document.

1.8.1. "Licensable" means having the right to grant, to the maximum extent possible, whether at the time of the initial grant or subsequently acquired, any and all of the rights conveyed herein.

1.9. "Modifications" means any addition to or deletion from the substance or structure of either the Original Code or any previous Modifications. When Covered Code is released as a series of files, a Modification is:

Any addition to or deletion from the contents of a file containing Original Code or previous Modifications.

Any new file that contains any part of the Original Code or previous Modifications.

1.10. "Original Code" means Source Code of computer software code which is described in the Source Code notice required by Exhibit A as Original Code, and which, at the time of its release under this License is not already Covered Code governed by this License.

1.10.1. "Patent Claims" means any patent claim(s), now owned or hereafter acquired, including without limitation, method, process, and apparatus claims, in any patent Licensable by grantor.

1.11. "Source Code" means the preferred form of the Covered Code for making modifications to it, including all modules it contains, plus any associated interface definition files, scripts used to control compilation and installation of an Executable, or source code differential comparisons against either the Original Code or another well known, available Covered Code of the Contributor's choice. The Source Code can be in a compressed or archival form, provided the appropriate decompression or de-archiving software is widely available for no charge.

1.12. "You" (or "Your") means an individual or a legal entity exercising rights under, and complying with all of the terms of, this License or a future version of this License issued under Section 6.1. For legal entities, "You" includes any entity which controls, is controlled by, or is under common control with You. For purposes of this definition, "control" means (a) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (b) ownership of more than fifty percent (50%) of the outstanding shares or beneficial ownership of such entity.

2. Source Code License.

2.1. The Initial Developer Grant.

The Initial Developer hereby grants You a world-wide, royalty-free, non-exclusive license, subject to third party intellectual property claims: under intellectual property rights (other than patent or trademark) Licensable by Initial Developer to use, reproduce, modify, display, perform, sublicense and distribute the Original Code (or portions thereof) with or without Modifications, and/or as part of a Larger Work; and under Patents Claims infringed by the making, using or selling of Original Code, to make, have made, use, practice, sell, and offer for sale, and/or otherwise dispose of the Original Code (or portions thereof).

the licenses granted in this Section 2.1 (a) and (b) are effective on the date Initial Developer first distributes Original Code under the terms of this License.

Notwithstanding Section 2.1 (b) above, no patent license is granted: 1) for code that You delete from the Original Code; 2) separate from the Original Code; or 3) for infringements caused by: i) the modification of the Original Code or ii) the combination of the Original Code with other software or devices.

2.2. Contributor Grant.

Subject to third party intellectual property claims, each Contributor hereby grants You a world-wide, royalty-free, non-exclusive license under intellectual property rights (other than patent or trademark) Licensable by Contributor, to use,

reproduce, modify, display, perform, sublicense and distribute the Modifications created by such Contributor (or portions thereof) either on an unmodified basis, with other Modifications, as Covered Code and/or as part of a Larger Work; and under Patent Claims infringed by the making, using, or selling of Modifications made by that Contributor either alone and/or in combination with its Contributor Version (or portions of such combination), to make, use, sell, offer for sale, have made, and/or otherwise dispose of: 1) Modifications made by that Contributor (or portions thereof); and 2) the combination of Modifications made by that Contributor with its Contributor Version (or portions of such combination).

the licenses granted in Sections 2.2 (a) and 2.2 (b) are effective on the date Contributor first makes Commercial Use of the Covered Code.

Notwithstanding Section 2.2 (b) above, no patent license is granted: 1) for any code that Contributor has deleted from the Contributor Version; 2) separate from the Contributor Version; 3) for infringements caused by: i) third party modifications of Contributor Version or ii) the combination of Modifications made by that Contributor with other software (except as part of the Contributor Version) or other devices; or 4) under Patent Claims infringed by Covered Code in the absence of Modifications made by that Contributor.

3. Distribution Obligations.

3.1. Application of License.

The Modifications which You create or to which You contribute are governed by the terms of this License, including without limitation Section 2.2. The Source Code version of Covered Code may be distributed only under the terms of this License or a future version of this License released under Section 6.1, and You must include a copy of this License with every copy of the Source Code You distribute. You may not offer or impose any terms on any Source Code version that alters or restricts the applicable version of this License or the recipients' rights hereunder. However, You may include an additional document offering the additional rights described in Section 3.5.

3.2. Availability of Source Code.

Any Modification which You create or to which You contribute must be made available in Source Code form under the terms of this License either on the same media as an Executable version or via an accepted Electronic Distribution Mechanism to anyone to whom you made an Executable version available; and if made available via Electronic Distribution Mechanism, must remain available for at least twelve (12) months after the date it initially became available, or at least six (6) months after a subsequent version of that particular Modification has been made available to such recipients. You are responsible for ensuring that the Source Code version remains available even if the Electronic Distribution Mechanism is maintained by a third party.

3.3. Description of Modifications.

You must cause all Covered Code to which You contribute to contain a file documenting the changes You made to create that Covered Code and the date of any change. You must include a prominent statement that the Modification is derived, directly or indirectly, from Original Code provided by the Initial Developer and including the name of the Initial Developer in (a) the Source Code, and (b) in any notice in an Executable version or related documentation in which You describe the origin or ownership of the Covered Code.

3.4. Intellectual Property Matters

(a) Third Party Claims

If Contributor has knowledge that a license under a third party's intellectual property rights is required to exercise the rights granted by such Contributor under Sections 2.1 or 2.2, Contributor must include a text file with the Source Code distribution titled "LEGAL" which describes the claim and the party making the claim in sufficient detail that a recipient will know whom to contact. If Contributor obtains such knowledge after the Modification is made available as described in Section 3.2, Contributor shall promptly modify the LEGAL file in all copies Contributor makes available thereafter and shall take other steps (such as notifying appropriate mailing lists or newsgroups) reasonably calculated to inform those who received the Covered Code that new knowledge has been obtained.

(b) Contributor APIs

If Contributor's Modifications include an application programming interface and Contributor has knowledge of patent licenses which are reasonably necessary to implement that API, Contributor must also include this information in the legal file.

(c) Representations.

Contributor represents that, except as disclosed pursuant to Section 3.4 (a) above, Contributor believes that Contributor's Modifications are Contributor's original creation(s) and/or Contributor has sufficient rights to grant the rights conveyed by this License.

3.5. Required Notices.

You must duplicate the notice in Exhibit A in each file of the Source Code. If it is not possible to put such notice in a particular Source Code file due to its structure, then You must include such notice in a location (such as a relevant directory) where a user would be likely to look for such a notice. If You created one or more Modification(s) You may add your name as a Contributor to the notice described in Exhibit A. You must also duplicate this License in any documentation for the Source Code where You describe recipients' rights or ownership rights relating to Covered Code. You may choose to offer, and to charge a fee for, warranty, support, indemnity or liability obligations to one or more recipients of Covered Code. However, You may do so only on Your own behalf, and not on behalf of the Initial Developer or any Contributor. You must make it absolutely clear than any such warranty, support, indemnity or liability obligation is offered by You alone, and You hereby agree to indemnify the Initial Developer and every Contributor for any liability incurred by the Initial Developer or such Contributor as a result of warranty, support, indemnity or liability terms You offer.

3.6. Distribution of Executable Versions.

You may distribute Covered Code in Executable form only if the requirements of Sections 3.1, 3.2, 3.3, 3.4 and 3.5 have been met for that Covered Code, and if You include a notice stating that the Source Code version of the Covered Code is available under the terms of this License, including a description of how and where You have fulfilled the obligations of Section 3.2. The notice must be conspicuously included in any notice in an Executable version, related documentation or collateral in which You describe recipients' rights relating to the Covered Code. You may distribute the Executable version of Covered Code or ownership rights under a license of Your choice, which may contain terms different from this License, provided that You are in compliance with the terms of this License and that the license for the Executable version does not attempt to limit or alter the recipient's rights in the Source Code version from the rights set forth in this License. If You distribute the Executable version under a different license You must make it absolutely clear that any terms which differ from this License are offered by You alone, not by the Initial Developer or any Contributor. You hereby agree to indemnify the Initial Developer and every Contributor for any liability incurred by the Initial Developer or such Contributor as a result of any such terms You offer.

3.7. Larger Works.

You may create a Larger Work by combining Covered Code with other code not governed by the terms of this License and distribute the Larger Work as a single product. In such a case, You must make sure the requirements of this License are fulfilled for the Covered Code.

4. Inability to Comply Due to Statute or Regulation.

If it is impossible for You to comply with any of the terms of this License with respect to some or all of the Covered Code due to statute, judicial order, or regulation then You must: (a) comply with the terms of this License to the maximum extent possible; and (b) describe the limitations and the code they affect. Such description must be included in the legal file described in Section 3.4 and must be included with all distributions of the Source Code. Except to the extent prohibited by statute or regulation, such description must be sufficiently detailed for a recipient of ordinary skill to be able to understand it.

5. Application of this License.

This License applies to code to which the Initial Developer has attached the notice in Exhibit A and to related Covered Code.

6. Versions of the License.

6.1. New Versions

Netscape Communications Corporation ("Netscape") may publish revised and/or new versions of the License from time to time. Each version will be given a distinguishing version number.

6.2. Effect of New Versions

Once Covered Code has been published under a particular version of the License, You may always continue to use it under the terms of that version. You may also choose to use such Covered Code under the terms of any subsequent version of the License published by Netscape. No one other than Netscape has the right to modify the terms applicable to Covered Code created under this License.

6.3. Derivative Works

If You create or use a modified version of this License (which you may only do in order to apply it to code which is not already Covered Code governed by this License), You must (a) rename Your license so that the phrases "Mozilla", "MOZILLAPL", "MOZPL", "Netscape", "MPL", "NPL" or any confusingly similar phrase do not appear in your license (except to note that your license differs from this License) and (b) otherwise make it clear that Your version of the license contains terms which differ from the Mozilla Public License and Netscape Public License. (Filling in the name of the Initial Developer, Original Code or Contributor in the notice described in Exhibit A shall not of themselves be deemed to be modifications of this License.)

7. Disclaimer of warranty

Covered code is provided under this license on an "as is" basis, without warranty of any kind, either expressed or implied, including, without limitation, warranties that the covered code is free of defects, merchantable, fit for a particular purpose or non-infringing. The entire risk as to the quality and performance of the covered code is with you. Should any covered code prove defective in any respect, you (not the initial developer or any other contributor) assume the cost of any necessary servicing, repair or correction. This disclaimer of warranty constitutes an essential part of this license. No use of any covered code is authorized hereunder except under this disclaimer.

8. Termination

8.1. This License and the rights granted hereunder will terminate automatically if You fail to comply with terms herein and fail to cure such breach within 30 days of becoming aware of the breach. All sublicenses to the Covered Code which are properly granted shall survive any termination of this License. Provisions which, by their nature, must remain in effect beyond the termination of this License shall survive.

8.2. If You initiate litigation by asserting a patent infringement claim (excluding declatory judgment actions) against Initial Developer or a Contributor (the Initial Developer or Contributor against whom You file such action is referred to as "Participant") alleging that:

such Participant's Contributor Version directly or indirectly infringes any patent, then any and all rights granted by such Participant to You under Sections 2.1 and/or 2.2 of this License shall, upon 60 days notice from Participant terminate prospectively, unless if within 60 days after receipt of notice You either: (i) agree in writing to pay Participant a mutually agreeable reasonable royalty for Your past and future use of Modifications made by such Participant, or (ii) withdraw Your litigation claim with respect to the Contributor Version against such Participant. If within 60 days of notice, a reasonable royalty and payment arrangement are not mutually agreed upon in writing by the parties or the litigation claim is not withdrawn, the rights granted by Participant to You under Sections 2.1 and/or 2.2 automatically terminate at the expiration of the 60 day notice period specified above.

any software, hardware, or device, other than such Participant's Contributor Version, directly or indirectly infringes any patent, then any rights granted to You by such Participant under Sections 2.1(b) and 2.2(b) are revoked effective as of the date You first made, used, sold, distributed, or had made, Modifications made by that Participant.

8.3. If You assert a patent infringement claim against Participant alleging that such Participant's Contributor Version directly or indirectly infringes any patent where such claim is resolved (such as by license or settlement) prior to the initiation of patent infringement litigation, then the reasonable value of the licenses granted by such Participant under Sections 2.1 or 2.2 shall be taken into account in determining the amount or value of any payment or license.

8.4. In the event of termination under Sections 8.1 or 8.2 above, all end user license agreements (excluding distributors and resellers) which have been validly granted by You or any distributor hereunder prior to termination shall survive termination.

9. Limitation of liability

Under no circumstances and under no legal theory, whether tort (including negligence), contract, or otherwise, shall you, the initial developer, any other contributor, or any distributor of covered code, or any supplier of any of such parties, be liable to any person for any indirect, special, incidental, or consequential damages of any character including, without limitation, damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses, even if such party shall have been informed of the possibility of such damages. This limitation of liability shall not apply to liability for death or personal injury resulting from such party's negligence to the extent applicable law prohibits such limitation. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so this exclusion and limitation may not apply to you.

10. U.S. government end users

The Covered Code is a "commercial item," as that term is defined in 48 C.F.R. 2.101 (Oct. 1995), consisting of "commercial computer software" and "commercial computer software documentation," as such terms are used in 48 C.F.R. 12.212 (Sept. 1995). Consistent with 48 C.F.R. 12.212 and 48 C.F.R. 227.7202-1 through 227.7202-4 (June 1995), all U.S. Government End Users acquire Covered Code with only those rights set forth herein.

11. Miscellaneous

This License represents the complete agreement concerning subject matter hereof. If any provision of this License is held to be unenforceable, such provision shall be reformed only to the extent necessary to make it enforceable. This License shall be governed by California law provisions (except to the extent applicable law, if any, provides otherwise), excluding its conflict-of-law provisions. With respect to disputes in which at least one party is a citizen of, or an entity chartered or registered to do business in the United States of America, any litigation relating to this License shall be subject to the jurisdiction of the Federal Courts of the Northern District of California, with venue lying in Santa Clara County, California, with the losing party responsible for costs, including without limitation, court costs and reasonable attorneys' fees and expenses. The application of the United Nations Convention on Contracts for the International Sale of Goods is expressly excluded. Any law or regulation which provides that the language of a contract shall be construed against the drafter shall not apply to this License.

12. Responsibility for claims

As between Initial Developer and the Contributors, each party is responsible for claims and damages arising, directly or indirectly, out of its utilization of rights under this License and You agree to work with Initial Developer and Contributors to distribute such responsibility on an equitable basis. Nothing herein is intended or shall be deemed to constitute any admission of liability.

13. Multiple-licensed code

Initial Developer may designate portions of the Covered Code as "Multiple-Licensed". "Multiple-Licensed" means that the Initial Developer permits you to utilize portions of the Covered Code under Your choice of the MPL or the alternative licenses, if any, specified by the Initial Developer in the file described in Exhibit A.

Exhibit A - Mozilla Public License.

"The contents of this file are subject to the Mozilla Public License

Version 1.1 (the "License"); you may not use this file except in

compliance with the License. You may obtain a copy of the License at

http://www.mozilla.org/MPL/

Software distributed under the License is distributed on an "AS IS"

basis, WITHOUT WARRANTY OF ANY KIND, either express or implied. See the

License for the specific language governing rights and limitations

under the License.

The Original Code is _____.

The Initial Developer of the Original Code is _____.

Portions created by _____ are Copyright (C) _____

_____. All Rights Reserved.

Contributor(s): _____.

Alternatively, the contents of this file may be used under the terms

of the _____ license (the "[___] License"), in which case the

provisions of [_____] License are applicable instead of those

above. If you wish to allow use of your version of this file only

under the terms of the [____] License and not to allow others to use

your version of this file under the MPL, indicate your decision by

deleting the provisions above and replace them with the notice and

other provisions required by the [___] License. If you do not delete

the provisions above, a recipient may use your version of this file

under either the MPL or the [___] License."

NOTE: The text of this Exhibit A may differ slightly from the text of the notices in the Source Code files of the Original Code. You should use the text of this Exhibit A rather than the text found in the Original Code Source Code for Your Modifications.

---

AMENDMENTS

The Netscape Public License Version 1.1 ("NPL") consists of the Mozilla Public License Version 1.1 with the following Amendments,

including Exhibit A-Netscape Public License. Files identified with "Exhibit A-Netscape Public License" are governed by the Netscape

Public License Version 1.1.

Additional Terms applicable to the Netscape Public License.

I. Effect.

These additional terms described in this Netscape Public License -- Amendments shall apply to the Mozilla Communicator

client code and to all Covered Code under this License.

II. "Netscape's Branded Code" means Covered Code that Netscape distributes and/or permits others to distribute under one or more trademark(s) which are controlled by Netscape but which are not licensed for use under this License.

III. Netscape and logo.

This License does not grant any rights to use the trademarks "Netscape", the "Netscape N and horizon" logo or the "Netscape

lighthouse" logo, "Netcenter", "Gecko", "Java" or "JavaScript", "Smart Browsing" even if such marks are included in the Original

Code or Modifications.

IV. Inability to Comply Due to Contractual Obligation.

Prior to licensing the Original Code under this License, Netscape has licensed third party code for use in Netscape's Branded Code.

To the extent that Netscape is limited contractually from making such third party code available under this License, Netscape may

choose to reintegrate such code into Covered Code without being required to distribute such code in Source Code form, even if

such code would otherwise be considered "Modifications" under this License.

V. Use of Modifications and Covered Code by Initial Developer.

V.1. In General.

The obligations of Section 3 apply to Netscape, except to the extent specified in this Amendment, Section V.2 and V.3.

V.2. Other Products.

Netscape may include Covered Code in products other than the Netscape's Branded Code which are released by Netscape during the two (2) years following the release date of the Original Code, without such additional products becoming subject to the terms of this License, and may license such additional products on different terms from those contained in this License.

V.3. Alternative Licensing.

Netscape may license the Source Code of Netscape's Branded Code, including Modifications incorporated therein, without such Netscape Branded Code becoming subject to the terms of this License, and may license such Netscape Branded Code on different terms from those contained in this License.

VI. Litigation.

Notwithstanding the limitations of Section 11 above, the provisions regarding litigation in Section 11(a), (b) and (c) of the License shall apply to all disputes relating to this License.

EXHIBIT A-Netscape Public License.

"The contents of this file are subject to the Netscape Public

License Version 1.1 (the "License"); you may not use this file

except in compliance with the License. You may obtain a copy of

the License at http://www.mozilla.org/NPL/

Software distributed under the License is distributed on an "AS

IS" basis, WITHOUT WARRANTY OF ANY KIND, either express or

implied. See the License for the specific language governing

rights and limitations under the License.

The Original Code is Mozilla Communicator client code, released

March 31, 1998.

The Initial Developer of the Original Code is Netscape

Communications Corporation. Portions created by Netscape are

Copyright (C) 1998-1999 Netscape Communications Corporation. All

Rights Reserved.

Contributor(s): _____.

Alternatively, the contents of this file may be used under the

terms of the _____ license (the "[___] License"), in which case

the provisions of [_____] License are applicable instead of

those above. If you wish to allow use of your version of this

file only under the terms of the [____] License and not to allow

others to use your version of this file under the NPL, indicate

your decision by deleting the provisions above and replace them

with the notice and other provisions required by the [___]

License. If you do not delete the provisions above, a recipient

may use your version of this file under either the NPL or the

[___] License."

# ICU4C 4.0.1

**Copyright (C) 1995-2008, International Business Machines Corporation and others**

---

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, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, provided that the above copyright notice(s) and this permission notice appear in all copies of the Software and that both the above copyright notice(s) and this permission notice appear in supporting documentation.

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 OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR HOLDERS INCLUDED IN THIS NOTICE BE LIABLE FOR ANY CLAIM, OR ANY SPECIAL INDIRECT OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

# 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.

# JSON4LUA 0.9.30

**Copyright (C) 2009, Craig Mason-Jones**

---

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 AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE,

ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

# LIBGD 2.0.35

---

Portions copyright 1994, 1995, 1996, 1997, 1998, 1999, 2000, 2001, 2002 by Cold Spring Harbor Laboratory. Funded under Grant

P41-RR02188 by the National Institutes of Health.

Portions copyright 1996, 1997, 1998, 1999, 2000, 2001, 2002 by Boutell.Com, Inc.

Portions relating to GD2 format copyright 1999, 2000, 2001, 2002 Philip Warner.

Portions relating to PNG copyright 1999, 2000, 2001, 2002 Greg Roelofs.

Portions relating to gdttf.c copyright 1999, 2000, 2001, 2002 John Ellson (ellson@lucent.com).

Portions relating to gdft.c copyright 2001, 2002 John Ellson (ellson@lucent.com).

Portions copyright 2000, 2001, 2002, 2003, 2004, 2005, 2006, 2007 Pierre-Alain Joye (pierre@libgd.org).

Portions relating to JPEG and to color quantization copyright 2000, 2001, 2002, Doug Becker and copyright (C) 1994, 1995, 1996, 1997, 1998, 1999, 2000, 2001, 2002, Thomas G. Lane. This software is based in part on the work of the Independent JPEG Group. See the file README-JPEG.TXT for more information.

Portions relating to WBMP copyright 2000, 2001, 2002 Maurice Szmurlo and Johan Van den Brande.

Permission has been granted to copy, distribute and modify gd in any context without fee, including a commercial application, provided that this notice is present in user-accessible supporting documentation.

This does not affect your ownership of the derived work itself, and the intent is to assure proper credit for the authors of gd, not to interfere with your productive use of gd. If you have questions, ask. "Derived works" includes all programs that utilize the library. Credit must be given in user-accessible documentation.

This software is provided "AS IS." The copyright holders disclaim all warranties, either express or implied, including but not limited to implied warranties of merchantability and fitness for a particular purpose, with respect to this code and accompanying documentation.

Although their code does not appear in gd, the authors wish to thank David Koblas, David Rowley, and Hutchison Avenue Software Corporation for their prior contributions.

# LIBJPEG 6B

**Copyright (C) 1991-2009, Thomas G. Lane, Guido Vollbeding**

---

LEGAL ISSUES

==========

In plain English:

1. We don't promise that this software works. (But if you find any bugs, please let us know!)

2. You can use this software for whatever you want. You don't have to pay us.

3. You may not pretend that you wrote this software. If you use it in a program, you must acknowledge somewhere in your documentation that you've used the IJG code.

In legalese:

The authors make NO WARRANTY or representation, either express or implied, with respect to this software, its quality, accuracy, merchantability, or fitness for a particular purpose. This software is provided "AS IS", and you, its user, assume the entire risk as to its quality and accuracy.

This software is copyright (C) 1991-2009, Thomas G. Lane, Guido Vollbeding.

All Rights Reserved except as specified below.

Permission is hereby granted to use, copy, modify, and distribute this software (or portions thereof) for any purpose, without fee, subject to these conditions:

(1) If any part of the source code for this software is distributed, then this README file must be included, with this copyright and no-warranty notice unaltered; and any additions, deletions, or changes to the original files must be clearly indicated in accompanying documentation.

(2) If only executable code is distributed, then the accompanying documentation must state that "this software is based in part on the work of the Independent JPEG Group".

(3) Permission for use of this software is granted only if the user accepts full responsibility for any undesirable consequences; the authors accept NO LIABILITY for damages of any kind.

These conditions apply to any software derived from or based on the IJG code, not just to the unmodified library. If you use our work, you ought to acknowledge us.

Permission is NOT granted for the use of any IJG author's name or company name in advertising or publicity relating to this software or products derived from it. This software may be referred to only as "the Independent JPEG Group's software".

We specifically permit and encourage the use of this software as the basis of commercial products, provided that all warranty or liability claims are assumed by the product vendor.

ansi2knr.c is included in this distribution by permission of L. Peter Deutsch, sole proprietor of its copyright holder, Aladdin Enterprises of Menlo Park, CA.

ansi2knr.c is NOT covered by the above copyright and conditions, but instead by the usual distribution terms of the Free Software Foundation; principally, that you must include source code if you redistribute it. (See the file ansi2knr.c for full details.) However, since ansi2knr.c is not needed as part of any program generated from the IJG code, this does not limit you more than the foregoing paragraphs do.

The Unix configuration script "configure" was produced with GNU Autoconf. It is copyright by the Free Software Foundation but is freely distributable.

The same holds for its supporting scripts (config.guess, config.sub, ltmain.sh). Another support script, install-sh, is copyright by X Consortium but is also freely distributable.

The IJG distribution formerly included code to read and write GIF files.

To avoid entanglement with the Unisys LZW patent, GIF reading support has been removed altogether, and the GIF writer has been simplified to produce "uncompressed GIFs". This technique does not use the LZW algorithm; the resulting GIF files are larger than usual, but are readable by all standard GIF decoders.

We are required to state that "The Graphics Interchange Format(c) is the Copyright property of CompuServe Incorporated. GIF(sm) is a Service Mark property of CompuServe Incorporated."

# LIBM (LRINT.C V 1.4, LRINTF.C,V 1.5)



# LIBPNG 1.2.8, 1.2.9, 1.2.42

libpng versions 0.97, January 1998, through 1.0.6, March 20, 2000, are Copyright (c) 1998, 1999 Glenn Randers-Pehrson, and are distributed according to the same disclaimer and license as libpng-0.96, with the following individuals added to the list of Contributing Authors:

Tom Lane

Glenn Randers-Pehrson

Willem van Schaik

libpng versions 0.89, June 1996, through 0.96, May 1997, are Copyright (c) 1996, 1997 Andreas Dilger Distributed according to the same disclaimer and license as libpng-0.88,

with the following individuals added to the list of Contributing Authors:

John Bowler

Kevin Bracey

Sam Bushell

Magnus Holmgren

Greg Roelofs

Tom Tanner

libpng versions 0.5, May 1995, through 0.88, January 1996, are Copyright (c) 1995, 1996 Guy Eric Schalnat, Group 42, Inc.

For the purposes of this copyright and license, "Contributing Authors" is defined as the following set of individuals:

Andreas Dilger

Dave Martindale

Guy Eric Schalnat

Paul Schmidt

Tim Wegner

The PNG Reference Library is supplied "AS IS". The Contributing Authors and Group 42, Inc. disclaim all warranties, expressed or implied, including, without limitation, the warranties of merchantability and of fitness for any purpose. The Contributing Authors and Group 42, Inc. assume no liability for direct, indirect, incidental, special, exemplary, or consequential damages, which may result from the use of the PNG Reference Library, even if advised of the possibility of such damage.

Permission is hereby granted to use, copy, modify, and distribute this source code, or portions hereof, for any purpose, without fee, subject to the following restrictions:

1. The origin of this source code must not be misrepresented.

2. Altered versions must be plainly marked as such and must not be misrepresented as being the original source.

3. This Copyright notice may not be removed or altered from any source or altered source distribution.

The Contributing Authors and Group 42, Inc. specifically permit, without fee, and encourage the use of this source code as a component to supporting the PNG file format in commercial products. If you use this source code in a product, acknowledgment is not required but would be appreciated.

A "png_get_copyright" function is available, for convenient use in "about" boxes and the like:

```
printf("%s",png_get_copyright(NULL));
```

Also, the PNG logo (in PNG format, of course) is supplied in the files "pngbar.png" and "pngbar.jpg (88x31) and "pngnow.png" (98x31).

Libpng is OSI Certified Open Source Software. OSI Certified Open Source is a certification mark of the Open Source Initiative.

# LIBUNGIF 3.0

**Copyright (C) 1997, Eric S. Raymond**

---

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 AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

# LIBXDR

**Copyright (C) Sun Microsystems, Inc**

---

Sun RPC is a product of Sun Microsystems, Inc. and is provided for unrestricted use provided that this legend is included on all tape media and as a part of the software program in whole or part.

Users may copy or modify Sun RPC without charge, but are not authorized to license or distribute it to anyone else except as part of a product or program developed by the user.

SUN RPC IS PROVIDED AS IS WITH NO WARRANTIES OF ANY KIND INCLUDING THE WARRANTIES OF DESIGN, MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE, OR ARISING FROM A COURSE OF DEALING, USAGE OR TRADE PRACTICE.

Sun RPC is provided with no support and without any obligation on the part of Sun Microsystems, Inc. to assist in its use, correction, modification or enhancement.

SUN MICROSYSTEMS, INC. SHALL HAVE NO LIABILITY WITH RESPECT TO THE INFRINGEMENT OF COPYRIGHTS, TRADE SECRETS OR ANY PATENTS BY SUN RPC OR ANY PART THEREOF.

In no event will Sun Microsystems, Inc. be liable for any lost revenue or profits or other special, indirect and consequential damages, even if Sun has been advised of the possibility of such damages.

Sun Microsystems, Inc.

2550 Garcia Avenue

Mountain View, California 94043

# LREXLIB 2.4

**Copyright (C) 2000-2008, Reuben Thomas Copyright (C) 2004-2008, Shmuel Zeigerman**

---

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 AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

# LUA 5.1.4

**Copyright (C) 1994-2008, Lua.org, PUC-Rio**

---

Lua License

---

Lua is licensed under the terms of the MIT license reproduced below.

This means that Lua is free software and can be used for both academic and commercial purposes at absolutely no cost.

For details and rationale, see http://www.lua.org/license.html .

Copyright (C) 1994-2008 Lua.org, PUC-Rio.

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 AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

# LZMALIB 4.43

---

# MD5.H

Copyright (C) 1999, Aladdin Enterprises

---

This software is provided "as-is", without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of 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 following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution.

L. Peter Deutsch (ghost@aladdin.com)

# 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.

# MD5-CC 1.02

**Copyright (C) 1991-1992, RSA Data Security, Inc**

**Copyright (C) 1995, Mordechai T. Abzug**

---

This software contains a C++/object oriented translation and modification of MD5 (version 1.02) by Mordechai T. Abzug. Translation and modification (c) 1995 by Mordechai T. Abzug

Copyright 1991-1992 RSA Data Security, Inc.

The MD5 algorithm is defined in RFC 1321. This implementation is derived from the reference C code in RFC 1321 which is covered by the following copyright statement:

Copyright (C) 1991-2, RSA Data Security, Inc. Created 1991. All rights reserved a été utilisée dans le développement de l'application.

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.

# OPENSSL 0.9.8K

**Copyright (C) 1998-2008, The OpenSSL Project**

---

LICENSE ISSUES

==========

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

OpenSSL License

---

==========

Copyright (c) 1998-2008 The OpenSSL Project. All rights reserved a été utilisée dans le développement de l'application.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project

for use in the OpenSSL Toolkit. (http://www.openssl.org/)" 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

==========

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

---

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)

All rights reserved a été utilisée dans le développement de l'application.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used.

This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

"This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"

The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES

(INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

# PCRE 7.7, 7.9

**Copyright (C) 1997-2009, University of Cambridge**

**Copyright (C) 2007-2008, Google Inc**

---

PCRE LICENCE

---

PCRE is a library of functions to support regular expressions whose syntax and semantics are as close as possible to those of the Perl 5 language.

Release 7 of PCRE is distributed under the terms of the "BSD" licence, as specified below. The documentation for PCRE, supplied in the "doc" directory, is distributed under the same terms as the software itself.

The basic library functions are written in C and are freestanding. Also included in the distribution is a set of C++ wrapper functions.

THE BASIC LIBRARY FUNCTIONS

---

Written by: Philip Hazel

Email local part: ph10

Email domain: cam.ac.uk

University of Cambridge Computing Service,

Cambridge, England.

Copyright (c) 1997-2009 University of Cambridge

All rights reserved a été utilisée dans le développement de l'application.

THE C++ WRAPPER FUNCTIONS

---

Contributed by: Google Inc.

# SHA1.C 1.2



# STLPORT 5.2.1

# SVCCTL.IDL

**Copyright (C) 2010, Microsoft Corporation**

---

# TINYXML 2.5.3

Copyright (C) 2000-2006, Lee Thomason

---

Original code (2.0 and earlier) copyright (c) 2000-2006 Lee Thomason (www.grinninglizard.com)

This software is provided "as-is", without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of 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 following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution.

# VISUAL STUDIO CRT SOURCE CODE 8.0

**Copyright (C) Microsoft Corporation**

---

# WINDOWS TEMPLATE LIBRARY 8.0

**Copyright (C) Microsoft Corporation**

---

Common Public License Version 1.0

THE ACCOMPANYING PROGRAM IS PROVIDED UNDER THE TERMS OF THIS COMMON PUBLIC LICENSE ("AGREEMENT"). ANY USE, REPRODUCTION OR DISTRIBUTION OF THE PROGRAM CONSTITUTES RECIPIENT'S ACCEPTANCE OF THIS AGREEMENT.

1. DEFINITIONS

"Contribution" means:

a) in the case of the initial Contributor, the initial code and documentation distributed under this Agreement, and

b) in the case of each subsequent Contributor:

i) changes to the Program, and

ii) additions to the Program;

where such changes and/or additions to the Program originate from and are distributed by that particular Contributor. A Contribution 'originates' from a Contributor if it was added to the Program by such Contributor itself or anyone acting on such Contributor's behalf. Contributions do not include additions to the Program which: (i) are separate modules of software distributed in conjunction with the Program under their own license agreement, and (ii) are not derivative works of the Program.

"Contributor" means any person or entity that distributes the Program.

"Licensed Patents " mean patent claims licensable by a Contributor which are necessarily infringed by the use or sale of its Contribution alone or when combined with the Program.

"Program" means the Contributions distributed in accordance with this Agreement.

"Recipient" means anyone who receives the Program under this Agreement, including all Contributors.

2. GRANT OF RIGHTS

a) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free copyright license to reproduce, prepare derivative works of, publicly display, publicly perform, distribute and sublicense the Contribution of such Contributor, if any, and such derivative works, in source code and object code form.

b) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free patent license under Licensed Patents to make, use, sell, offer to sell, import and otherwise transfer the Contribution of such Contributor, if any, in source code and object code form. This patent license shall apply to the combination of the Contribution and the Program if, at the time the Contribution is added by the Contributor, such addition of the Contribution causes such combination to be covered by the Licensed Patents. The patent license shall not apply to any other combinations which include the Contribution. No hardware per se is licensed hereunder.

c) Recipient understands that although each Contributor grants the licenses to its Contributions set forth herein, no assurances are provided by any Contributor that the Program does not infringe the patent or other intellectual property rights of any other entity. Each Contributor disclaims any liability to Recipient for claims brought by any other entity based on infringement of intellectual property rights or otherwise. As a condition to exercising the rights and licenses granted hereunder, each Recipient hereby assumes sole responsibility to secure any other intellectual property rights needed, if any. For example, if a third party patent license is required to allow Recipient to distribute the Program, it is Recipient's responsibility to acquire that license before distributing the Program.

d) Each Contributor represents that to its knowledge it has sufficient copyright rights in its Contribution, if any, to grant the copyright license set forth in this Agreement.

3. REQUIREMENTS

A Contributor may choose to distribute the Program in object code form under its own license agreement, provided that:

a) it complies with the terms and conditions of this Agreement; and

b) its license agreement:

i) effectively disclaims on behalf of all Contributors all warranties and conditions, express and implied, including warranties or conditions of title and non-infringement, and implied warranties or conditions of merchantability and fitness for a particular purpose;

ii) effectively excludes on behalf of all Contributors all liability for damages, including direct, indirect, special, incidental and consequential damages, such as lost profits;

iii) states that any provisions which differ from this Agreement are offered by that Contributor alone and not by any other party; and

iv) states that source code for the Program is available from such Contributor, and informs licensees how to obtain it in a reasonable manner on or through a medium customarily used for software exchange.

When the Program is made available in source code form:

a) it must be made available under this Agreement; and

b) a copy of this Agreement must be included with each copy of the Program.

Contributors may not remove or alter any copyright notices contained within the Program.

Each Contributor must identify itself as the originator of its Contribution, if any, in a manner that reasonably allows subsequent Recipients to identify the originator of the Contribution.

4. COMMERCIAL DISTRIBUTION

Commercial distributors of software may accept certain responsibilities with respect to end users, business partners and the like. While this license is intended to facilitate the commercial use of the Program, the Contributor who includes the Program in a commercial product offering should do so in a manner which does not create potential liability for other Contributors. Therefore, if a Contributor includes the Program in a commercial product offering, such Contributor ("Commercial Contributor") hereby agrees to defend and indemnify every other Contributor ("Indemnified Contributor") against any losses, damages and costs (collectively "Losses") arising from claims, lawsuits and other legal actions brought by a third party against the Indemnified Contributor to the extent caused by the acts or omissions of such Commercial Contributor in connection with its distribution of the Program in a commercial product offering. The obligations in this section do not apply to any claims or Losses relating to any actual or alleged intellectual property infringement. In order to qualify, an Indemnified Contributor must: a) promptly notify the Commercial Contributor in writing of such claim, and b) allow the Commercial Contributor to control, and cooperate with the Commercial Contributor in, the defense and any related settlement negotiations. The Indemnified Contributor may participate in any such claim at its own expense.

For example, a Contributor might include the Program in a commercial product offering, Product X. That Contributor is then a Commercial Contributor. If that Commercial Contributor then makes performance claims, or offers warranties related to Product X, those performance claims and warranties are such Commercial Contributor's responsibility alone. Under this section, the Commercial Contributor would have to defend claims against the other Contributors related to those performance claims and warranties, and if a court requires any other Contributor to pay any damages as a result, the Commercial Contributor must pay those damages.

5. NO WARRANTY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, THE PROGRAM IS PROVIDED ON AN "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OR CONDITIONS OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Each Recipient is solely responsible for determining the appropriateness of using and distributing the Program and assumes all risks associated with its exercise of rights under this Agreement, including but not limited to the risks and costs of program errors, compliance with applicable laws, damage to or loss of data, programs or equipment, and unavailability or interruption of operations.

6. DISCLAIMER OF LIABILITY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, NEITHER RECIPIENT NOR ANY CONTRIBUTORS SHALL HAVE ANY LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOST PROFITS), 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 OR DISTRIBUTION OF THE PROGRAM OR THE EXERCISE OF ANY RIGHTS GRANTED HEREUNDER, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. GENERAL

If any provision of this Agreement is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Agreement, and without further action by the parties hereto, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

If Recipient institutes patent litigation against a Contributor with respect to a patent applicable to software (including a cross-claim or counterclaim in a lawsuit), then any patent licenses granted by that Contributor to such Recipient under this Agreement shall terminate as of the date such litigation is filed. In addition, if Recipient institutes patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Program itself (excluding combinations of the Program with other software or hardware) infringes such Recipient's patent(s), then such Recipient's rights granted under Section 2(b) shall terminate as of the date such litigation is filed.

All Recipient's rights under this Agreement shall terminate if it fails to comply with any of the material terms or conditions of this Agreement and does not cure such failure in a reasonable period of time after becoming aware of such noncompliance. If all Recipient's rights under this Agreement terminate, Recipient agrees to cease use and distribution of the Program as soon as reasonably practicable. However, Recipient's obligations under this Agreement and any licenses granted by Recipient relating to the Program shall continue and survive.

Everyone is permitted to copy and distribute copies of this Agreement, but in order to avoid inconsistency the Agreement is copyrighted and may only be modified in the following manner. The Agreement Steward reserves the right to publish new versions (including revisions) of this Agreement from time to time. No one other than the Agreement Steward has the right to modify this Agreement. IBM is the initial Agreement Steward. IBM may assign the responsibility to serve as the Agreement Steward to a suitable separate entity. Each new version of the Agreement will be given a distinguishing version number. The Program (including Contributions) may always be distributed subject to the version of the Agreement under which it was received. In addition, after a new version of the Agreement is published, Contributor may elect to distribute the Program (including its Contributions) under the new version. Except as expressly stated in Sections 2(a) and 2(b) above, Recipient receives no rights or licenses to the intellectual property of any Contributor under this Agreement, whether expressly, by implication, estoppel or otherwise. All rights in the Program not expressly granted under this Agreement are reserved.

This Agreement is governed by the laws of the State of New York and the intellectual property laws of the United States of America. No party to this Agreement will bring a legal action under this Agreement more than one year after the cause of action arose. Each party waives its rights to a jury trial in any resulting litigation.

# ZLIB 1.0.4, 1.0.8, 1.2.2, 1.2.3

**Copyright (C) 1995-2010, Jean-loup Gailly and Mark Adler**

---

This software is provided "as-is", without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of 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 following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly

Mark Adler

# MOYENS D'EXPLOITATION

Les moyens d'exploitation, les instruments et les autres moyens des éditeurs tiers ont été utilisés pour créer l'application.

## DANS CETTE SECTION



# MS DDK 4.0, 2000

**Copyright (C) Microsoft Corporation**

---

# MS WDK 6000, 6001, 6002

**Copyright (C) 2001-2007, Microsoft Corporation**

---

# WINDOWS INSTALLER XML (WIX) TOOLSET 3.0

**Copyright (C) Microsoft Corporation**

---

Common Public License Version 1.0

THE ACCOMPANYING PROGRAM IS PROVIDED UNDER THE TERMS OF THIS COMMON PUBLIC LICENSE ("AGREEMENT"). ANY USE, REPRODUCTION OR DISTRIBUTION OF THE PROGRAM CONSTITUTES RECIPIENT'S ACCEPTANCE OF THIS AGREEMENT.

1. DEFINITIONS

"Contribution" means:

a) in the case of the initial Contributor, the initial code and documentation distributed under this Agreement, and

b) in the case of each subsequent Contributor:

i) changes to the Program, and

ii) additions to the Program;

where such changes and/or additions to the Program originate from and are distributed by that particular Contributor. A Contribution 'originates' from a Contributor if it was added to the Program by such Contributor itself or anyone acting on such Contributor's behalf. Contributions do not include additions to the Program which: (i) are separate modules of software distributed in conjunction with the Program under their own license agreement, and (ii) are not derivative works of the Program.

"Contributor" means any person or entity that distributes the Program.

"Licensed Patents" mean patent claims licensable by a Contributor which are necessarily infringed by the use or sale of its Contribution alone or when combined with the Program.

"Program" means the Contributions distributed in accordance with this Agreement.

"Recipient" means anyone who receives the Program under this Agreement, including all Contributors.

2. GRANT OF RIGHTS

a) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free copyright license to reproduce, prepare derivative works of, publicly display, publicly perform, distribute and sublicense the Contribution of such Contributor, if any, and such derivative works, in source code and object code form.

b) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free patent license under Licensed Patents to make, use, sell, offer to sell, import and otherwise transfer the Contribution of such Contributor, if any, in source code and object code form. This patent license shall apply to the combination of the Contribution and the Program if, at the time the Contribution is added by the Contributor, such addition of the Contribution causes such combination to be covered by the Licensed Patents. The patent license shall not apply to any other combinations which include the Contribution. No hardware per se is licensed hereunder.

c) Recipient understands that although each Contributor grants the licenses to its Contributions set forth herein, no assurances are provided by any Contributor that the Program does not infringe the patent or other intellectual property rights of any other entity. Each Contributor disclaims any liability to Recipient for claims brought by any other entity based on infringement of intellectual property rights or otherwise. As a condition to exercising the rights and licenses granted hereunder, each Recipient hereby assumes sole responsibility to secure any other intellectual property rights needed, if any. For example, if a third party patent license is required to allow Recipient to distribute the Program, it is Recipient's responsibility to acquire that license before distributing the Program.

d) Each Contributor represents that to its knowledge it has sufficient copyright rights in its Contribution, if any, to grant the copyright license set forth in this Agreement.

3. REQUIREMENTS

A Contributor may choose to distribute the Program in object code form under its own license agreement, provided that:

a) it complies with the terms and conditions of this Agreement; and

b) its license agreement:

i) effectively disclaims on behalf of all Contributors all warranties and conditions, express and implied, including warranties or conditions of title and non-infringement, and implied warranties or conditions of merchantability and fitness for a particular purpose;

ii) effectively excludes on behalf of all Contributors all liability for damages, including direct, indirect, special, incidental and consequential damages, such as lost profits;

iii) states that any provisions which differ from this Agreement are offered by that Contributor alone and not by any other party; and

iv) states that source code for the Program is available from such Contributor, and informs licensees how to obtain it in a reasonable manner on or through a medium customarily used for software exchange.

When the Program is made available in source code form:

a) it must be made available under this Agreement; and

b) a copy of this Agreement must be included with each copy of the Program.

Contributors may not remove or alter any copyright notices contained within the Program.

Each Contributor must identify itself as the originator of its Contribution, if any, in a manner that reasonably allows subsequent Recipients to identify the originator of the Contribution.

4. COMMERCIAL DISTRIBUTION

Commercial distributors of software may accept certain responsibilities with respect to end users, business partners and the like. While this license is intended to facilitate the commercial use of the Program, the Contributor who includes the Program in a commercial product offering should do so in a manner which does not create potential liability for other Contributors. Therefore, if a Contributor includes the Program in a commercial product offering, such Contributor ("Commercial Contributor") hereby agrees to defend and indemnify every other Contributor ("Indemnified Contributor") against any losses, damages and costs (collectively "Losses") arising from claims, lawsuits and other legal actions brought by a third party against the Indemnified Contributor to the extent caused by the acts or omissions of such Commercial Contributor in connection with its distribution of the Program in a commercial product offering. The obligations in this section do not apply to any claims or Losses relating to any actual or alleged intellectual property infringement. In order to qualify, an Indemnified Contributor must: a) promptly notify the Commercial Contributor in writing of such claim, and b) allow the Commercial Contributor to control, and cooperate with the Commercial Contributor in, the defense and any related settlement negotiations. The Indemnified Contributor may participate in any such claim at its own expense.

For example, a Contributor might include the Program in a commercial product offering, Product X. That Contributor is then a Commercial Contributor. If that Commercial Contributor then makes performance claims, or offers warranties related to Product X, those performance claims and warranties are such Commercial Contributor's responsibility alone. Under this section, the Commercial Contributor would have to defend claims against the other Contributors related to those performance claims and warranties, and if a court requires any other Contributor to pay any damages as a result, the Commercial Contributor must pay those damages.

5. NO WARRANTY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, THE PROGRAM IS PROVIDED ON AN "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OR CONDITIONS OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Each Recipient is solely responsible for determining the appropriateness of using and distributing the Program and assumes all risks associated with its exercise of rights under this Agreement, including but not limited to the risks and costs of program errors, compliance with applicable laws, damage to or loss of data, programs or equipment, and unavailability or interruption of operations.

6. DISCLAIMER OF LIABILITY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, NEITHER RECIPIENT NOR ANY CONTRIBUTORS SHALL HAVE ANY LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOST PROFITS), 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 OR DISTRIBUTION OF THE PROGRAM OR THE EXERCISE OF ANY RIGHTS GRANTED HEREUNDER, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. GENERAL

If any provision of this Agreement is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Agreement, and without further action by the parties hereto, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

If Recipient institutes patent litigation against a Contributor with respect to a patent applicable to software (including a cross-claim or counterclaim in a lawsuit), then any patent licenses granted by that Contributor to such Recipient under this Agreement shall terminate as of the date such litigation is filed. In addition, if Recipient institutes patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Program itself (excluding combinations of the Program with other software or hardware) infringes such Recipient's patent(s), then such Recipient's rights granted under Section 2(b) shall terminate as of the date such litigation is filed.

All Recipient's rights under this Agreement shall terminate if it fails to comply with any of the material terms or conditions of this Agreement and does not cure such failure in a reasonable period of time after becoming aware of such noncompliance. If all Recipient's rights under this Agreement terminate, Recipient agrees to cease use and distribution of the Program as soon as reasonably practicable. However, Recipient's obligations under this Agreement and any licenses granted by Recipient relating to the Program shall continue and survive.

Everyone is permitted to copy and distribute copies of this Agreement, but in order to avoid inconsistency the Agreement is copyrighted and may only be modified in the following manner. The Agreement Steward reserves the right to publish new versions (including revisions) of this Agreement from time to time. No one other than the Agreement Steward has the right to modify this Agreement. IBM is the initial Agreement Steward. IBM may assign the responsibility to serve as the Agreement Steward to a suitable separate entity. Each new version of the Agreement will be given a distinguishing version number. The Program (including Contributions) may always be distributed subject to the version of the Agreement under which it was received. In addition, after a new version of the Agreement is published, Contributor may elect to distribute the Program (including its Contributions) under the new version. Except as expressly stated in Sections 2(a) and 2(b) above, Recipient receives no rights or licenses to the intellectual property of any Contributor under this Agreement, whether expressly, by implication, estoppel or otherwise. All rights in the Program not expressly granted under this Agreement are reserved.

This Agreement is governed by the laws of the State of New York and the intellectual property laws of the United States of America. No party to this Agreement will bring a legal action under this Agreement more than one year after the cause of action arose. Each party waives its rights to a jury trial in any resulting litigation.

# CODE D'APPLICATION DIFFUSE

Le code d'application indépendant des éditeurs tiers de type d'origine ou binaire sans modifications est diffusé dans la composition de l'application.

## DANS CETTE SECTION

# GRUB4DOS 0.4.4-2009-10-16 (FILE GRLDR)

**Copyright (C) 1999, 2000, 2001, 2002, 2004, 2005 Free Software Foundation, Inc**

---

GNU GENERAL PUBLIC 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.

# GRUBINST 1.1

**Copyright (C) 2007, Bean (bean123ch@gmail.com)**

---

GNU GENERAL PUBLIC LICENSE

Version 3, 29 June 2007

Copyright © 2007 Free Software Foundation, Inc. <http://fsf.org/>

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The GNU General Public License is a free, copyleft license for software and other kinds of works.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free software for all its users. We, the Free Software Foundation, use the GNU General Public License for most of our software; it applies also to any other work released this way by its authors. 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 them 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 prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. 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.

Developers that use the GNU GPL protect your rights with two steps: (1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS

0. Definitions.

"This License" refers to version 3 of the GNU General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

"The Program" refers to any copyrightable work licensed under this License. Each licensee is addressed as "you". "Licensees" and "recipients" may be individuals or organizations.

To "modify" a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a "modified version" of the earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based on the Program.

To "propagate" a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays "Appropriate Legal Notices" to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The "source code" for a work means the preferred form of the work for making modifications to it. "Object code" means any non-source form of a work.

A "Standard Interface" means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The "System Libraries" of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A "Major Component", in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The "Corresponding Source" for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the

covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

4. Conveying Verbatim Copies.

You may convey 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; keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified it, and giving a relevant date.

b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to "keep intact all notices".

c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.

d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an "aggregate" if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software

interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.

d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A "User Product" is either (1) a "consumer product", which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, "normally used" refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

"Installation Information" for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

"Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or

b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or

c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or

d) Limiting the use for publicity purposes of names of licensors or authors of the material; or

e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or

f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered "further restrictions" within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An "entity transaction" is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A "contributor" is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's "contributor version".

A contributor's "essential patent claims" are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, "control" includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To "grant" such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. "Knowingly relying" means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is "discriminatory" if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If 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 convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU 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 that a certain numbered version of the GNU General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

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.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS 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.

17. Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

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 state 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 a brief idea of what it does.>

Copyright (C) <year> <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 3 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, see <http://www.gnu.org/licenses/>.

Also add information on how to contact you by electronic and paper mail.

If the program does terminal interaction, make it output a short notice like this when it starts in an interactive mode:

<program> Copyright (C) <year> <name of author>

This program 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, your program's commands might be different; for a GUI interface, you would use an "about box".

You should also get your employer (if you work as a programmer) or school, if any, to sign a "copyright disclaimer" for the program, if necessary. For more information on this, and how to apply and follow the GNU GPL, see <http://www.gnu.org/licenses/>.

The GNU 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. But first, please read <http://www.gnu.org/philosophy/why-not-lgpl.html>.

# AUTRES INFORMATIONS

L'analyse de la signature numérique électronique dans Kaspersky Anti-Virus repose sur la bibliothèque logicielle de protection de l'information "Crypto-Si" développée par CryptoEx OOO http://www.cryptoex.ru.

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



## E



## F



## I



## M

## N



## P



## Q



## R



## S

## Z