# Kaspersky PURE


## Manuel de l’utilisateur

VERSION DE L’APPLICATION : 3.0

Cher utilisateur,

Merci d'avoir choisi notre produit. Nous espérons que ce document vous aidera dans votre travail et répondra à la plupart des problèmes émergents.



Ce document peut être modifié sans 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 : 04/12/2012



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

# TABLE DES MATIERES

# PRESENTATION DU GUIDE

Ce document est le guide de l'utilisateur de Kaspersky PURE.

Pour tirer le meilleur parti de l'utilisation de Kaspersky PURE, l'utilisateur doit connaître l'interface du système d'exploitation utilisé, maîtriser les principales tâches et maîtrise du courrier électronique et d'Internet.

Ce guide poursuit les objectifs suivants :

- Aider à installer Kaspersky PURE, à activer l'application et à l'utiliser.
- Offrir un accès rapide aux informations pour répondre aux questions liées à l'application.
- Présenter les sources complémentaires d'informations sur l'application et les modes d'obtention du Support Technique.

### DANS CETTE SECTION



# CONTENU DU GUIDE

Ce document contient les sections suivantes.

### Sources d'informations sur l'application

Cette section contient la description des sources d'informations sur l'application et les renseignements sur les sites Internet que vous pouvez consulter pour discuter du fonctionnement de l'application.

### Kaspersky PURE

Cette section décrit les possibilités de l'application et offre une brève description des fonctionnalités et des modules. Vous y découvrirez le contenu de la distribution et les services offerts aux utilisateurs enregistrés. La section fournit des informations sur la configuration matérielle et logicielle requise pour l'installation de l'application.

### Installation et suppression de l'application

Cette section explique, étape par étape, comment installer et désinstaller l'application.

### Licence de l'application

Cette section présente les notions principales relatives à l'activation de l'application. Cette section explique le rôle du Contrat de licence, les types de licence, les modes d'activation de l'application et le renouvellement de la licence.

### Résolution des problèmes types

Cette section explique, étape par étape, comment exécuter les principales tâches que l'utilisateur peut accomplir à l'aide de l'application.

### Contacter le Support Technique

Cette section contient des informations sur moyens de contacter le Support Technique de Kaspersky Lab.

### Annexes

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

### Glossaire

Cette section contient une liste des termes qui apparaissent dans ce document et leur définition.

### Kaspersky Lab

Cette section contient des informations sur Kaspersky Lab ZAO.

### Informations sur le code tiers

Cette section contient des informations sur le code tiers utilisé dans l'application.

### Notice sur les marques de commerce

Cette section cite les marques commerciales d'autres propriétaires cités dans le document.

### Index

Cette section permet de trouver rapidement les informations souhaitées dans le document.

# CONVENTIONS

Le texte du document est suivi des éléments de sens sur lesquels nous attirons votre attention : avertissements, conseils, exemples.

Les conventions sont utilisées pour identifier les éléments de sens. Les conventions et les exemples de leur utilisation sont repris dans le tableau ci-dessous.

*Tableau 1. Conventions*

| EXEMPLE DU TEXTE | DESCRIPTION DE LA CONVENTION |
|---|---|
| N'oubliez pas que... | Les avertissements apparaissent en rouge et sont encadrés.<br>Les avertissements contiennent les informations sur les actions indésirables potentielles qui peuvent amener à la perte des informations ou à la perturbation du fonctionnement du matériel ou du système d'exploitation. |
| Il est conseillé d'utiliser... | Les remarques sont encadrées.<br>Les remarques peuvent contenir des conseils utiles, des recommandations, des valeurs importantes de paramètres ou des cas particuliers importants dans le fonctionnement de l'application. |
| **Exemple** :<br>... | Les exemples sont présentés sur un fond jaune sous le titre "Exemple". |

| EXEMPLE DU TEXTE | DESCRIPTION DE LA CONVENTION |
|---|---|
| La *mise à jour*, c'est...<br>L'événement *Bases dépassées* survient. | Les éléments de sens suivants sont en italique :<br>• nouveaux termes ;<br>• noms des états et des événements de l'application. |
| Appuyez sur la touche **ENTER**.<br>Appuyez sur la combinaison des touches **ALT**+**F4**. | Les noms des touches du clavier sont en caractères mi-gras et en lettres majuscules.<br>Deux noms de touche unis par le caractère "+" représentent une combinaison de touches. Il faut appuyer simultanément sur ces touches. |
| Cliquez sur le bouton **Activer**. | Les noms des éléments de l'interface de l'application, par exemple, les champs de saisie, les options du menu, les boutons, sont en caractères mi-gras. |
| ➧ *Pour programmer une tâche, procédez comme suit :* | Les phrases d'introduction des instructions sont en italique et ont l'icône "flèche". |
| Dans la ligne de commande, saisissez le texte help<br>Les informations suivantes s'affichent :<br>Indiquez la date au format JJ:MM:AA. | Les types suivants du texte apparaissent dans un style spécial :<br>• texte de la ligne de commande ;<br>• texte des messages affichés sur l'écran par l'application ;<br>• données à saisir par l'utilisateur. |
| <Nom d'utilisateur> | Les variables sont écrites entre chevrons. La valeur correspondant à la variable remplace cette variable. Par ailleurs, les parenthèses angulaires sont omises. |

# SOURCES D'INFORMATIONS SUR L'APPLICATION

Cette section contient la description des sources d'informations sur l'application et les renseignements sur les sites Internet que vous pouvez consulter pour discuter du fonctionnement de l'application.

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 LES RECHERCHES INDEPENDANTES

Vous pouvez utiliser les sources suivantes pour rechercher les informations sur l'application :

- page sur le site Internet de Kaspersky Lab ;
- page sur le site Internet du Support Technique (Base des connaissances) ;
- aide électronique ;
- documentation.

Si vous ne trouvez pas la solution à votre problème, nous vous conseillons de contacter le Support Technique de Kaspersky Lab (cf. section "Assistance technique par téléphone" à la page 76).

Une connexion Internet est requise pour utiliser les sources d'informations sur le site Internet de Kaspersky Lab.

### Page sur le site Internet de Kaspersky Lab

Le site Internet de Kaspersky Lab contient une page particulière pour chaque application.

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

La page contient le lien vers la boutique en ligne. Ce lien permet d'acheter l'application ou de renouveler le droit d'utilisation de l'application.

### Page sur le site Internet du service du Support Technique (Base des connaissances)

La Base des connaissances est une section du site Internet du Support Technique contenant les recommandations pour travailler avec les applications de Kaspersky Lab. La Base de connaissance est composée des articles d'aide regroupés selon les thèmes.

La page de l'application dans la Base des connaissances (http://support.kaspersky.com/fr/pure2) permet de trouver les articles qui proposent des informations utiles, des recommandations et des réponses aux questions fréquemment posées sur l'achat, l'installation et l'utilisation de l'application.

Les articles peuvent répondre à des questions en rapport non seulement avec Kaspersky PURE, mais également avec d'autres applications de Kaspersky Lab. De plus, ils peuvent fournir des informations sur l'assistance technique en général.

### Aide électronique

L'aide électronique de l'application est composée de fichiers d'aide.

L'aide contextuelle contient les informations sur chaque fenêtre de l'application : la liste et la description des paramètres et la liste des tâches à effectuer.

L'aide complète contient les détails sur la gestion de la protection, la configuration des paramètres de l'application et l'exécution des tâches principales pour l'utilisateur.

### Documentation

Le guide de l'utilisateur contient les informations sur l'installation, l'activation, la configuration des paramètres, ainsi que sur la manière d'utiliser l'application. Il décrit l'interface graphique et l'exécution des tâches les plus fréquentes.

## DISCUSSION SUR LES LOGICIELS DE KASPERSKY LAB SUR LE FORUM

Si votre question n'est pas urgente, vous pouvez la soumettre aux experts de Kaspersky Lab et aux autres utilisateurs de nos applications sur notre forum (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 VENTE

Si vous avez des questions sur la sélection, sur l'achat ou sur le renouvellement de la licence, vous pouvez contacter nos experts du Service commercial à l'aide d'un des moyens suivants :

- En appelant notre siège central à Moscou (http://www.kaspersky.com/fr/about/contactinfo).
- En envoyant un message avec votre question à l'adresse électronique sales@kaspersky.com.

La réponse sera formulée en français ou en anglais suivant votre demande.

## CONTACTER LE SERVICE DE LOCALISATION ET DE REDACTION DE LA DOCUMENTATION TECHNIQUE

Si vous avez des questions sur la documentation de l'application, vous pouvez contacter les membres du groupe de rédaction de la documentation. Vous pouvez par exemple faire parvenir des commentaires sur la documentation à nos experts.

# KASPERSKY PURE

Cette section décrit les possibilités de l'application et offre une brève description des fonctionnalités et des modules. Vous y découvrirez le contenu de la distribution et les services offerts aux utilisateurs enregistrés. La section fournit des informations sur la configuration matérielle et logicielle requise pour l'installation de l'application.

### DANS CETTE SECTION



# NOUVEAUTES

Les capacités suivantes ont été introduites dans Kaspersky PURE :

- Pour une utilisation sécurisée des services de banque en ligne et des systèmes de paiement dans les boutiques en ligne, la Protection des transactions bancaires a été ajoutée (cf. page 45).
- Amélioration de la protection contre les enregistreurs de frappes qui interceptent les données personnelles saisies sur les sites Internet :
  - Ajout de la Protection des données saisies au clavier (cf. page 49)
  - L'application ajoute automatiquement le bouton de lancement du clavier virtuel (cf. section "Utilisation du clavier virtuel" à la page 47) dans le champ de saisie du mot de passe sur les sites Internet.
- Possibilité d'utiliser la Stockage en ligne (cf. section "Utilisation du Stockage en ligne" à la page 63) pour enregistrer les copies de sauvegarde des fichiers. Ceci augmente la sécurité du stockage des informations et simplifie l'accès aux données grâce aux technologies du Cloud.
- Pour empêcher un individu malintentionné d'utiliser les vulnérabilités de votre ordinateur, la fonction de protection contre les Exploits a été ajoutée dans la Surveillance du système.
- Amélioration du Gestionnaire de mots de passe Vous pouvez désormais enregistrée la base de mots de passe sur des serveurs distants. Grâce à la synchronisation, les mots de passe et les données personnelles à jour seront accessibles sur tous les ordinateurs portables et de bureau dotés de Kaspersky PURE.
- L'interface de Kaspersky PURE a été améliorée : introduction de fenêtres contextuelles proposant des informations utiles sur l'utilisation de l'application.
- La procédure d'installation de l'application (cf. section "Installation et suppression de l'application" à la page 17) a été simplifiée. Possibilité d'installer automatiquement la dernière version de Kaspersky PURE qui contient l'ensemble des dernières mises à jour des bases de l'application.
- La taille des bases a été diminuée, ce qui permet de réduire le volume des données téléchargées et accélérer l'installation des mises à jour.

- L'analyse heuristique, exécutée lors de l'analyse des sites Internet à la recherche de phishing, a été améliorée.
- Reformulation des messages du Contrôle Parental destinés aux enfants. Amélioration de la précision du fonctionnement du Contrôle Parental : ce module est désormais capable d'utiliser la technologie du Cloud pour identifier le contenu indésirable sur un site Internet.

# FONCTIONNALITES PRINCIPALES DE L'APPLICATION

Kaspersky PURE offre une protection complète pour votre ordinateur. La protection complète inclut la protection de l'ordinateur, la protection des données et la protection des utilisateurs ainsi que l'administration à distance des fonctions de Kaspersky PURE sur tous les postes du réseau. Pour remplir les fonctions liées à la protection complète, Kaspersky PURE propose différents fonctions et modules de protection.

### Protection de l'ordinateur

Les *modules de protection* ont été développés pour protéger les ordinateurs contre les menaces connues ou non, les attaques réseau, les escroqueries, les messages non sollicités et les informations indésirables. Chaque type de menace est pris en charge par un module de protection particulier (cf. la description des modules ci-après). Les modules peuvent être activés, désactivés et configurés indépendamment les uns des autres.

En plus de la protection en temps réel effectuée par les modules de protection, il est recommandé d'*analyser* périodiquement votre ordinateur pour déceler d'éventuels virus. Cette opération est indispensable pour éviter le risque de propagation de programmes malveillants qui n'ont pas été détectés par les modules de protection, par exemple si le niveau de protection est trop faible ou pour toute autre raison.

Afin de maintenir Kaspersky PURE à jour, il faut *mettre à jour* les bases et les modules logiciels exploités par l'application.

Les applications dont vous n'êtes pas sûr peuvent être lancées dans un *environnement protégé* spécial.

Certaines tâches spécifiques qui requièrent une exécution périodique sont exécutées à l'aide d'outils et d'*Assistants d'optimisation* : par exemple, la configuration du navigateur Microsoft® Internet Explorer® ou la suppression des traces d'activité de l'utilisateur dans le système.

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

Vous trouverez ci-après une description du fonctionnement des modules de protection selon le mode de fonctionnement de Kaspersky PURE recommandé par les experts de Kaspersky Lab (à savoir, selon les paramètres par défaut).

Antivirus Fichiers

L'Antivirus Fichiers permet d'éviter l'infection du système de fichiers de l'ordinateur. Le module 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 connectés. Kaspersky PURE intercepte chaque requête adressée à un fichier et vérifie si ce fichier contient des virus connus. La suite de l'utilisation du fichier est possible uniquement si le fichier 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 analyse le courrier entrant et sortant sur votre ordinateur. Tout message sera remis à son destinataire uniquement s'il ne contient aucun objet dangereux.

Antivirus Internet

L'Antivirus Internet intercepte et bloque l'exécution de scripts situés sur des sites Internet si ces scripts constituent une menace pour la sécurité de l'ordinateur. L'Antivirus Internet contrôle également tout le trafic Internet et bloque l'accès aux sites dangereux.

Antivirus IM ("Chat")

L'Antivirus IM ("Chat") garantit la sécurité de l'utilisation des messageries instantanées. Le module protège les informations envoyées vers votre ordinateur via les protocoles des clients de messagerie instantanée. L'Antivirus IM ("Chat") 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 nuire à l'ordinateur. Le module repose sur la surveillance et l'analyse du comportement de toutes les applications installées sur l'ordinateur. En fonction des actions réalisées par une application, Kaspersky PURE détermine si celle-ci constitue 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.

Contrôle des Applications

Le Contrôle des Applications enregistre les actions effectuées par les applications dans le système et réglemente l'activité des applications en fonction du groupe dans lequel le module place cette application. Il existe un ensemble de règles défini pour chaque groupe. 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 module filtre l'activité réseau selon deux types de règles : *règles pour les applications* et *règles pour les paquets*.

Surveillance du réseau

La Surveillance du réseau a été mise au point pour observer en temps réel l'activité réseau.

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 réseau. Dès qu'il détecte une tentative d'attaque contre l'ordinateur, Kaspersky PURE bloque toute activité 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 reçoivent un en-tête spécial. Vous pouvez configurer les actions de l'Anti-Spam sur les messages non sollicités (par exemple, suppression automatique, placement dans un dossier spécial).

Anti-Phishing

L'Anti-Phishing permet de déterminer si une adresse Internet quelconque figure dans la liste des URL malveillantes ou de phishing. Ce module est intégré à l'Antivirus Internet, à l'Anti-Spam et à l'Antivirus IM ("chat").

Anti-bannière

L'Anti-bannière bloque les bannières qui apparaissent sur les sites Internet et dans l'interface des applications.

Protection des transactions bancaires

La Protection des transactions bancaires assure la protection des données confidentielles lors de l'utilisation des services des banques en ligne et des systèmes de paiement et prévient aussi le vol des instruments de paiement lors des paiements en ligne.

### Protection des informations

Afin de protéger les données contre la perte, l'accès non autorisé ou le vol, l'application propose les fonctions Sauvegarde, Cryptage des données et Gestionnaire de mots de passe.

Sauvegarde

Plusieurs causes peuvent être à l'origine de la perte ou de l'endommagement de données, par exemple l'attaque d'un virus, la suppression ou la modification de données par un autre utilisateur. Pour éviter la perte de données importantes, il est primordial de réaliser des sauvegardes des données à intervalle régulier.

Comme son nom l'indique, la Sauvegarde permet de créer des copies de sauvegarde des données dans un stockage spécial sur le support sélectionné. Il faut configurer pour ce faire une tâche de sauvegarde. Après le lancement manuel ou automatique (selon une programmation) de la tâche, les copies de sauvegarde des fichiers sélectionnés sont créées dans le stockage. Le cas échéant, il sera possible de restaurer la version requise du fichier au départ de la copie de sauvegarde.

Mon Coffre-fort

Les données confidentielles conservées au format électronique ont besoin d'une protection complémentaire contre l'accès non autorisé. Une telle protection permet de conserver les données dans un coffre-fort crypté.

La fonction Cryptage des données crée des coffres-forts cryptés spéciaux sur le support sélectionné. Ces coffres-forts apparaissent dans le système comme des disques amovibles virtuels. Pour pouvoir accéder aux données contenues dans ce coffre-fort, il faut saisir un mot de passe.

Gestionnaire de mots de passe

L'accès à la majorité des ressources et des services sur Internet requiert une inscription et la saisie des données du compte utilisateur. Pour des questions de sécurité, il est conseillé d'utiliser des noms d'utilisateur et des mots de passe différents pour chaque service et de ne pas enregistrer ceux-ci.

Le Gestionnaire de mots de passe est une solution qui permet de conserver, sous forme chiffrée, les données d'identification de différents comptes utilisateur (par exemple, les noms, les mots de passe, les cartes de crédit, les numéros de téléphone, etc.) L'accès aux données est protégé par un mot de passe principal. Une fois le mot de passe principal saisi, le Gestionnaire de mots de passe permet de remplir automatiquement les champs de divers formulaires d'autorisation sur des sites Internet. Le mot de passe principal permet de gérer tous vos comptes utilisateurs sur des sites Internet.

### Contrôle Parental

Les fonctions du Contrôle Parental visent à protéger les enfants et les adolescents des menaces qu'ils pourraient croiser sur l'ordinateur et sur Internet.

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

### Mon Réseau

Souvent, un réseau domestique est composé de plusieurs ordinateurs, ce qui complique la gestion de la sécurité. Un ordinateur vulnérable peut mettre en jeu la sécurité de tout le réseau.

Mon Réseau permet de lancer les tâches d'analyse et de mise à jour sur tous les ordinateurs du réseau ou sur certains d'entre eux, de gérer la sauvegarde des données et de configurer les paramètres du Contrôle Parental sur l'ensemble des postes du réseau directement depuis le Bureau. L'administration à distance de tous les postes du réseau est ainsi garantie.

# DISTRIBUTION

Vous pouvez acheter l'application sous une des formes suivantes :

- **Dans une boîte**. Le produit est distribué via notre réseau de partenaires.
- **Via la boutique en ligne**. L'application peut être achetée dans la boutique en ligne de Kaspersky Lab (par exemple http://www.kaspersky.com/fr, section **Boutique en ligne**) ou sur le site d'un partenaire.

Si vous achetez le produit en boîte, vous recevez les éléments suivants :

- pochette cachetée contenant le cédérom d'installation où sont enregistrés les fichiers de l'application et la documentation de l'application ;
- bref manuel de l'utilisateur contenant le code d'activation de l'application ;
- Contrat de licence reprenant les conditions d'utilisation de l'application.

Ces éléments peuvent varier en fonction du pays où l'application est diffusée.

Si vous achetez Kaspersky PURE via la boutique en ligne, vous devrez télécharger l'application depuis le site Internet. Les informations indispensables à l'activation de l'application vous seront envoyées par courrier électronique après le paiement.

Pour en savoir plus sur les modes d'achat et de distribution, contactez notre Service vente sales@kaspersky.com.

# SERVICE POUR LES UTILISATEURS

Quand vous acheté une licence d'utilisation de l'application, vous pouvez obtenir les services suivants pendant la durée de validité de la licence :

- mise à jour des bases et nouvelles versions de l'application ;
- support par téléphone et par courrier électronique sur toutes les questions en rapport avec l'installation, la configuration et l'utilisation de l'application ;
- notification sur la sortie de nouvelles applications de Kaspersky Lab et informations sur l'émergence de nouveaux virus ou le déclenchement d'épidémies de virus. Pour bénéficier de ce service, vous devez être abonné à la diffusion d'informations de Kaspersky Lab ZAO sur le site Internet du Support Technique.

Aucun support ne sera apporté sur l'utilisation du système d'exploitation ou des logiciels tiers.

# CONFIGURATIONS LOGICIELLE ET MATERIELLE

Afin de garantir un fonctionnement optimal de Kaspersky PURE, votre ordinateur doit répondre au minimum à la configuration suivante :

Recommandations d'ordre général :

- Espace disponible sur le disque dur : 700 Mo.
- CD-/DVD-ROM (pour l'installation de Kaspersky PURE depuis un cédérom).
- Souris.
- Connexion à Internet (pour l'activation de l'application et la mise à jour des bases ou modules de l'application).
- Microsoft Internet Explorer 8.0 ou suivant.
- Microsoft Windows® Installer 3.0.

Exigences pour les systèmes d'exploitation Microsoft Windows XP Home Edition (Service Pack 3 ou suivant), Microsoft Windows XP Professional (Service Pack 3 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.

Configuration requise pour le système d'exploitation Microsoft Windows Vista® Home Basic (Service Pack 2 ou suivant), Microsoft Windows Vista Home Premium (Service Pack 2 ou suivant), Microsoft Windows Vista Business (Service Pack 2 ou suivant), Microsoft Windows Vista Enterprise (Service Pack 2 ou suivant), Microsoft Windows Vista Ultimate (Service Pack 2 ou suivant), Microsoft Windows 7 Starter (Service Pack 1 ou suivant), Microsoft Windows 7 Home Basic (Service Pack 1 ou suivant), Microsoft Windows 7 Home Premium (Service Pack 1 ou suivant), Microsoft Windows 7 Professional (Service Pack 1 ou suivant), Microsoft Windows 7 Ultimate (Service Pack 1 ou suivant), Microsoft Windows 8, Microsoft Windows 8 Pro, Windows 8 Enterprise ou suivant (x32 et x64) :

- Processeur Intel Pentium 1 GHz 32 bits (x86)/ 64 bits (x64) ou supérieur (ou analogue compatible) ;
- 1 Go de mémoire vive disponible (pour les systèmes d'exploitation de 32 bits) ; 2 Go de mémoire vive disponible (pour les systèmes d'exploitation de 64 bits).

Exigences pour les netbooks :

- Processeur Intel Atom™ 1,6 MHz (Z520) ou analogue compatible.
- 1 Go de mémoire vive disponible.
- Carte vidéo Intel GMA950 avec une mémoire d'au moins 64 Mo (ou analogue compatible).
- Ecran de 10.1 pouces minimum.

En cas d'utilisation d'une version 64 bits du système d'exploitation, l'application ne prend pas en charge le Gestionnaire de mots de passe.

# INSTALLATION ET SUPPRESSION DE L'APPLICATION

Cette section explique, étape par étape, comment installer et désinstaller l'application.

### DANS CETTE SECTION



## INSTALLATION DE L'APPLICATION SUR L'ORDINATEUR

L'installation de Kaspersky PURE 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 doit protéger plus d'un ordinateur (le nombre maximal d'ordinateurs protégés dépend de votre licence), la procédure d'installation sera identique sur tous les ordinateurs.

- *Pour installer Kaspersky PURE sur l'ordinateur,*

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

Pour installer Kaspersky PURE, vous pouvez utiliser la distribution obtenue sur Internet. L'Assistant d'installation affiche quelques étapes complémentaires d'installation pour certaines langues de localisation.

### DANS CETTE SECTION

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

Avant l'installation, Kaspersky PURE vérifie la présence d'une version de l'application plus récente sur les serveurs de mises à jour de Kaspersky Lab.

Si les serveurs de Kaspersky Lab n'hébergent pas de 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 de Kaspersky PURE, vous serez invité à la télécharger et à l'installer sur votre ordinateur. Il est conseillé d'installer une nouvelle version de l'application afin de bénéficier des nouvelles améliorations qui permettent de protéger votre ordinateur d'une manière plus efficace. 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 votre ordinateur et l'Assistant d'installation de la nouvelle version sera lancé automatiquement. Pour connaître les avantages de la version plus récente, lisez la documentation correspondant à l'application.

## ETAPE 2. DEBUT DE L'INSTALLATION DE L'APPLICATION

A cette étape, l'Assistant d'installation vous propose d'installer l'application.

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

Selon le type d'installation et la langue de localisation, à cette étape l'Assistant d'installation vous propose de prendre connaissance du Contrat de licence qui est conclu entre vous et Kaspersky Lab et vous propose aussi d'accepter de participer au programme Kaspersky Security Network.

## ETAPE 3. CONSULTATION DU CONTRAT DE LICENCE

A 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 **Accepter**. L'installation de l'application se poursuivra.

Si le Contrat de licence n'est pas accepté, l'installation de l'application n'est pas effectuée.

## ETAPE 4. REGLEMENT D'UTILISATION DE KASPERSKY SECURITY NETWORK

Cette étape de l'Assistant d'installation vous propose de participer au programme Kaspersky Security Network. La participation au programme implique l'envoi à Kaspersky Lab, Ltd. d'informations sur les nouvelles menaces détectées sur l'ordinateur, sur les applications exécutées, sur les applications signées et les informations relatives au système. Vos données personnelles ne sont ni recueillies, ni traitées, ni enregistrées.

Lisez les dispositions relatives à l'utilisation de Kaspersky Security Network. Si vous êtes d'accord avec tous les points, cochez la case dans la fenêtre de l'Assistant **Je veux participer au programme Kaspersky Security Network (KSN)**.

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

# ETAPE 5. INSTALLATION

L'installation de l'application peut durer un certain temps. Attendez jusqu'à la fin avant de passer à l'étape suivante.

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

Pendant l'installation, Kaspersky PURE effectue une série de vérifications. Une fois ces vérifications effectuées, les problèmes suivants peuvent être détectés :

- **Non-conformité du système d'exploitation par rapport aux exigences logicielles**. Pendant l'installation, l'Assistant analyse le respect des conditions suivantes :

  - correspondance du système d'exploitation et des paquets des mises à jour (Service Pack) par rapport aux exigences logicielles ;
  - présence des programmes nécessaires ;
  - présence d'espace libre sur le disque nécessaire à l'installation.

  Si une des conditions énumérées n'est pas remplie, un message apparaîtra.

- **Présence de programmes incompatibles sur l'ordinateur**. Si des applications incompatibles sont détectées, une liste s'affichera à l'écran et vous aurez la possibilité de les supprimer. Les applications que Kaspersky PURE ne peut supprimer automatiquement doivent être supprimées manuellement. Au cours de la suppression des applications incompatibles, le redémarrage du système est requis. Ensuite, l'installation de Kaspersky PURE se poursuivra automatiquement.

- **Présence d'applications malveillantes sur l'ordinateur**. En cas de détection d'applications malveillantes sur l'ordinateur qui empêchent l'installation des applications 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 se lancera automatiquement. Si l'Assistant ne parvient pas à télécharger l'utilitaire, il vous proposera de le télécharger vous-même en cliquant sur le lien proposé.

# ETAPE 6. FIN DE L'INSTALLATION

Cette fenêtre de l'Assistant vous signale la fin de l'installation de l'application. Pour commencer à utiliser Kaspersky PURE immédiatement, assurez-vous que la case **Démarrer Kaspersky PURE** est cochée, puis cliquez sur le bouton **Terminer**.

Dans certains cas, le redémarrage du système d'exploitation peut être requis pour terminer l'installation. Si la case **Démarrer Kaspersky PURE** est cochée, l'application sera lancée automatiquement après le redémarrage.

Si avant la fin de l'Assistant vous avez décoché la case **Démarrer Kaspersky PURE 3.0**, il faudra lancer 'application sera manuellement.

# ETAPE 7. ACTIVATION DE L'APPLICATION

A cette étape, l'Assistant d'installation vous propose d'activer l'application.

L'*activation* est une procédure d'activation de la version complète pour une durée de validité définie.

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

Vous avez le choix entre les options suivantes pour activer Kaspersky PURE :

- **Activer la version commerciale**. Sélectionnez cette option et saisissez le code d'activation (cf. section "A propos du code d'activation" à la page 27) si vous avez acheté une version commerciale de l'application.

- **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 durée de validité définie par les termes de la version d'évaluation de la licence. Une fois la licence expirée, vous ne pourrez plus activer la version d'évaluation.

## ETAPE 8. ENREGISTREMENT DE L'UTILISATEUR

Cette étape est accessible uniquement lors de l'activation de la version commerciale de l'application. En cas d'activation de la version d'évaluation, cette étape est ignorée.

Les utilisateurs enregistrés peuvent envoyer des requêtes au Support Technique et au Laboratoire d'étude des virus via Mon Espace Personnel sur le site Internet de Kaspersky Lab, administrer aisément les codes d'activation, ainsi que les informations opérationnelles sur les nouveaux produits et les offres spéciales.

Si vous acceptez de vous enregistrer, saisissez les données requises dans les champs correspondants pour envoyer vos données d'enregistrement à Kaspersky Lab, puis cliquez sur le bouton **Suivant**.

## ETAPE 9. FIN DE L'ACTIVATION

L'Assistant vous signale la réussite de l'activation de Kaspersky PURE. De plus, la fenêtre reprend les informations sur la licence valide : type de licence (commerciale, évaluation, etc.), fin de validité de la licence et nombre d'ordinateurs couverts par cette licence.

En cas d'activation par l'abonnement, les informations relatives à la durée de validité de la licence sont remplacées par des informations sur l'état de l'abonnement.

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

# MISE A JOUR DE LA VERSION ANTERIEURE DE KASPERSKY PURE

Si votre ordinateur est doté de la version précédente de Kaspersky PURE, il faudra la mettre à jour jusque à la version la plus récente. Si vous possédez une licence valide de Kaspersky PURE, il n'est pas nécessaire d'activer l'application : l'Assistant d'installation reçoit automatiquement les informations sur la licence de Kaspersky PURE et les utilise pendant l'installation.

L'installation de Kaspersky PURE 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 doit protéger plus d'un ordinateur (le nombre maximal d'ordinateurs protégés dépend de votre licence), la procédure d'installation sera identique sur tous les ordinateurs.

➡ *Pour installer Kaspersky PURE sur l'ordinateur,*

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

Pour installer Kaspersky PURE, vous pouvez utiliser la distribution obtenue sur Internet. L'Assistant d'installation affiche quelques étapes complémentaires d'installation pour certaines langues de localisation.

**DANS CETTE SECTION**



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

Avant l'installation, Kaspersky PURE vérifie la présence d'une version de l'application plus récente sur les serveurs de mises à jour de Kaspersky Lab.

Si les serveurs de Kaspersky Lab n'hébergent pas de 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 de Kaspersky PURE, vous serez invité à la télécharger et à l'installer sur votre ordinateur. Il est conseillé d'installer une nouvelle version de l'application afin de bénéficier des nouvelles améliorations qui permettent de protéger votre ordinateur d'une manière plus efficace. 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 votre ordinateur et l'Assistant d'installation de la nouvelle version sera lancé automatiquement. Pour connaître les avantages de la version plus récente, lisez la documentation correspondant à l'application.

# ETAPE 2. DEBUT DE L'INSTALLATION DE L'APPLICATION

A cette étape, l'Assistant d'installation vous propose d'installer l'application.

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

Selon le type d'installation et la langue de localisation, à cette étape l'Assistant d'installation vous propose de prendre connaissance du Contrat de licence qui est conclu entre vous et Kaspersky Lab et vous propose aussi d'accepter de participer au programme Kaspersky Security Network.

# ETAPE 3. CONSULTATION DU CONTRAT DE LICENCE

A 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 **Accepter**. L'installation de l'application se poursuivra.

Si le Contrat de licence n'est pas accepté, l'installation de l'application n'est pas effectuée.

# ETAPE 4. REGLEMENT D'UTILISATION DE KASPERSKY SECURITY NETWORK

Cette étape de l'Assistant d'installation vous propose de participer au programme Kaspersky Security Network. La participation au programme implique l'envoi à Kaspersky Lab, Ltd. d'informations sur les nouvelles menaces détectées sur l'ordinateur, sur les applications exécutées, sur les applications signées et les informations relatives au système. Vos données personnelles ne sont ni recueillies, ni traitées, ni enregistrées.

Lisez les dispositions relatives à l'utilisation de Kaspersky Security Network. Si vous êtes d'accord avec tous les points, cochez la case dans la fenêtre de l'Assistant **Je veux participer au programme Kaspersky Security Network (KSN)**.

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

# ETAPE 5. INSTALLATION

L'installation de l'application peut durer un certain temps. Attendez jusqu'à la fin avant de passer à l'étape suivante.

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

Pendant l'installation, Kaspersky PURE effectue une série de vérifications. Une fois ces vérifications effectuées, les problèmes suivants peuvent être détectés :

- **Non-conformité du système d'exploitation par rapport aux exigences logicielles**. Pendant l'installation, l'Assistant analyse le respect des conditions suivantes :

  - correspondance du système d'exploitation et des paquets des mises à jour (Service Pack) par rapport aux exigences logicielles ;

  - présence des programmes nécessaires ;

  - présence d'espace libre sur le disque nécessaire à l'installation.

  Si une des conditions énumérées n'est pas remplie, un message apparaîtra.

- **Présence de programmes incompatibles sur l'ordinateur**. Si des applications incompatibles sont détectées, une liste s'affichera à l'écran et vous aurez la possibilité de les supprimer. Les applications que Kaspersky PURE ne peut supprimer automatiquement doivent être supprimées manuellement. Au cours de la suppression des applications incompatibles, le redémarrage du système est requis. Ensuite, l'installation de Kaspersky PURE se poursuivra automatiquement.

- **Présence d'applications malveillantes sur l'ordinateur**. En cas de détection d'applications malveillantes sur l'ordinateur qui empêchent l'installation des applications 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 se lancera automatiquement. Si l'Assistant ne parvient pas à télécharger l'utilitaire, il vous proposera de le télécharger vous-même en cliquant sur le lien proposé.

# ETAPE 6. FIN DE L'INSTALLATION

Cette fenêtre de l'Assistant vous signale la fin de l'installation de l'application.

A l'issue de l'installation, il faut redémarrer le système d'exploitation.

Si la case **Lancer Kaspersky PURE** est cochée, l'application sera lancée automatiquement après le redémarrage.

Si avant la fin de l'Assistant vous avez décoché la case **Lancer Kaspersky PURE**, l'application devra être lancée manuellement.

# SUPPRESSION DE L'APPLICATION

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

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

*Pour lancer l'Assistant,*

sélectionnez dans le menu **Démarrer** l'option **Programmes** → **Kaspersky PURE** → **Supprimer Kaspersky PURE**.

### 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).

Vous pouvez désigner les types de données suivants à réutiliser :

- **Information de licence** : données permettant de ne pas activer ultérieurement l'application à installer, mais d'utiliser automatiquement la licence déjà valide, à condition qu'elle soit toujours valable au moment de l'installation.
- **Objets en quarantaine** : fichiers analysés par l'application et placés dans le stockage ou en quarantaine.

  Lors de la suppression de Kaspersky PURE de l'ordinateur, les fichiers en quarantaine ne seront pas disponibles. Pour pouvoir manipuler à nouveau ces fichiers, il faut installer Kaspersky PURE.
- **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.

  Kaspersky Lab ne garantit pas la prise en charge des paramètres de la version antérieure de l'application. Une fois que vous avez installé une version plus récente de l'application, il est conseillé de vérifier si elle a été correctement configurée.
- **Données iChecker** : fichiers contenant les informations sur les objets déjà analysés à l'aide de la technologie iChecker.
- **Coffre-fort sécurisé (avec les données)** : fichiers placés dans les coffres-forts chiffrés à l'aide de la fonction Cryptage des données.
- **Bases du Gestionnaire de mots de passe (pour tous les utilisateurs)** : les comptes utilisateur, les notes personnelles, les signets et les identités créées à l'aide des fonctions du Gestionnaire de mots de passe.
- **Bases de l'Anti-Spam** : bases contenant les modèles des messages non sollicités reçus et enregistrés.

Par défaut, l'application propose d'enregistrer les informations sur l'activation.

- *Pour enregistrer les données pour une réutilisation,*

  cochez les cases en regard des données à enregistrer.

## ETAPE 2. CONFIRMATION DE LA SUPPRESSION

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**.

## 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 requiert 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 éteint et allumé de nouveau.

# LICENCE DE L'APPLICATION

Cette section présente les notions principales relatives à l'activation de l'application. Cette section explique le rôle du Contrat de licence, les types de licence, les modes d'activation de l'application et le renouvellement de la licence.

### DANS CETTE SECTION



# A PROPOS DU CONTRAT DE LICENCE

Le contrat de licence est un accord juridique conclu entre vous et Kaspersky Lab qui prévoit les conditions dans lesquelles vous pouvez utiliser le logiciel que vous avez acheté.

Veuillez lire attentivement les conditions du Contrat de licence avant d'utiliser l'application.

Vous êtes réputé avoir accepté les conditions du Contrat de licence lorsque vous avez décidé d'installer l'application. Si vous n'êtes pas d'accord avec les termes du Contrat de licence, vous devez interrompre l'installation de l'application ou ne pas utiliser l'application.

# A PROPOS DE LA LICENCE

La *licence* est un droit d'utilisation de l'application, limité dans le temps et octroyé dans le cadre du Contrat de licence. La licence est associée à un code d'activation unique de votre copie de Kaspersky PURE.

La licence vous donne droit aux types de service suivants :

- Utilisation de l'application sur un ou plusieurs périphériques.

  Le nombre d'appareils sur lequel vous pouvez utiliser l'application est défini par les termes du Contrat de licence.

- Contacter le Support Technique de Kaspersky Lab.

- Accès aux autres services proposés par Kaspersky Lab ou ses partenaires pendant la durée de validité de la licence (cf. section "Services pour les utilisateurs" à la page 15).

Le volume de services offert et la durée d'utilisation de l'application dépendent du type de licence utilisée pour activer l'application.

Il existe les types de licence suivants :

- *Evaluation* : une licence gratuite conçue pour découvrir l'application.

  En général, la durée de validité d'une licence d'évaluation est brève. Une fois que la licence d'évaluation de Kaspersky PURE arrive à échéance, toutes les fonctions de l'application sont désactivées. Pour pouvoir continuer à utiliser l'application, il faut acheter une licence commerciale.

- *Commerciale* : licence payante octroyée à l'achat de l'application.

  A l'expiration de la licence commerciale, l'application continue à fonctionner, mais ses fonctionnalités sont limitées (par exemple, la mise à jour et l'utilisation de Kaspersky Security Network ne sont pas disponibles). Vous pouvez toujours soumettre l'ordinateur à une analyse antivirus et utiliser tous les modules de l'application et toutes les autres applications, présentant une menace, mais uniquement à l'aide des bases installées avant l'expiration de la licence. Pour pouvoir continuer à utiliser toutes les fonctionnalités de Kaspersky PURE, il faut renouveler la validité de la licence commerciale.

  Il est conseillé de renouveler la durée de validité de la licence avant sa date d'expiration afin de garantir la protection maximale de l'ordinateur contre toutes les menaces.

# PRESENTATION DES DONNEES

Pour augmenter le niveau de protection opérationnel, en acceptant les conditions du Contrat de licence, vous acceptez de fournir automatiquement les informations suivantes à Kaspersky Lab :

- les informations sur les sommes de contrôle des fichiers traités (MD5) ;
- les informations pour définir la réputation URL ;
- les statistiques d'utilisation des notifications de produit ;
- les données statistiques pour la protection contre le courrier indésirable ;
- les données sur l'activation et sur la version utilisée de Kaspersky PURE ;
- les informations sur les types de menaces détectées ;
- les informations sur les certificats numériques utilisés et les informations nécessaires pour vérifier leur authenticité.

Si l'ordinateur est équipé d'un module TPM (Trusted Platform Module), alors vous acceptez de présenter à Kaspersky Lab le rapport TPM sur le démarrage du système d'exploitation de l'ordinateur et les informations nécessaires pour vérifier l'authenticité du rapport. En cas d'erreur d'installation de Kaspersky PURE, vous acceptez de transmettre automatiquement à Kaspersky Lab les informations sur le code de l'erreur, sur le distributif utilisé et sur l'ordinateur.

En participant au programme Kaspersky Security Network, Kaspersky Lab reçoit automatiquement les informations suivantes, reçues lors du fonctionnement de Kaspersky PURE sur l'ordinateur :

- les informations sur les logiciels et le matériel installés ;
- les informations sur l'état de la protection antivirus de l'ordinateur, ainsi que sur tous les objets potentiellement malveillants et les actions et les décisions, prises relativement à ces objets et actions ;
- les informations sur les programmes téléchargés et lancés ;
- les informations sur les erreurs et sur l'utilisation de l'interface utilisateur de Kaspersky PURE ;
- les informations sur la version des bases de l'application utilisées ;

- les statistiques des mises à jour et des connexions aux serveurs de Kaspersky Lab.

- les statistiques sur le temps passé par les modules de l'application à analyser les objets.

Ainsi, des fichiers (ou leurs parties) dont le risque d'utilisation par les individus malintentionnés peut nuire à l'ordinateur ou aux données peuvent être envoyés à Kaspersky Lab pour une analyse complémentaire.

Les informations obtenues sont protégées par Kaspersky Lab conformément aux exigences établies par la loi. Kaspersky Lab utilise les informations obtenues uniquement sous forme de statistiques. Les données générales des statistiques sont automatiquement formées à partir des informations d'origine obtenues et ne contiennent pas les données personnelles ou d'autres informations confidentielles. Les informations d'origine obtenues sont enregistrées sous forme cryptée et sont supprimées au fur et à mesure de leur accumulation (deux fois par an). Les données des statistiques générales sont conservées de manière illimitée.

# A PROPOS DU CODE D'ACTIVATION

Le *code d'activation* est un code que vous obtenez après avoir acheté une licence commerciale et qui vous permet d'utiliser Kaspersky PURE. Ce code est indispensable pour activer l'application.

Le code d'activation est une suite unique de 20 caractères alphanumériques (alphabet latin) au format XXXXX-XXXXX-XXXXX-XXXXX.

En fonction du mode d'acquisition de l'application, vous pouvez obtenir le code d'activation d'une des manières suivantes :

- Si vous avez acheté Kaspersky PURE en magasin, le code d'activation figure dans la documentation présente dans la boîte contenant le cédérom d'installation.

- Si vous avez acheté Kaspersky PURE en ligne, le code d'activation est envoyé à l'adresse de messagerie que vous avez renseignée lors de la commande.

Le décompte de la durée de validité de la licence débute à partir du jour où l'application a été activée. Si vous avez acheté une licence autorisant l'utilisation de Kaspersky PURE sur plusieurs appareils, le décompte de la durée de validité débute à partir du jour de la première utilisation du code d'activation.

En cas de perte ou de suppression accidentelle du code après l'activation de l'application, vous devez envoyer une demande au Support Technique de Kaspersky Lab pour le récupérer.

# RESOLUTION DES PROBLEMES TYPES

Cette section explique, étape par étape, comment exécuter les principales tâches que l'utilisateur peut accomplir à l'aide de l'application.

## DANS CETTE SECTION

# ACTIVATION DE L'APPLICATION

Pour pouvoir profiter des fonctions de l'application et des services complémentaires associés à celle-ci, il faut activer l'application.

Si vous n'avez pas activé l'application pendant l'installation, vous pouvez le faire plus tard. Les notifications de Kaspersky PURE dans la zone de notifications de la barre des tâches vous rappelleront qu'il faut activer l'application. L'activation de Kaspersky PURE s'effectue à l'aide de l'Assistant d'installation.

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

- Cliquez sur le lien **Activer** dans la fenêtre de notification de Kaspersky PURE 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 **Licence** qui s'ouvre, cliquez sur le bouton **Activer l'application**.

Lorsque l'Assistant d'activation de l'application fonctionne, certains paramètres doivent être indiqués.

## Etape 1. Saisie du code d'activation

Saisissez le code d'activation (cf. section "A propos du code d'activation" à la page 27) dans le champ correspondant, puis cliquez sur le bouton **Suivant**.

## Etape 2. Demande d'activation

Si la demande d'activation réussit, l'Assistant passe automatiquement à l'étape suivante.

## Etape 3. Saisie des données d'enregistrement

Les utilisateurs enregistrés bénéficient des possibilités suivantes :

- envoyer les demandes au Support Technique et au Laboratoire d'étude des virus via Mon Espace Personnel sur le site Internet de Kaspersky Lab ;
- gérer les codes d'activation ;
- recevoir les informations sur des nouveaux produits et sur les offres spéciales de Kaspersky Lab.

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

## Etape 4. Activation

Si l'activation de l'application a réussi, l'Assistant passe automatiquement à la fenêtre suivante.

## Etape 5. Fin de l'Assistant

La fenêtre de l'Assistant affiche les résultats de l'activation.

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

# ACHAT D'UNE LICENCE OU RENOUVELLEMENT

Si vous avez installé Kaspersky PURE sans licence commerciale, vous pourrez acheter celle-ci après l'installation de l'application. A l'achat d'une licence commerciale, vous recevez le code d'activation requis pour activer l'application (cf. section "Activation de l'application" à la page 29).

Quand la licence est sur le point d'expirer, vous pouvez la renouveler. Pour ce faire, vous pouvez désigner dans l'application un code d'activation de réserve avant l'expiration de la licence. A l'issue de la période de validité de la licence, Kaspersky PURE est activé automatiquement à l'aide du code d'activation de réserve.

*Pour acheter une licence, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Le lien **Licence**, situé dans la partie inférieure de la fenêtre principale, permet d'ouvrir la fenêtre **Licence**.
3. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Acheter le code d'activation**.

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

*Pour ajouter un code d'activation de réserve, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Le lien **Licence**, situé dans la partie inférieure de la fenêtre principale, permet d'ouvrir la fenêtre **Licence**.
3. Dans la fenêtre Licence qui s'ouvre, cliquez sur le bouton **Activer l'application**.

   La fenêtre de l'Assistant d'activation de l'application s'ouvre.
4. Saisissez le code d'activation dans les champs correspondants, puis cliquez sur **Suivant**.

   Kaspersky PURE envoie les données au serveur d'activation pour vérification. Si la vérification réussit, l'Assistant passe automatiquement à l'étape suivante.
5. A la fin de l'Assistant, cliquez sur **Terminer**.

# UTILISATION DES NOTIFICATIONS DE L'APPLICATION

Les notifications de l'application qui apparaissent dans la zone de notifications de la barre des tâches signalent les événements survenus pendant l'utilisation de l'application et qui nécessitent 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 pour assurer la protection de l'ordinateur (par exemple : découverte d'un objet malveillant ou d'une activité dangereuse dans le système). Les fenêtres des notifications et des messages contextuels critiques sont en rouge.
- *Importants* : signalent des événements potentiellement importants pour assurer la protection de l'ordinateur (par exemple : découverte d'un objet potentiellement infecté ou d'une activité suspecte dans le système). Les fenêtres des notifications et des messages contextuels importants sont en jaune.
- *Informations* : signalent des événements qui ne sont pas critiques pour assurer la protection de l'ordinateur. Les fenêtres des notifications et des messages contextuels à titre d'informations sont en vert.

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

# ANALYSE DE L'ETAT DE PROTECTION DE L'ORDINATEUR ET SUPPRESSION DES PROBLEMES DE SECURITE

La couleur de la fenêtre principale de Kaspersky PURE (cf. ill. ci-après) signale les problèmes 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 de résoudre immédiatement les problèmes de sécurité et de supprimer les menaces.


*Illustration 1. Couleur rouge de la fenêtre principale*

Quand un problème de sécurité existe sur l'ordinateur, le bouton **Corriger** apparaît dans la partie supérieure droite de la fenêtre principale de l'application (cf. ill. ci-dessus) sur l'indicateur d'état de la protection. En cliquant sur le bouton **Corriger** dans la fenêtre principale, vous pouvez ouvrir la fenêtre **Problèmes de sécurité** (cf. ill. ci-après) qui affiche des informations détaillées sur l'état de la protection de l'ordinateur et qui propose diverses solutions pour résoudre les problèmes de sécurité et supprimer les menaces.

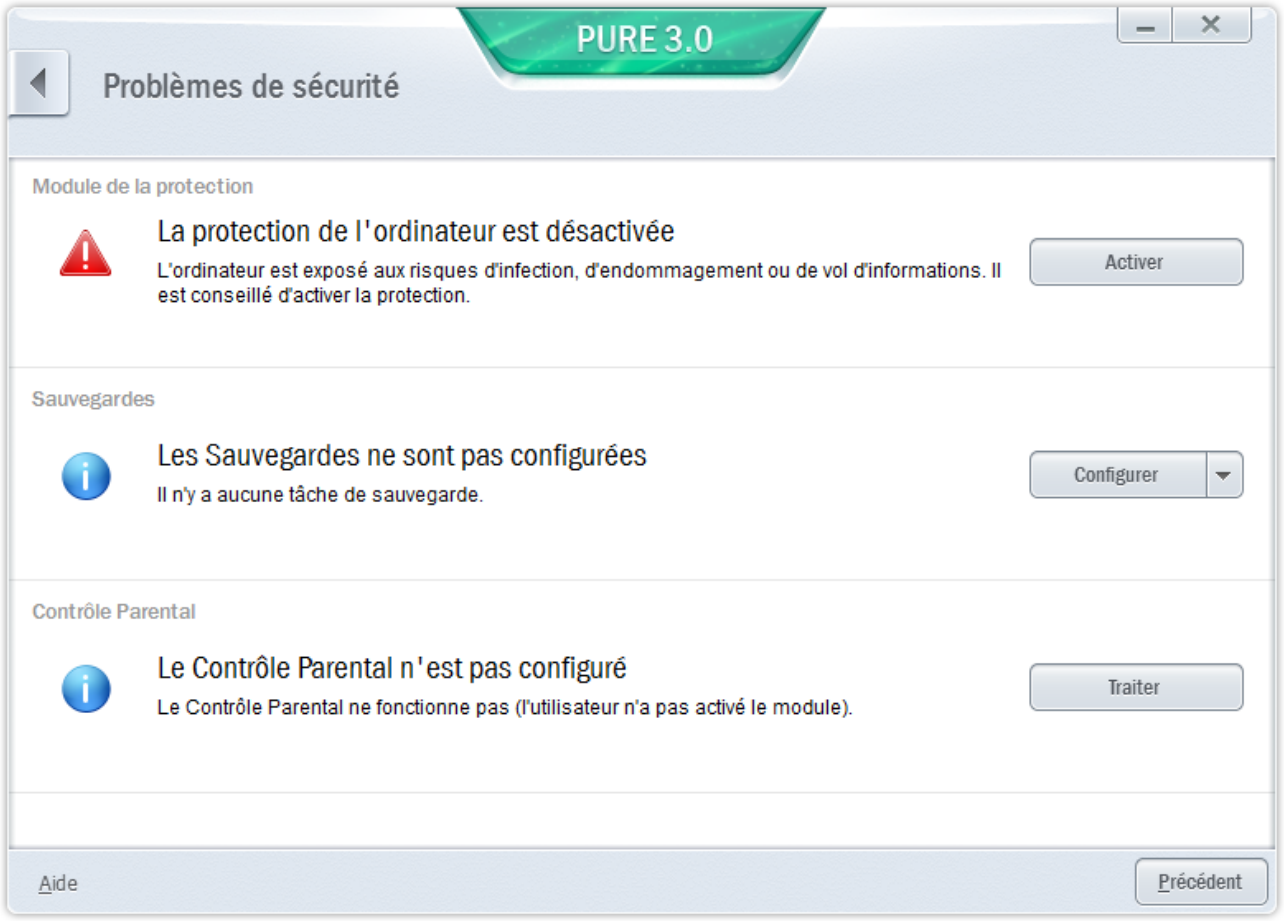


*Illustration 2. Fenêtre **Problèmes de sécurité***

Les problèmes de protection sont regroupés selon les catégories auxquelles ils appartiennent. Chaque problème possède des actions que vous pouvez exécuter pour le résoudre.

Vous pouvez vérifier l'état de la protection sur les autres ordinateurs du réseau domestique via Mon Réseau (cf. section "Administration à distance de la protection du réseau domestique" à la page 41).

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

Kaspersky PURE 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 PURE les télécharge et les installe en arrière-plan. Vous pouvez lancer la mise à jour de Kaspersky PURE à tout moment depuis la fenêtre principale de l'application ou depuis le menu contextuel de l'icône de l'application dans la zone des notifications de la barre des tâches.

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

- *Pour lancer la mise à jour depuis le menu contextuel de l'icône de l'application dans la zone de notifications de la barre des tâches,*

  choisissez l'option **Mise à jour** dans le menu contextuel de l'icône de l'application.

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

  1. Ouvrez la fenêtre principale de l'application.
  2. Dans le groupe **Protection de l'ordinateur**, cliquez sur le lien **Mise à jour** pour lancer la mise à jour des bases.

# ANALYSE RAPIDE DE L'ORDINATEUR

L'analyse rapide désigne l'analyse des objets suivants :

- objets chargés au démarrage du système d'exploitation ;
- mémoire système ;
- secteurs d'amorçage du disque.

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

  1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Ma Protection**.
  2. Dans la partie gauche de la fenêtre, sélectionnez la section **Analyse**.
  3. Dans le groupe **Analyse rapide** dans la partie droite de la fenêtre, cliquez sur le bouton  .

# ANALYSE COMPLETE DE L'ORDINATEUR

Pendant l'analyse complète, Kaspersky PURE analyse par défaut les objets suivants :

- mémoire système ;
- objets chargés au démarrage du système d'exploitation ;
- sauvegarde ;
- disques durs et amovibles.

Il est conseillé de réaliser une analyse complète directement après l'installation de Kaspersky PURE sur l'ordinateur.

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

  1. Ouvrez la fenêtre principale de l'application.
  2. Dans le groupe **Protection de l'ordinateur**, cliquez sur le lien **Analyse** afin d'ouvrir la liste des tâches d'analyse.
  3. Cliquez sur le lien **Analyse complète** afin de lancer l'analyse complète.

# ANALYSE D'UN FICHIER, D'UN DOSSIER, D'UN DISQUE OU D'UN AUTRE OBJET

Pour analyser un objet, utilisez une des méthodes suivantes :

- au départ du menu contextuel de l'objet ;
- au départ de la fenêtre principale de l'application.

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

1. Ouvrez la fenêtre de l'Explorateur Microsoft Windows et accédez au dossier contenant l'objet à analyser.
2. Cliquez-droit pour ouvrir le menu contextuel de l'objet (cf. ill. ci-après) et sélectionnez l'option **Rechercher d'éventuels virus**.

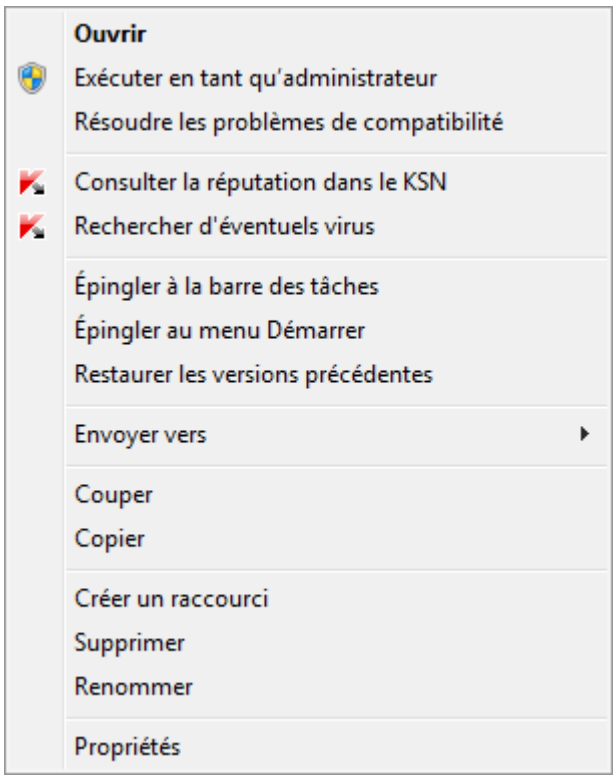


*Illustration 3. Menu contextuel du fichier exécutable*

*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 cliquez sur le bouton **Ma Protection**.
2. Dans la partie gauche de la fenêtre, sélectionnez la section **Analyse**.
3. Désignez l'objet à analyser à l'aide d'un des moyens suivants :
   - Cliquez sur le lien **désignez** situé dans la partie inférieure droite de la fenêtre pour ouvrir la fenêtre **Analyse personnalisée**, puis cochez les cases en regard des dossiers et des disques à analyser.

     Si l'objet à analyser ne figure pas dans la liste, procédez comme suit :

     a. Le lien **Ajouter** dans la partie inférieure gauche de la fenêtre ouvre la fenêtre **Sélection de l'objet à analyser**.

     b. Dans la fenêtre **Sélection de l'objet à analyser** qui s'ouvre, sélectionnez l'objet à analyser.

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


*Illustration 4. Zone de la section **Analyse** sur laquelle il faut déposer l'objet à analyser*

# RECHERCHE DE LA PRESENCE DE VULNERABILITES SUR L'ORDINATEUR

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

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

1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Ma Protection**.
2. Dans la partie gauche de la fenêtre, sélectionnez la section **Analyse**.
3. Dans le groupe **Recherche de vulnérabilités** de la fenêtre qui s'ouvre, cliquez sur le bouton  .

# RESTAURATION DU FICHIER SUPPRIME OU REPARE PAR L'APPLICATION

Kaspersky Lab déconseille la restauration des fichiers supprimés ou réparés car ils peuvent constituer une menace pour votre ordinateur.

La restauration d'un fichier supprimé ou réparé s'opère sur la base de sa copie de sauvegarde créée par l'application lors de l'analyse.

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

1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Ma Protection**.
2. Dans la partie gauche de la fenêtre qui s'ouvre, cliquez sur le lien **Quarantaine : <nombre de fichiers>** (cf. ill. ci-après).


*Illustration 5. Fenêtre **Protection de l'ordinateur***

3. Dans la fenêtre **Quarantaine** qui s'ouvre, sélectionnez le fichier requis dans la liste et cliquez sur le bouton **Restaurer** (cf. ill. ci-après).

Kaspersky PURE restaure le fichier indiqué dans le dossier dans lequel se trouvait le fichier supprimé ou réparé par l'application.

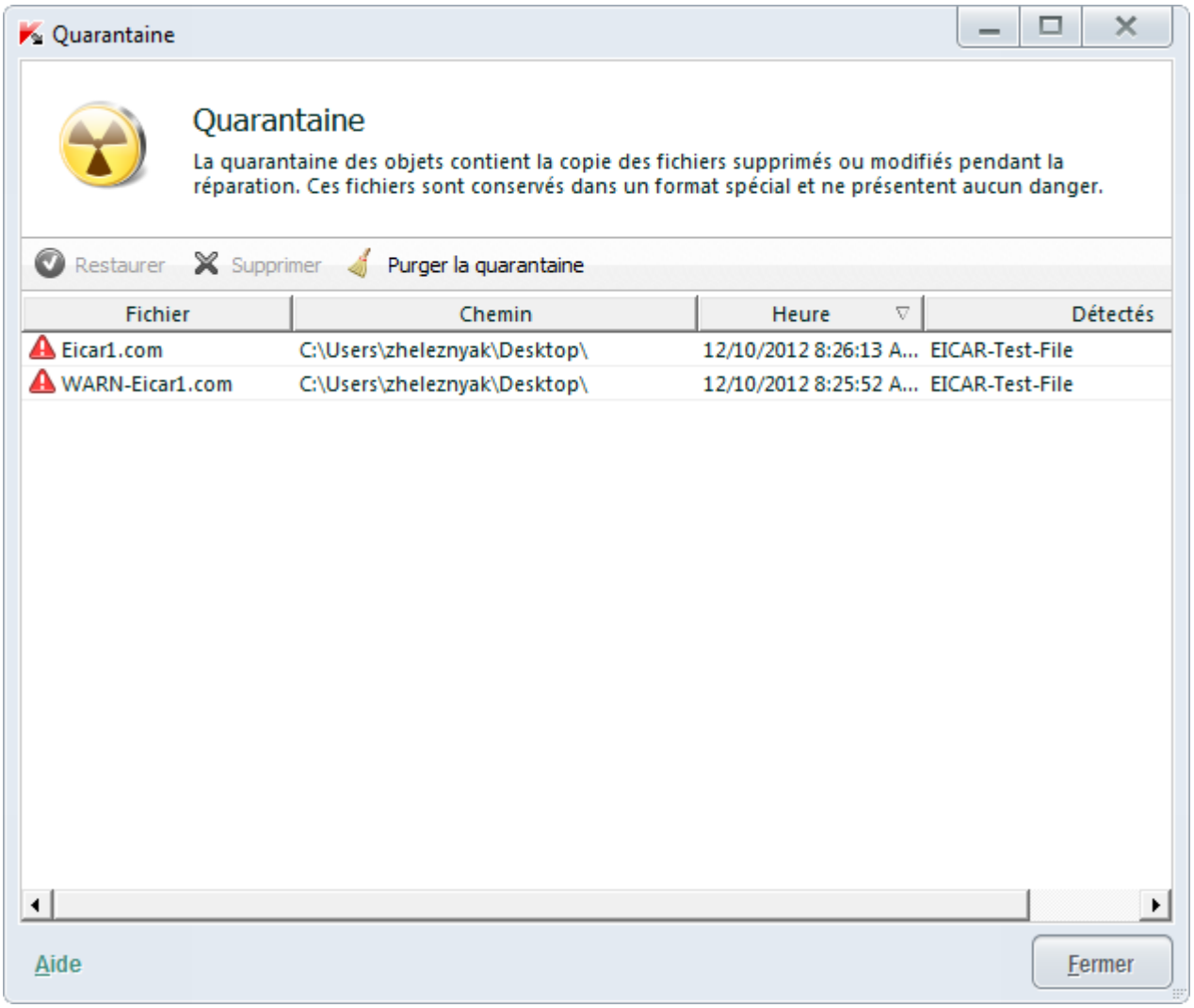


*Illustration 6. Fenêtre **Quarantaine***

# RESTAURATION DU SYSTEME D'EXPLOITATION APRES INFECTION

Si vous soupçonnez que le système d'exploitation de votre ordinateur a été endommagé ou modifié suite aux actions d programmes malveillants ou suite à un dysfonctionnement du système, utilisez l'A*ssistant de restauration après infection*, qui élimine les traces des 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 dommages 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 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 examen, l'Assistant analyse les informations recueillies afin d'identifier les dommages 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.

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

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre, sélectionnez la section **Outils complémentaires**.
3. Dans la fenêtre ouverte dans le groupe **Restauration du système**, cliquez sur le bouton **Exécuter**.

   La fenêtre de l'Assistant de restauration du système s'ouvre.

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**.

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** est 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 éliminer. 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 constituent 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 effectue 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, décochez la case en regard de celle-ci.

Il est vivement déconseillé de décocher les cases cochées 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.

# BLOCAGE DU COURRIER INDESIRABLE (SPAM)

Si vous recevez un volume important de courrier indésirable, activez le module Anti-Spam et définissez le niveau de protection recommandé.

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

1. Ouvrez la fenêtre principale de l'application.
2. Cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
3. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le module **Anti-Spam**.
4. Dans la partie droite de la fenêtre, cochez la case **Activer l'Anti-Spam**.
5. Assurez-vous que le niveau **Recommandé** est défini dans le groupe **Niveau de protection**.

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

# ANALYSE DU COURRIER ET FILTRAGE DES PIECES JOINTES DANS LES MESSAGES

Kaspersky PURE permet d'analyser les messages du courrier électronique et de rechercher la présence éventuelle d'objets dangereux à l'aide de l'Antivirus Courrier. L'Antivirus Courrier se lance au démarrage du système d'exploitation, se trouve en permanence dans la mémoire vive de l'ordinateur et analyse les messages envoyés et reçus via les protocoles POP3, SMTP, IMAP, MAPI et NNTP (y compris les messages envoyés via des connexions sécurisées (SSL) via les protocoles POP3, SMTP et IMAP).

L'Antivirus Courrier analyse par défaut aussi bien les messages entrants que les messages sortants. En cas de nécessité, vous pouvez activer l'analyse des messages entrants uniquement.

*Pour vérifier les messages entrants uniquement, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
3. Dans la partie gauche de la fenêtre, dans la section **Centre de protection**, sélectionnez le module **Antivirus Courrier**.
4. Dans la partie droite de la fenêtre, cliquez sur le bouton **Configuration**.

   La fenêtre **Antivirus Courrier** s'ouvre.
5. Dans la fenêtre qui s'ouvre, dans le groupe **Zone de protection** de l'onglet **Général**, sélectionnez l'option **Analyser uniquement le courrier entrant**.

Si aucune menace n'a été détectée dans le message ou les objets infectés ont été réparés avec succès, le message peut être utilisé. Si l'objet infecté ne peut pas être réparé, l'Antivirus Courrier donne un autre nom ou supprime l'objet du message et place dans l'objet du message une notification indiquant que le message a été traité par Kaspersky PURE. En cas de suppression de l'objet, Kaspersky PURE crée sa copie de sauvegarde et le place en quarantaine.

Les applications malveillantes peuvent se diffuser sous forme de pièces jointes dans les messages. Vous pouvez activer le filtrage des pièces jointes dans les messages. Le filtrage permet de renommer automatiquement ou de supprimer les types de pièces jointes que vous avez indiqués.

*Pour activer le filtrage des pièces jointes dans les messages, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
3. Dans la partie gauche de la fenêtre, dans la section **Centre de protection**, sélectionnez le module **Antivirus Courrier**.
4. Dans la partie droite de la fenêtre, cliquez sur le bouton **Configuration**.

   La fenêtre **Antivirus Courrier** s'ouvre.
5. Dans la fenêtre qui s'ouvre sous l'onglet **Filtre des pièces jointes**, sélectionnez le mode de filtrage des pièces jointes (**Renommer les types de pièces jointes indiqués** ou **Supprimer les types de pièces jointes indiqués**).
6. Dans la liste des types de fichiers (extensions), sélectionnez les types de pièces jointes à filtrer.

   Si vous voulez ajouter le masque du nouveau type de fichier, procédez comme suit :

   a. Cliquez sur le lien **Ajouter** situé dans la partie inférieure de la fenêtre afin d'ouvrir la fenêtre **Masque de nom de fichier**.

   b. Dans la fenêtre qui s'ouvre, indiquez le masque nécessaire du type de fichiers.
7. Dans la fenêtre **Configuration**, cliquez sur le bouton **Appliquer**.

# DEFINITION DE LA SECURITE D'UN SITE INTERNET

Kaspersky PURE permet d'analyser la sécurité d'un site Internet avant de cliquer sur le lien de ce site Internet. Pour ce faire, il utilise le *module d'analyse des liens*.

Le module d'analyse des liens n'est pas accessible dans le navigateur Microsoft Internet Explorer 10 de style Metro, ainsi que dans le navigateur Microsoft Internet Explorer 10 si la case **Activer le mode protégé** (Enhanced Protected Mode) est cochée dans les paramètres du navigateur.

Le module d'analyse des liens s'intègre dans les navigateurs Microsoft Internet Explorer, Google Chrome™ et Mozilla™ Firefox™ et analyse les liens sur la page Internet ouverte dans le navigateur. A côté de chaque lien, Kaspersky PURE affiche une des icônes suivantes :

-  – si la page Internet, qui s'ouvre à l'aide du lien, est saine selon les données de Kaspersky Lab ;
-  – s'il n'y pas d'informations sur la sécurité de la page Internet ouverte à l'aide du lien ;
-  – si la page Internet ouverte à l'aide du lien, est dangereuse selon les données de Kaspersky Lab.

Lorsque vous placez le curseur de la souris sur l'icône, la fenêtre contextuelle avec la description plus détaillée du lien s'affiche.

Par défaut, Kaspersky PURE analyse les liens uniquement dans les résultats de recherche. Vous pouvez activer l'analyse des liens sur n'importe quel site Internet.

*Pour activer l'analyse des liens sur un site Internet, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.

3. Dans la fenêtre **Configuration** qui s'ouvre, dans la section **Centre de protection**, sélectionnez la sous-section **Antivirus Internet**, puis cliquez sur le bouton **Configuration**.

   La fenêtre **Antivirus Internet** s'ouvre.

4. Dans la fenêtre qui s'ouvre sous l'onglet **Filtrage de liens** dans le groupe **Analyse des liens (URL Advisor)**, cliquez sur le bouton **Configuration**.

   La fenêtre **Configuration du module d'analyse des liens** s'ouvre.

5. Dans la fenêtre qui s'ouvre dans le groupe **Mode d'analyse**, sélectionnez l'option **N'importe quel lien**.

6. Dans la fenêtre **Configuration**, cliquez sur le bouton **Appliquer**.

# BLOCAGE DE L'ACCES AUX SITES INTERNET DE DIFFERENTES REGIONS

Selon les statistiques de Kaspersky Lab, le degré d'infection des sites Internet varie en fonction des différents pays. Kaspersky PURE permet d'interdire l'accès aux sites Internet appartenant à des domaines régionaux caractérisés par un haut niveau d'infection, à l'aide du module Géolocalisation.

Lorsque Filtrage par géolocalisation est activé, Kaspersky PURE, selon votre choix, autorise ou interdit l'accès à un domaine régional, ou demande l'autorisation d'accès.

*Pour activer et configurer le Filtrage par géolocalisation, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.

2. Cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.

3. Dans la fenêtre **Configuration** qui s'ouvre, dans la section **Centre de protection**, sélectionnez la sous-section **Antivirus Internet**, puis cliquez sur le bouton **Configuration**.

   La fenêtre **Antivirus Internet** s'ouvre.

4. Dans la fenêtre qui s'ouvre sous l'onglet **Filtre par géolocalisation**, cochez la case **Filtrer la navigation Internet vers les sites étrangers**.

5. Dans la partie inférieure de la fenêtre dans la liste des domaines contrôlés, indiquez les domaines dont il faut autoriser ou interdire l'accès, ou demander l'autorisation d'accès.

6. Dans la fenêtre **Configuration**, cliquez sur le bouton **Appliquer**.

# ADMINISTRATION A DISTANCE DE LA PROTECTION DU RESEAU DOMESTIQUE

Le module Mon Réseau est prévu pour l'administration à distance de Kaspersky PURE sur les ordinateurs du réseau domestique depuis le poste de travail de l'administrateur.

Mon Réseau permet de résoudre les tâches suivantes liées à la sécurité du réseau domestique :

- consulter la liste des problèmes de sécurité sur un ordinateur en particulier et résoudre certains d'entre eux à distance ;

- rechercher la présence éventuelle de virus simultanément sur plusieurs ordinateurs du réseau domestique ;

- mettre à jour simultanément les bases sur plusieurs ordinateurs du réseau domestique.

- *Pour consulter la liste des problèmes de sécurité détectés sur un ordinateur distinct du réseau, procédez comme suit :*

  1. Ouvrez la fenêtre principale de l'application, puis cliquez sur le bouton **Mon Réseau**.
  2. Dans la partie supérieure de la fenêtre **Mon Réseau** qui s'ouvre, sélectionnez l'ordinateur dont vous souhaitez afficher les problèmes, puis accédez à la section **Informations**.
  3. Dans la section **Problèmes** de la partie droite de la fenêtre, cliquez sur le bouton **Liste**.

     La fenêtre **Problèmes de sécurité** s'ouvre et affiche les informations relatives aux problèmes de sécurité sur l'ordinateur sélectionné.

- *Pour rechercher la présence éventuelle de virus sur plusieurs ordinateurs du réseau, procédez comme suit :*

  1. Ouvrez la fenêtre principale de l'application, puis cliquez sur le bouton **Mon Réseau**.

     La fenêtre **Mon Réseau** s'ouvre.
  2. Le lien **Rechercher d'éventuels virus** ouvre la fenêtre **Lancement groupé de l'analyse**.
  3. Dans la fenêtre **Lancement groupé de l'analyse**, sélectionnez l'onglet correspondant au type d'analyse souhaité (**Analyse complète** ou **Analyse rapide**).
  4. Sélectionnez les ordinateurs que vous souhaitez analyser, puis cliquez sur le bouton **Lancer l'analyse**.

- *Pour mettre à jour les bases simultanément sur plusieurs ordinateurs, procédez comme suit :*

  1. Ouvrez la fenêtre principale de l'application, puis cliquez sur le bouton **Mon Réseau**.

     La fenêtre **Mon Réseau** s'ouvre.
  2. Le lien **Mettre à jour les bases** ouvre la fenêtre **Lancement groupé de la mise à jour**.
  3. Dans la fenêtre **Lancement groupé de la mise à jour**, sélectionnez les ordinateurs sur lesquels vous souhaitez actualiser les bases, puis cliquez sur le bouton **Lancer la mise à jour**.

# TRAITEMENT DES PROGRAMMES INCONNUS

Grâce à Kaspersky PURE, vous pouvez réduire les risques liés à l'utilisation d'applications inconnues (par exemple, risques d'infection par des virus ou modification non sollicitée des paramètres du système d'exploitation).

Kaspersky PURE propose des outils et des modules qui permettent de vérifier la réputation d'une application et de l'exécuter dans un environnement protégé, isolé du système d'exploitation.

## CONTROLE DES ACTIONS DE L'APPLICATION SUR L'ORDINATEUR ET DANS LE RESEAU

Le Contrôle des Applications prévient l'exécution des actions dangereuses pour le système, et il assure aussi le contrôle de l'accès aux ressources du système d'exploitation et de vos données personnelles.

Le module surveille les actions exécutées dans le système par les applications installées sur les ordinateurs, et il les règle à partir des règles du Contrôle des Applications. Ces règles réglementent les activités qui ont un impact sur la sécurité de l'ordinateur, notamment l'accès des applications aux ressources protégées (fichiers et dossiers, clés du registre, adresses réseau, etc.).

L'activité réseau est contrôlée par le module Pare-feu.

Au premier lancement de l'application sur l'ordinateur, le module Contrôle des Applications analyse sa sécurité et place dans un des groupes (De confiance, Douteuses, Restrictions élevées ou Restrictions faibles). Le groupe définit les règles que Kaspersky PURE appliquera pour contrôler l'activité de cette application.

Vous pouvez modifier manuellement les règles de contrôle des actions de l'application.

*Pour modifier manuellement la règle de contrôle de l'application, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
3. Dans la fenêtre **Configuration** qui s'ouvre, dans la section **Centre de protection**, sélectionnez la sous-section **Contrôle des Applications**.
4. Dans la partie droite de la fenêtre, dans le groupe **Configuration des règles pour les applications, protection des données et d'autres ressources**, cliquez sur le bouton **Applications**.
5. Dans la fenêtre **Applications** qui s'ouvre, sélectionnez dans la liste l'application nécessaire et cliquez sur le bouton **Modifier**.
6. Dans la fenêtre **Règles pour l'application** qui s'ouvre, définissez les règles de contrôle de l'application :
   - Pour configurer les règles d'accès de l'application aux ressources du système d'exploitation, procédez comme suit :
     a. Sous l'onglet **Fichiers et base de registres**, sélectionnez la catégorie de ressources nécessaire.
     b. En cliquant droit dans la colonne comprenant l'action pouvant être exécutée sur la ressource (**Lecture**, **Ecriture**, **Suppression** ou **Création**), ouvrez le menu contextuel et sélectionnez la valeur nécessaire (**Autoriser**, **Interdire** ou **Confirmer l'action**).
   - Pour configurer les privilèges de l'application relatifs à l'exécution de différentes actions dans le système d'exploitation, procédez comme suit :
     a. Sous l'onglet **Privilèges**, sélectionnez la catégorie de privilèges nécessaire.
     b. En cliquant droit dans la colonne **Autorisation**, ouvrez le menu contextuel et sélectionnez la valeur nécessaire (**Autoriser**, **Interdire** ou **Confirmer l'action**).
   - Pour configurer les privilèges de l'application relatifs à l'exécution de différentes actions dans le réseau, procédez comme suit :
     a. Sous l'onglet **Règles réseau**, cliquez sur le bouton **Ajouter**.

        La fenêtre **Règle réseau** s'ouvre.
     b. Dans la fenêtre qui s'ouvre, définissez les paramètres nécessaires, puis cliquez sur le bouton **OK**.
     c. Pour définir la priorité de la nouvelle règle, déplacez-la vers le haut ou vers le bas de la liste à l'aide des boutons **Haut** et **Bas**.
   - Pour désactiver certaines actions d'analyse du Contrôle des Applications, sous l'onglet **Exclusions**, cochez les cases pour les actions à ne pas contrôler.

   Toutes les exclusions créées dans les règles des applications sont accessibles dans la fenêtre de configuration de l'application, dans le groupe **Menaces et exclusions**.
7. Dans la fenêtre **Configuration**, cliquez sur le bouton **Appliquer**.

# VERIFICATION DE LA REPUTATION DES APPLICATIONS

Kaspersky PURE permet de vérifier la réputation des applications auprès des utilisateurs dans le monde entier. La réputation de l'application reprend les indices suivants :

- nom de l'éditeur ;
- informations sur la signature numérique (disponible en présence de la signature numérique) ;
- informations sur le groupe dans lequel l'application a été placée par le Contrôle des Applications ou par la majorité des utilisateurs de Kaspersky Security Network ;
- nombre d'utilisateurs de Kaspersky Security Network qui utilisent l'application (disponible si l'application est classée dans le groupe De confiance dans la base Kaspersky Security Network) ;
- heure à laquelle l'application est devenue connue de Kaspersky Security Network ;
- pays dans lesquels l'application est la plus répandue.

La fonction de vérification de la réputation des applications est disponible uniquement si vous avez accepté de participer au Kaspersky Security Network.

*Pour connaître la réputation d'une application,*

ouvrez le menu contextuel du fichier exécutable de l'application et sélectionnez l'option **Consulter la réputation dans le KSN** (cf. ill. ci-après).

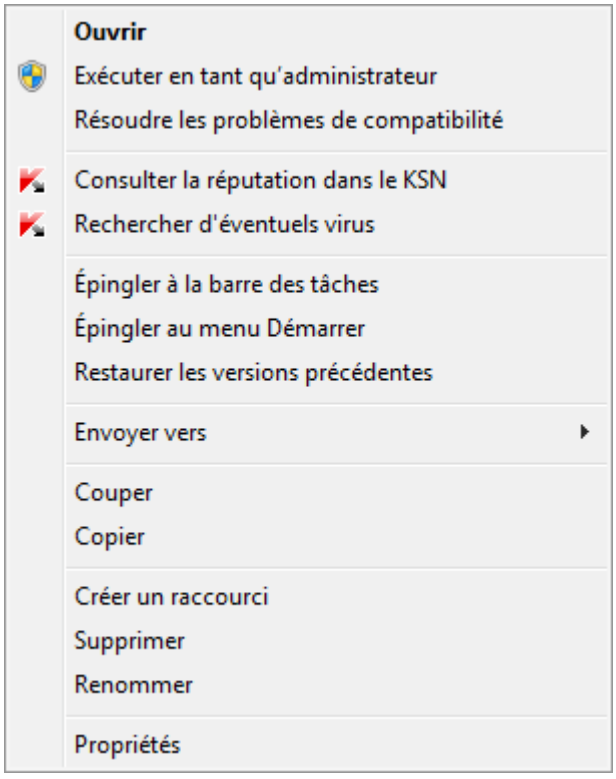


*Illustration 7. Menu contextuel du fichier exécutable dans Microsoft Windows*

Une fenêtre reprenant les données sur la réputation de l'application dans le KSN s'ouvre.

# PROTECTION DES DONNEES PERSONNELLES CONTRE VOL

Kaspersky PURE protèges vos 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 ;
- fichiers confidentiels.

Kaspersky PURE reprend des modules 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.

La Protection des transactions bancaires possède des fonctions pour protéger les données lors de l'utilisation des services d'une banque en ligne et lors des paiements en ligne.

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

Le clavier virtuel, la Protection des données saisies au clavier et le Gestionnaire de mots de passe ont été développés pour prévenir l'interception des données saisies au clavier.

Mon Coffre-fort sert à protéger les fichiers contre l'accès non autorisé.

L'Assistant d'élimination des traces d'activité permet de supprimer les informations sur les actions de l'utilisateur sur un ordinateur.

## DANS CETTE SECTION



# PROTECTION DES TRANSACTIONS BANCAIRES

Pour protéger les données confidentielles que vous saisissez sur les sites Internet des banques et des systèmes de paiement (par exemple, les numéros des cartes bancaires, les mots de passe d'accès aux services des transactions bancaires en ligne), ainsi que pour prévenir le vol des moyens de paiements lors des paiements en ligne, Kaspersky PURE propose d'ouvrir ces sites Internet en mode navigateur protégé.

Le lancement de la navigation sécurisée est impossible si la case **Activer l'autodéfense** est décochée dans la section **Paramètres avancés**, sous-section **Autodéfense** de la fenêtre de configuration de l'application.

Vous pouvez configurer la Protection des transactions bancaires pour définir automatiquement les sites Internet des banques et des systèmes de paiement.

La Protection des transactions bancaires n'est pas accessible dans le navigateur Microsoft Internet Explorer 10 de style Metro, ainsi que dans le navigateur Microsoft Internet Explorer 10 si la case **Activer le mode protégé** (Enhanced Protected Mode) est cochée dans les paramètres du navigateur. Vous pouvez lancer le mode du navigateur protégé depuis l'interface Kaspersky PURE.

*Pour configurer la Protection des transactions bancaires, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
3. Dans la fenêtre **Configuration** qui s'ouvre, dans la section **Centre de protection**, sélectionnez la sous-section **Protection des transactions bancaires**.
4. Cochez la case **Activer la Protection des transactions bancaires**.
5. Pour activer la notification sur les vulnérabilités détectées dans le système d'exploitation avant le lancement du navigateur protégé, cochez la case **Signaler les vulnérabilités dans le système d'exploitation**.
6. Pour configurer la Protection des transactions bancaires pour le site Internet défini, procédez comme suit :
   a. Dans la liste **Sites Internet des banques et des systèmes de paiement**, cliquez sur le bouton **Ajouter**.

      La fenêtre **Site Internet pour la Protection des transactions bancaires** s'ouvre.

   b. Dans la fenêtre qui s'ouvre, dans le champ **Site Internet d'une banque ou d'un système de paiement**, saisissez l'adresse du site Internet à ouvrir en mode navigateur protégé.

      Devant l'adresse du site Internet, le protocole https:// utilisé par le navigateur protégé par défaut, doit être indiqué.

   c. En cas de nécessité, saisissez le nom ou la description de ce site Internet dans le champ **Description**.
   d. Sélectionnez le mode de lancement du navigateur protégé lors de l'ouverture de ce site Internet :
      - Si vous voulez que Kaspersky PURE propose de lancer le navigateur protégé chaque fois à l'ouverture de ce site Internet, sélectionnez l'option **Confirmer l'action**.
      - Si vous voulez que Kaspersky PURE ouvre automatiquement ce site Internet en mode navigateur protégé, sélectionnez l'option **Lancer automatiquement le navigateur protégé**.
      - Si vous voulez activer la Protection des transactions bancaires pour ce site Internet, sélectionnez l'option **Ne pas lancer le navigateur protégé**.
7. Dans la fenêtre **Configuration**, cliquez sur le bouton **Appliquer**.

# PROTECTION CONTRE LE PHISHING

L'Anti-Phishing, inclus dans l'Antivirus Internet, l'Antivirus Courrier et l'Antivirus IM ("Chat"), garantit la protection contre le phishing. Activez ces modules pour garantir la protection la plus efficace contre le phishing.

Vous pouvez configurer des paramètres complémentaires de protection contre le phishing dans les modules Antivirus Internet et Antivirus IM.

*Pour configurer la protection contre le phishing lors du fonctionnement de l'Antivirus Internet, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.

3. Dans la fenêtre **Configuration** qui s'ouvre, dans la section **Protection**, sélectionnez la sous-section **Antivirus Internet**, puis cliquez sur le bouton **Configuration**.

   La fenêtre **Antivirus Internet** s'ouvre.

4. Dans la fenêtre qui s'ouvre sous l'onglet **Général**, dans le groupe **Analyse des liens**, cochez la case **Vérifier si les pages appartiennent à un site de phishing**.

5. Si vous souhaitez que l'Anti-Phishing utilise l'analyse heuristique lors de l'analyse des pages Internet, cliquez sur le bouton **Avancé**.

   La fenêtre **Configuration de l'Anti-Phishing** s'ouvre.

6. Dans la fenêtre qui s'ouvre, cochez la case **Utiliser l'analyse heuristique lors de la recherche d'éventuels liens de phishing dans les pages Internet** et définissez le niveau de détail de l'analyse.

7. Dans la fenêtre **Configuration**, cliquez sur le bouton **Appliquer**.

*Pour configurer la protection contre le phishing lors du fonctionnement de l'Antivirus IM ("Chat"), procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.

2. Cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.

3. Dans la fenêtre **Configuration** qui s'ouvre, dans la section **Protection**, sélectionnez la sous-section **Antivirus IM ("Chat")**.

4. Cochez la case **Analyser les liens selon la base des adresses Internet de phishing** dans le groupe **Méthodes d'analyse** de la partie droite de la fenêtre.

5. Dans la fenêtre **Configuration**, cliquez sur le bouton **Appliquer**.

# UTILISATION DU CLAVIER VIRTUEL

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

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

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

Le clavier virtuel protège contre l'interception des données personnelles uniquement avec les navigateurs Microsoft Internet Explorer, Mozilla Firefox et Google Chrome. Si vous utilisez un autre navigateur Internet, le clavier virtuel ne protège pas les données personnelles saisies contre l'interception.

Le clavier virtuel n'est pas accessible dans le navigateur Microsoft Internet Explorer 10 de style Metro, ainsi que dans le navigateur Microsoft Internet Explorer 10 si la case **Activer le mode protégé** (Enhanced Protected Mode) est cochée dans les paramètres du navigateur. Dans ce cas, il est conseillé d'ouvrir le clavier virtuel depuis l'interface Kaspersky PURE.

Le clavier virtuel ne peut protéger vos données si le site Internet 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 analyser et 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 ne prévient pas la capture des images de l'écran à l'aide de la touche **Print Screen** et d'autres combinaisons de touches définies dans les paramètres du système d'exploitation, ainsi que la capture des images de l'écran à l'aide de la technologie DirectX.

Le clavier virtuel possède les particularités suivantes :

- Il faut appuyer sur les touches du clavier à l'aide de la souris.
- A la différence du clavier ordinaire, le clavier virtuel ne vous permet pas d'appuyer sur plusieurs 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. Le fait d'appuyer une nouvelle fois sur une touche annule l'activation de la touche.
- La langue de saisie du clavier virtuel est modifiée à l'aide de la même combinaison de touches que celle définie dans les paramètres du système d'exploitation pour le clavier normal. La deuxième touche doit être activée d'un clic droit de la souris (par exemple, si les paramètres du système d'exploitation indiquent que le changement de la langue du clavier s'opère à l'aide de la combinaison **ALT GAUCHE**+**MAJ**, il faudra cliquer sur la touche **ALT GAUCHE** avec le bouton gauche de la souris, puis cliquer avec le bouton droit sur la touche **SHIFT**).

Pour protéger les données saisies à l'aide du clavier virtuel, l'ordinateur doit être redémarré après l'installation de Kaspersky PURE.

Pour ouvrir le clavier virtuel, les options suivantes sont possibles :

- via le menu contextuel de l'icône de l'application dans la zone de notifications ;
- à partir de la fenêtre principale de l'application ;
- à partir du navigateur Microsoft Internet Explorer, Mozilla Firefox ou Google Chrome ;
- à l'aide de l'icône d'accès rapide du clavier virtuel dans le champ de saisie sur les sites Internet ;

  L'affichage de l'icône d'accès rapide dans les champs de saisie sur les sites Internet peut être configuré.

- à l'aide d'une combinaison de touches du clavier normal.

*Pour ouvrir le clavier virtuel depuis le menu contextuel de l'icône de l'application dans la zone de notification,*

sélectionnez l'option **Outils** → **Clavier virtuel** dans le menu contextuel de l'icône de l'application (cf. ill. ci-après).

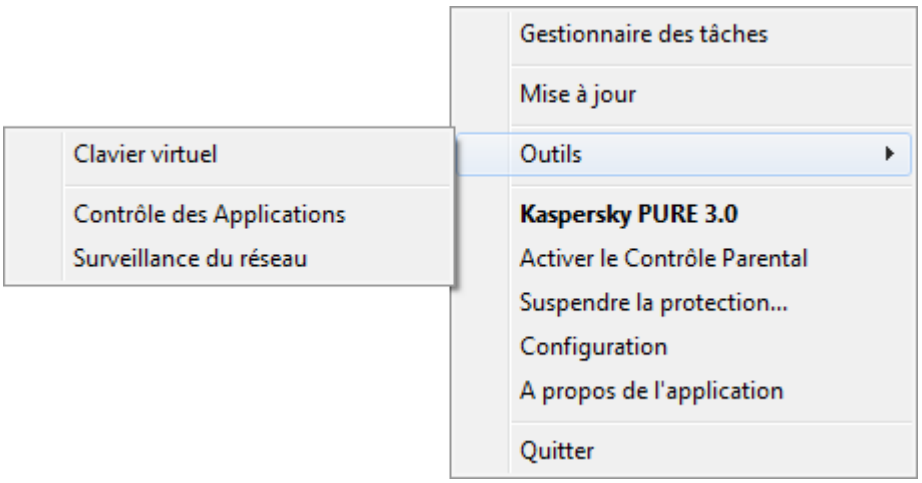


*Illustration 8. Menu contextuel de l'icône Kaspersky PURE*

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

  1. Sélectionnez la section **Gestionnaire de mots de passe** dans la partie inférieure de la fenêtre principale de l'application.
  2. Dans la partie inférieure de la fenêtre qui s'ouvre, cliquez sur **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, Mozilla Firefox ou Google Chrome.

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

  appuyez sur la combinaison des touches **CTRL**+**ALT**+**MAJ**+**P**.

- *Pour configurer l'affichage de l'icône d'accès rapide du clavier virtuel dans les champs de saisie sur les sites Internet, procédez comme suit :*

  1. Ouvrez la fenêtre principale de l'application.
  2. Cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
  3. Dans la fenêtre ouverte **Configuration** dans la section **Centre de protection**, sélectionnez la sous-section **Saisie sécurisée de données**.
  4. Dans la partie droite de la fenêtre dans le groupe **Clavier virtuel**, cochez la case **Afficher l'icône d'accès rapide dans les champs de saisie** et cliquez sur le bouton **Configuration**.

     La fenêtre **Clavier virtuel** s'ouvrira.
  5. Dans la fenêtre qui s'ouvre, définissez les règles d'affichage de l'icône d'accès rapide :

     - Sous l'onglet **Catégories**, cochez les cases pour les catégories des sites Internet sur lesquels il faut afficher l'icône d'accès rapide dans les champs de saisie.
     - Si vous voulez que l'icône d'accès rapide s'affiche dans les champs de saisie pour les sites Internet qui s'ouvrent dans le navigateur protégé lors du fonctionnement de la Protection des transactions bancaires, cochez la case **Afficher l'icône d'accès rapide dans les champs de saisie de la Protection des transactions bancaires** sous l'onglet **Catégories**.
     - Si vous voulez activer l'affichage de l'icône d'accès rapide dans les champs de saisie sur un site Internet défini, procédez comme suit :

       a. Sous l'onglet **Exclusions** dans la liste **Afficher l'icône d'accès rapide sur les sites Internet**, cliquez sur le bouton **Ajouter**.

          La fenêtre **Afficher l'icône d'accès rapide** s'ouvre.

       b. Dans la fenêtre qui s'ouvre, saisissez l'adresse du site Internet dans le champ **Adresse Internet** et sélectionnez une des options d'affichage de l'icône d'accès rapide sur ce site Internet (**Afficher l'icône uniquement sur la page Internet indiquée** ou **Afficher l'icône sur tout le site Internet**).
  6. Dans la fenêtre **Configuration**, cliquez sur le bouton **Appliquer**.

# PROTECTION DES DONNEES SAISIES AU CLAVIER

Au cours de l'utilisation d'Internet, 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 Internet, lors de l'achat sur une boutique en ligne ou en cas d'utilisation des services d'une banque en ligne.

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

La protection des données saisies au clavier permet d'éviter l'interception de ces données.

La protection des données saisies au clavier fonctionne uniquement dans les navigateurs Microsoft Internet Explorer, Mozilla Firefox et Google Chrome. En cas d'utilisation d'autres navigateurs Internet, les données saisies au clavier ne sont pas protégées contre l'interception.

La protection des données saisies n'est pas accessible dans le navigateur Microsoft Internet Explorer 10 de style Metro, ainsi que dans le navigateur Microsoft Internet Explorer 10 si la case **Activer le mode protégé** (Enhanced Protected Mode) est cochée dans les paramètres du navigateur.

La protection des données saisies au clavier ne peut protéger vos données si le site Internet nécessitant la saisie de ces données a été compromis car dans ce cas, les données tombent directement entre les mains des individus malintentionnés.

Vous pouvez configurer la protection des données saisies au clavier sur des différents sites Internet. Dès que la protection des données saisies au clavier est configurée, il n'est pas nécessaire d'exécuter les actions complémentaires lors de la saisie des données.

Pour protéger la saisie des données au clavier, l'ordinateur doit être redémarré une fois Kaspersky PURE installé.

*Pour configurer la protection des données saisies au clavier, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
3. Dans la fenêtre ouverte **Configuration** dans la section **Centre de protection**, sélectionnez la sous-section **Saisie sécurisée de données**.
4. La partie droite de la fenêtre dans le groupe **Protection des données saisies au clavier**, cochez la case **Protéger les données saisies au clavier** et cliquez sur le bouton **Configuration**.

   La fenêtre **Protection de la saisie au clavier** s'ouvre.
5. Dans la fenêtre qui s'ouvre, définissez la zone de protection des données saisies au clavier :
   - Sous l'onglet **Catégories**, cochez les cases pour les catégories des sites Internet sur lesquels il faut protéger les données saisies au clavier.
   - Si vous voulez que les données saisies au clavier soient protégées sur les sites Internet qui s'ouvrent dans le navigateur protégé en mode de Protection des transactions bancaires, cochez la case **Protéger les données saisies au clavier pour la Protection des transactions bancaires** sous l'onglet **Catégories**.
   - Si vous voulez que les données saisies au clavier soient protégées dans les champs pour la saisie des mots de passe sur tous les sites Internet, cochez la case **Protéger les champs pour la saisie des mots de passe sur tous les sites Internet** sous l'onglet **Catégories**.
   - Si vous voulez activer la protection des données saisies au clavier sur le site Internet définie, procédez comme suit :
     a. Sous l'onglet **Exclusions** dans la liste **Protéger la saisie des données au clavier sur les sites Internet**, cliquez sur le bouton **Ajouter**.

        La fenêtre **Site Internet protégé** s'ouvre.

     b. Dans la fenêtre qui s'ouvre, saisissez l'adresse du site Internet dans le champ **Adresse Internet** et sélectionnez une des options de protection de la saisie des données sur ce site Internet (**Activer la protection uniquement sur la page Internet indiquée** ou **Activer la protection sur tout le site Internet**).
6. Dans la fenêtre **Configuration**, cliquez sur le bouton **Appliquer**.

# PROTECTION DES MOTS DE PASSE

Kaspersky PURE enregistre et protège vos données personnelles (par exemple, mots de passe, noms d'utilisateur, contacts, informations financières). Kaspersky PURE associe les mots de passe et les comptes utilisateur aux applications et aux sites Internet qui requièrent une autorisation. Les données personnelles sont stockées sous forme cryptée dans un stockage accessible uniquement après saisie d'un mot de passe principal. Si le stockage est déverrouillé, vous pouvez accéder aisément aux mots de passe et aux données. Kaspersky PURE permet de saisir rapidement et facilement le mot de passe, le nom d'utilisateur ainsi que d'autres données personnelles dans le cadre de l'autorisation sur des sites Internet ou dans des applications. Il permet également les autorisations automatiques.

Vous pouvez accéder à vos données personnelles depuis n'importe lequel de vos périphériques sur lesquels l'application est installée et en présence d'une connexion Internet. Si le périphérique n'est pas connecté à Internet, vous pouvez enregistrer vos mots de passe et vos données sur un périphérique. Dès que le périphérique obtient l'accès à Internet, Kaspersky PURE propose de synchroniser les mots de passe et les données avec le stockage sur des serveurs distants.

De plus, vous pouvez utiliser les fonctionnalités suivantes de Kaspersky PURE :

- créer des mots de passe robustes pour les comptes utilisateur à l'aide du Générateur de mots de passe ;
- synchroniser les mots de passe et les données personnelles à jour sur tous vos périphériques dotés de Kaspersky PURE.

## DANS CETTE SECTION



# AJOUT DE COMPTES POUR UNE AUTORISATION AUTOMATIQUE

L'application permet de réaliser l'autorisation automatique (saisie du nom d'utilisateur et du mot de passe) sur des sites Internet ou dans des applications. L'application utilise les comptes pour réaliser l'autorisation automatique.

Vous pouvez créer deux type de comptes utilisateurs :

- des comptes utilisateur Internet utilisés pour les autorisations sur les sites Internet ;
- des comptes utilisateur d'applications pour les autorisations dans les applications, par exemple dans un client de messagerie.

*Pour ajouter un nouveau compte Internet depuis la fenêtre principale de Kaspersky PURE, procédez comme suit :*

1. Ouvrez la fenêtre principale du programme et cliquez sur le bouton **Gestionnaire de mots de passe**.

   La fenêtre Gestionnaire de mots de passe s'ouvre.

2. Appuyez sur le bouton **Mots de passe et données**.

   Le contenu du stockage des mots de passe et des donnés va s'afficher.

3. Ouvrez la section **Internet** dans la fenêtre du Gestionnaire de mots de passe.

   Les champs des données du compte utilisateur vont apparaitre dans la partie droite de la fenêtre.

4. Dans la partie **haute** de la fenêtre du champ Dénomination du compte utilisateur vous pouvez insérer la dénomination du compte utilisateur. Cliquez sur  .

   Le nom du compte utilisateur va être sauvegardé.

5. Dans le champ **Lien** indiquez l'adresse du site Inernet où le compte utilisateur sera utilisé lors de l'autorisation.

6. Saisissez le nom d'utilisateur auquel vous souhaitez autoriser l'accès au site dans le champ **Nom d'utilisateur**.

7. Saisissez le mot de passe du compte dans le champ **Mot de passe**. Pour créer le mot de passe automatiquement, cliquez sur le lien **Générateur de mots de passe**.

8. Dans la partie inférieure de la fenêtre, cliquez sur le bouton **Ajouter**.

   Le compte utilisateur créé va être affiché dans la section **Internet**.

*Pour ajouter un compte utilisateur d'application, procédez comme suit :*

1. Ouvrez la fenêtre principale du programme et cliquez sur le bouton **Gestionnaire de mots de passe**.

   La fenêtre Gestionnaire de mots de passe s'ouvre.

2. Appuyez sur le bouton **Mots de passe et données**.

   Le contenu du stockage des mots de passe et des donnés va s'afficher.

3. Ouvrez la section **Applications**. Appuyez sur le bouton **Ajouter le compte utilisateur de l'application**.

4. Dans la partie haute de la fenêtre du champ **Dénomination du compte utilisateur** vous pouvez insérer la dénomination du compte utilisateur. Cliquez sur  .

   Le nom du compte utilisateur va être sauvegardé.

5. Dans le champ **Application** indiquez l'accès vers le fichier d'exécution de l'application où le compte utilisateur sera utilisé lors de l'autorisation.

6. Saisissez le nom d'utilisateur à autoriser dans l'application dans le champ **Nom d'utilisateur**.

7. Saisissez le mot de passe du compte dans le champ **Mot de passe**. Pour créer le mot de passe automatiquement, cliquez sur le lien **Générateur de mots de passe**.

8. Dans la partie inférieure de la fenêtre, cliquez sur le bouton **Ajouter**.

   Le compte utilisateur créé va être affiché dans la section **Applications**.

## UTILISATION DU GENERATEUR DE MOTS DE PASSE

La sécurité des données est en fonction directe avec la fiabilité de mots de passe. Les données pourront être soumises au risque dans les cas suivants :

- le même mot de passe est utilisé pour tous les comptes ;
- les mots de passe sont très simples ;
- le mot de passe contient l'information qui est facile à deviner (par exemple, les noms de membres de la famille ou la date de leur naissance).

Pour assurer la sécurité des données, l'outil Kaspersky PURE permet de créer les mots de passe uniques et fiables à l'aide du générateur de lots de passe.

Le mot de passe est considéré comme fiable s'il contient plus de quatre caractères et aussi les caractères spéciaux, les chiffres, les lettres majuscules et minuscules.

*Afin de créer un mot de passe fiable à l'aide du générateur des mots de passe, procédez comme suit :*

1. Ouvrez la fenêtre principale du programme et cliquez sur le bouton **Gestionnaire de mots de passe**.

   La fenêtre Gestionnaire de mots de passe s'ouvre.

2. Cliquez sur le bouton **Générateur de mots de passe**.

   Vous pouvez également utiliser le générateur de mot de passe directement lord de l'indication du mot de passe pour le compte utilisateur. Pour appeler le générateur des paroles, utiliser le lien **Générateur des mots de passe** dans la zone de contrôle du compte utilisateur à côté du champ de saisie du mot de passe.

3. Dans la fenêtre ouverte **Générateur des mots de passe** dans le champ **Longueur du mot de passe** saisissez le nombre des caractères du mot de passe.

   La longueur du mot de passe pourrait être de 4 à 99 caractères. Il est estimé, plus le mot de passe est long, plus il est fiable.

4. Si besoin configurez les paramètres complémentaires du générateur des mots de passe, pour cela dans le bloc **Paramètres complémentaires** activez / désactivez les drapeaux à côté des paramètres souhaités.

5. Cliquez sur le bouton **Générer**.

   Dans le champ **Mot de passe** le mot de passe créé va apparaitre.

## AJOUT D'UNE NOUVELLE PAIRE NOM D'UTILISATEUR-MOT DE PASSE

Parfois il est nécessaire d'utiliser quelques couples différentes nom d'utilisateur - mot de passe sur le même site / application. Par exemple, vous pouvez utiliser quelques courriers électroniques sur le même serveur, ou les utilisateurs possédant le même ordinateur peuvent avoir besoin d'accéder à leurs pages sur les réseaux sociaux. Dans ce cas l'outil Kaspersky PURE vous permet de créer un compte associé au site Inernet ou avec l'application souhaitée et spécifier plusieurs paires nom d'utilisateur - mot de passe pour ce compte.

Lors du chargement de cette application, Kaspersky PURE propose de spécifier la couple correspondante nom d'utilisateur - mot de passe pour la saisie dans les champs d'inscription.

Kaspersky PURE reconnait automatiquement un nouveau nom d'utilisateur et propose de l'insérer dans le compte utilisateur de cette application/site Inernet. Vous pouvez ajouter une nouvelle paire nom d'utilisateur-mot de passe manuellement, puis la modifier. Vous pouvez également utiliser la même paire nom d'utilisateur-mot de passe pour différents comptes utilisateur.

*Pour ajouter une nouvelle paire nom d'utilisateur-mot de passe pour un compte utilisateur, procédez comme suit :*

1. Ouvrez la fenêtre principale du programme et cliquez sur le bouton **Gestionnaire de mots de passe**.

   La fenêtre Gestionnaire de mots de passe s'ouvre.

2. Appuyez sur le bouton **Mots de passe et données**.

   Le contenu du stockage des mots de passe et des donnés va s'afficher.

3. Ouvrez la section **Internet** ou **Applications**, en fonction du type de compte utilisateur auquel vous souhaitez ajouter un nom d'utilisateur et un mot de passe.

4. Sélectionnez dans la liste le compte utilisateur souhaité, puis cliquez sur le bouton  .

5. Dans le menu qui s'ouvre, sélectionnez l'option **Ajouter le nom d'utilisateur**.

6. Saisissez le nom d'utilisateur dans le champ **Nom d'utilisateur** et le mot de passe dans le champ **Mot de passe**.

   Si vous voulez ajouter le nom d'utilisateur et le mot de passe qui sont déjà utilisés dans les autres compte utilisateur, appuyez sur le bouton dans le champs **Nom d'utilisateur**. Dans la fenêtre ouverte **Sélection des comptes utilisateur pour l'association** sélectionnez le compte utilisateur contenant le nom d'utilisateur nécessaire et appuyer sur le bouton **Associer**.

7. Si vous voulez que le Gestionnaire de mots de passe saisisse automatiquement les nom d'utilisateur et mot de passe sur le site Inernet ou dans l'application, mettez le drapeau **Entrée automatique** dans la section inférieure de la zone du contrôle du compte utilisateur.

   Si vous ne souhaitez pas que le Gestionnaire de mots de passe saisit automatiquement les noms d'utilisateurs et les mots de passe dans les champs de l'autorisation, décochez la case **Entrée automatique**. Dans ce cas, afin d'utiliser la saisie automatique, il vous faudra sélectionner le nom d'utilisateur et le mot de passe dans le menu contextuel de l'icône du programme ou du bouton du démarrage rapide.

8. Dans la partie inférieure de la fenêtre, cliquez sur le bouton **Ajouter**.

   Le nombre des noms d'utilisateur ajoutés dans le compte utilisateur va être affiché dans la liste des comptes utilisateurs.

# CRYPTAGE DES DONNEES

Pour protéger les données confidentielles contre l'accès non autorisé, il est conseillé de les conserver sous forme chiffrée dans un coffre-fort spécial.

Par défaut, après l'installation de Kaspersky PURE, vous avez accès à un coffre-fort possédant une configuration standard. Pour pouvoir utiliser ce coffre-fort, il faut définir un mot de passe. Vous pouvez également créer des coffres-forts avec les paramètres qui vous conviennent.

Pour que les données soient protégées, elles doivent être placées dans un coffre-fort et chiffrées. Par la suite, pour pouvoir accéder au coffre-fort, il faudra saisir le mot de passe.

*Pour créer un coffre-fort chiffré, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Mes Coffres-forts**.
2. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Créer un coffre-fort** (cf. ill. ci-après).

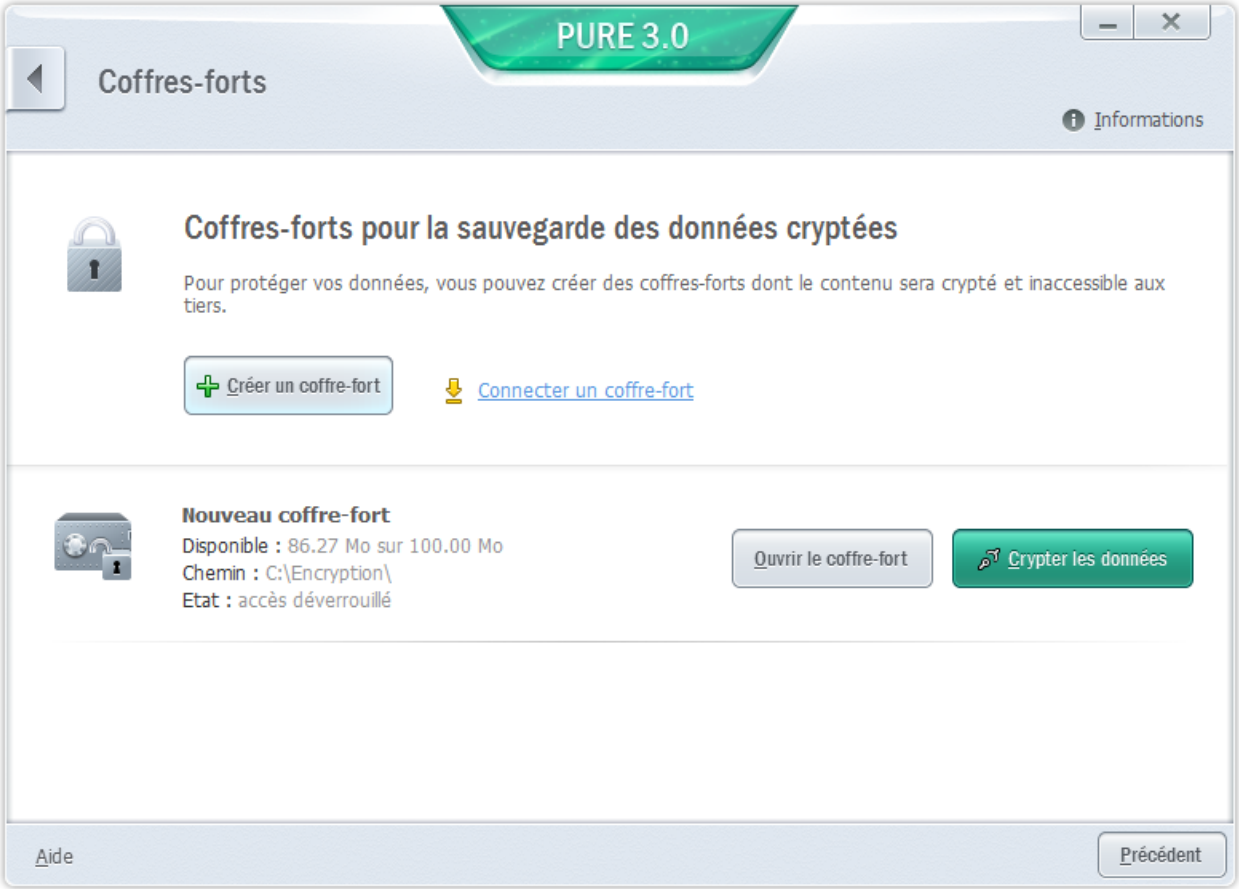


*Illustration 9. Fenêtre **Coffres-forts***

3. Dans la fenêtre **Création d'un coffre-fort crypté**, définissez les paramètres du nouveau coffre-fort.

4. Cliquez sur le bouton **OK**.

*Pour enregistrer les données dans le coffre-fort, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Mes Coffres-forts**.

2. Dans la fenêtre qui s'ouvre, sélectionnez le coffre-fort dans la liste, puis cliquez sur **Ouvrir le coffre-fort**.

   Le coffre-fort s'ouvre dans une fenêtre de l'Assistant Microsoft Windows.

3. Enregistrez les données que vous souhaitez crypter dans le coffre-fort.

4. Dans la fenêtre **Mes Coffres-forts**, cliquez sur le bouton **Crypter les données**.

*Pour accéder aux données dans le coffre-fort, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Mes Coffres-forts**.

2. Dans la fenêtre qui s'ouvre, sélectionnez le coffre-fort dans la liste, puis cliquez sur **Décrypter les données**.

3. Dans la fenêtre qui s'ouvre, saisissez le mot de passe d'accès au coffre-fort.

4. Dans la fenêtre **Mes Coffres-forts**, cliquez sur le bouton **Ouvrir le coffre-fort**.

## SUPPRESSION DES DONNEES NON UTILISEES

Au fil du temps, des fichiers temporaires et des fichiers inutilisés s'accumulent dans le système d'exploitation. Ces fichiers peuvent occuper un volume important, ce qui réduit les performances du système. Ils peuvent également être exploités par des individus malintentionnés.

Les fichiers temporaires sont créés au lancement de n'importe quel système d'exploitation ou application. Une fois l'application fermée, tous ces fichiers ne sont pas automatiquement supprimés. Kaspersky PURE propose un Assistant de suppression des données non utilisées.

L'Assistant de suppression des données non utilisées permet de supprimer les fichiers suivants :

- journaux des événements système dans lequel sont consignés les noms de toutes les applications ouvertes ;
- journaux des événements de divers utilitaires ou applications (par exemple, Windows Updater) ;
- journaux des connexions système ;
- fichiers temporaires des navigateurs Internet (cookies) ;
- fichiers temporaires qui restent après l'installation ou la désinstallation d'une application ;
- contenu de la Corbeille ;
- fichiers du dossier TEMP dont la taille peut parfois atteindre plusieurs gigaoctets.

Outre la suppression des fichiers inutiles, l'Assistant se débarrasse également des fichiers pouvant contenir des données confidentielles (mots de passe, noms d'utilisateurs ou informations tirées de formulaires d'enregistrement). Ceci étant dit, pour supprimer complètement de telles données, il est conseillé d'utiliser l'Assistant de suppression des traces d'activité (cf. page 59).

*Pour lancer l'Assistant de suppression des données inutilisées, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre, cliquez sur le bouton **Outils complémentaires**.

   La fenêtre **Outils complémentaires** s'ouvre (cf. ill. ci-dessous).

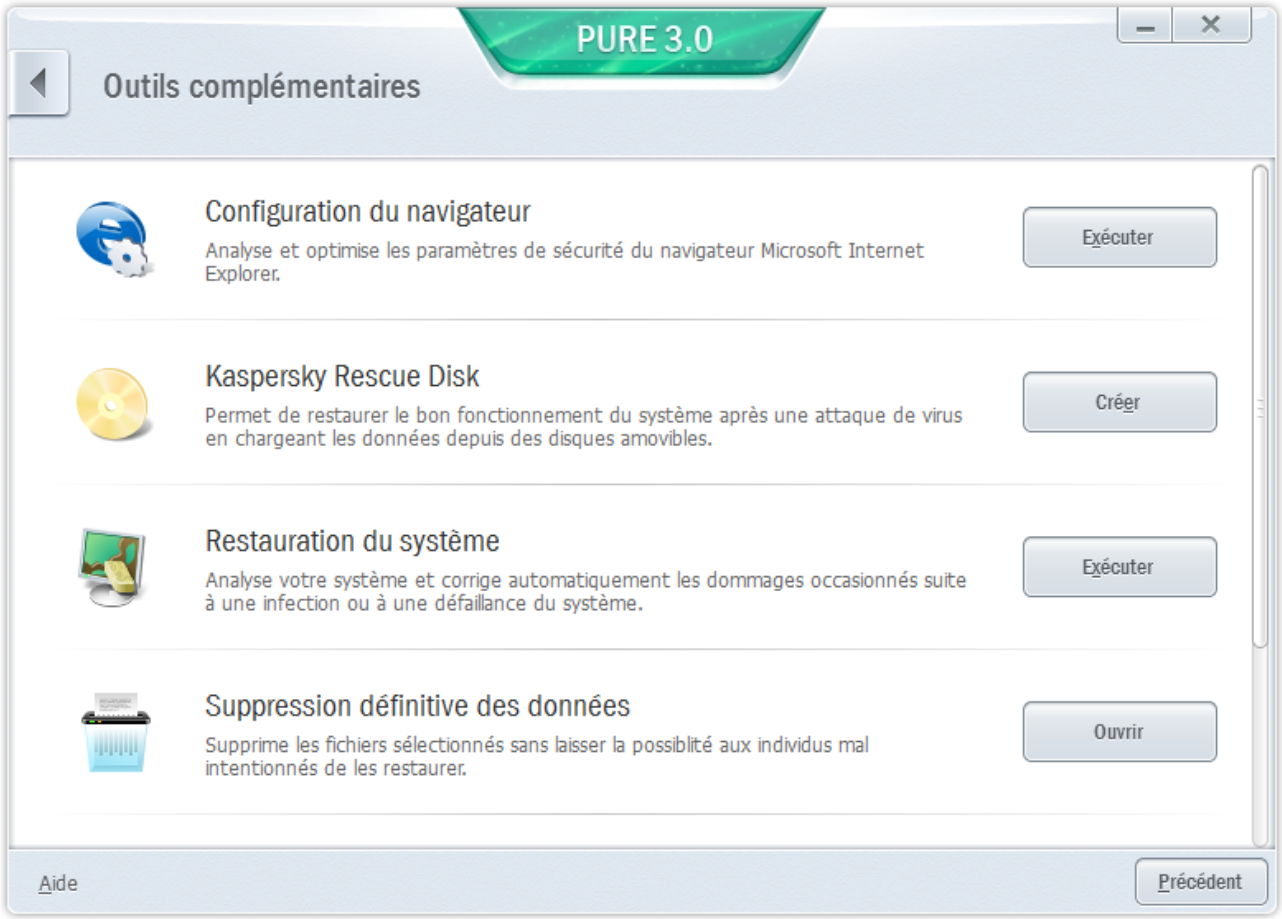


*Illustration 10. Fenêtre **Outils complémentaires***

3. Dans le groupe **Suppression des données non utilisées** de la fenêtre qui s'ouvre, cliquez sur le bouton **Exécuter**.

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**.

Examinons en détails les étapes de l'Assistant.

## Etape 1. Début de l'Assistant

La première fenêtre de l'Assistant propose des informations relatives à la suppression des données non utilisées.

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

## Etape 2. Recherche des données non utilisées

L'Assistant recherche les données non utilisées sur l'ordinateur. La recherche peut durer un certain temps. Une fois la recherche terminée, l'Assistant passe automatiquement à l'étape suivante.

### Etape 3. Sélection de l'action pour la suppression des données non utilisées

A la fin de la recherche, l'Assistant de suppression des données non utilisées affiche la liste des actions qui peuvent être réalisées sur les données en question.

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

Pour que l'Assistant effectue 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, décochez la case en regard de celle-ci.

Il est déconseillé de décochez les cases sélectionnées par défaut. Cela pourrait créer des menaces contre la sécurité de votre ordinateur.

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

### Etape 4. Nettoyage du disque

L'Assistant exécute les actions sélectionnées à l'étape précédente. La suppression des informations non utilisées peut durer un certain temps.

Après le nettoyage du disque, l'Assistant passe automatiquement à l'étape suivante.

Pendant l'exécution de l'Assistant, il se peut que certains fichiers (par exemple, le fichier journal de Microsoft Windows ou le journal des événements de Microsoft Office) soient utilisés par le système. Afin de pouvoir supprimer ces fichiers, l'Assistant propose de redémarrer le système.

### Etape 5. Fin de l'Assistant

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

## SUPPRESSION DEFINITIVE DES DONNEES

La protection contre la restauration non autorisée des données supprimées par des individus malintentionnés constitue un niveau de sécurité supplémentaire pour les données personnelles.

Kaspersky PURE propose un module pour la suppression irréversible des données qui met en échec les outils de restauration logiciels traditionnels.

Kaspersky PURE permet de supprimer de manière irréversible les données sur les types de support suivants :

- Disques locaux. La suppression est possible si l'utilisateur possède les privilèges d'écriture et de suppression des informations.
- Disques amovibles ou autres périphériques identifiés comme disque amovibles (par exemple, disquettes, cartes mémoire, cartes USB ou téléphones mobiles). La suppression des données sur la carte mémoire est possible si le mode de protection contre l'écriture n'a pas été activé mécaniquement.

Vous pouvez supprimer les données auxquelles vous avez accès sous les privilèges de votre compte. Avant de supprimer des données, assurez-vous que ces données ne sont pas utilisées par des applications en exécution.

*Pour supprimer les données sans possibilité de les restaurer, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre, cliquez sur le bouton **Outils complémentaires**.

La fenêtre **Suppression définitive des données** s'ouvre (cf. ill. ci-après).

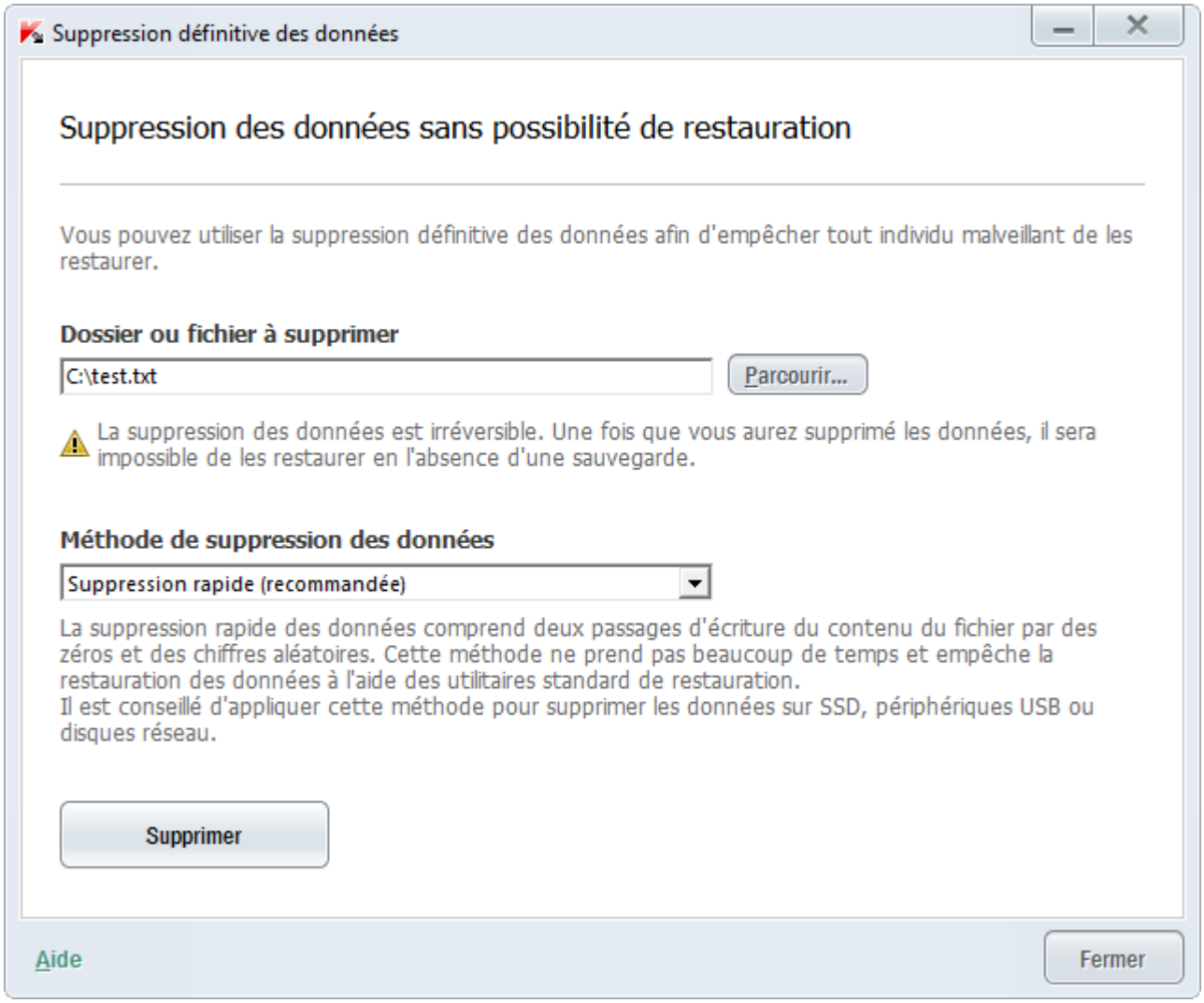


*Illustration 11. Fenêtre **Suppression définitive des données***

3. Dans le groupe **Suppression définitive des données** de la fenêtre qui s'ouvre, cliquez sur le bouton **Ouvrir**.

4. Dans la fenêtre **Suppression irréversible des données** qui s'ouvre, cliquez sur le bouton **Parcourir** et dans la fenêtre **Fichier ou dossier** qui s'ouvre, sélectionnez le fichier ou le dossier à supprimer de manière irréversible.

   La suppression de fichiers système peut entraîner des échecs dans le système d'exploitation. Si vous avez choisi des fichiers ou des dossiers système à supprimer, l'application vous invite à confirmer la suppression de ceux-ci.

5. Sélectionnez l'algorithme de suppression des données souhaité dans la liste déroulante **Méthode de suppression des données**.

   Pour supprimer les données sur un périphérique SSD, USB ou sur des disques réseau, il faut utiliser la méthode Suppression rapide ou GOST R 50739-95. Les autres algorithmes de suppression pourraient nuire au périphérique réseau ou amovible.

6. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **OK** pour confirmer la suppression des données. Si certains fichiers n'ont pas été supprimés, relancez la suppression en cliquant sur le bouton **Réessayer** dans la fenêtre qui s'ouvre. Pour sélectionner un autre objet à supprimer, cliquez sur **Terminer**.

# SUPPRESSION DES TRACES D'ACTIVITE

Lorsque vous utilisez votre ordinateur, vos activités sont enregistrées dans le système d'exploitation. Les informations suivantes sont conservées :

- données sur les termes de recherche et les sites Internet visités ;
- informations sur l'exécution d'applications et l'ouverture et l'enregistrement de fichiers ;
- entrées dans le journal système Microsoft Windows ;
- autres informations relatives aux actions de l'utilisateur.

Les informations relatives aux actions de l'utilisateur impliquant des données confidentielles sont potentiellement accessibles aux individus malintentionnés et aux tiers.

Kaspersky PURE propose un Assistant de suppression des traces d'activité de l'utilisateur dans le système.

*Pour lancer l'Assistant de suppression des traces d'activité, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre, sélectionnez la section **Outils complémentaires**.
3. Dans le groupe **Suppression des traces d'activité** de la fenêtre qui s'ouvre, cliquez sur le bouton **Exécuter**.

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**.

Examinons en détails les étapes de l'Assistant.

## Etape 1. Début de l'Assistant

Assurez-vous que l'option **Rechercher les traces d'activité de l'utilisateur** est sélectionnée, puis appuyez sur le bouton **Suivant** pour lancer l'Assistant.

## Etape 2. Recherche des 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 supprimer les traces d'activité

A la fin de la recherche, l'Assistant indique les traces d'activité détectées et les moyens proposés pour les éliminer (cf. ill. ci-après).

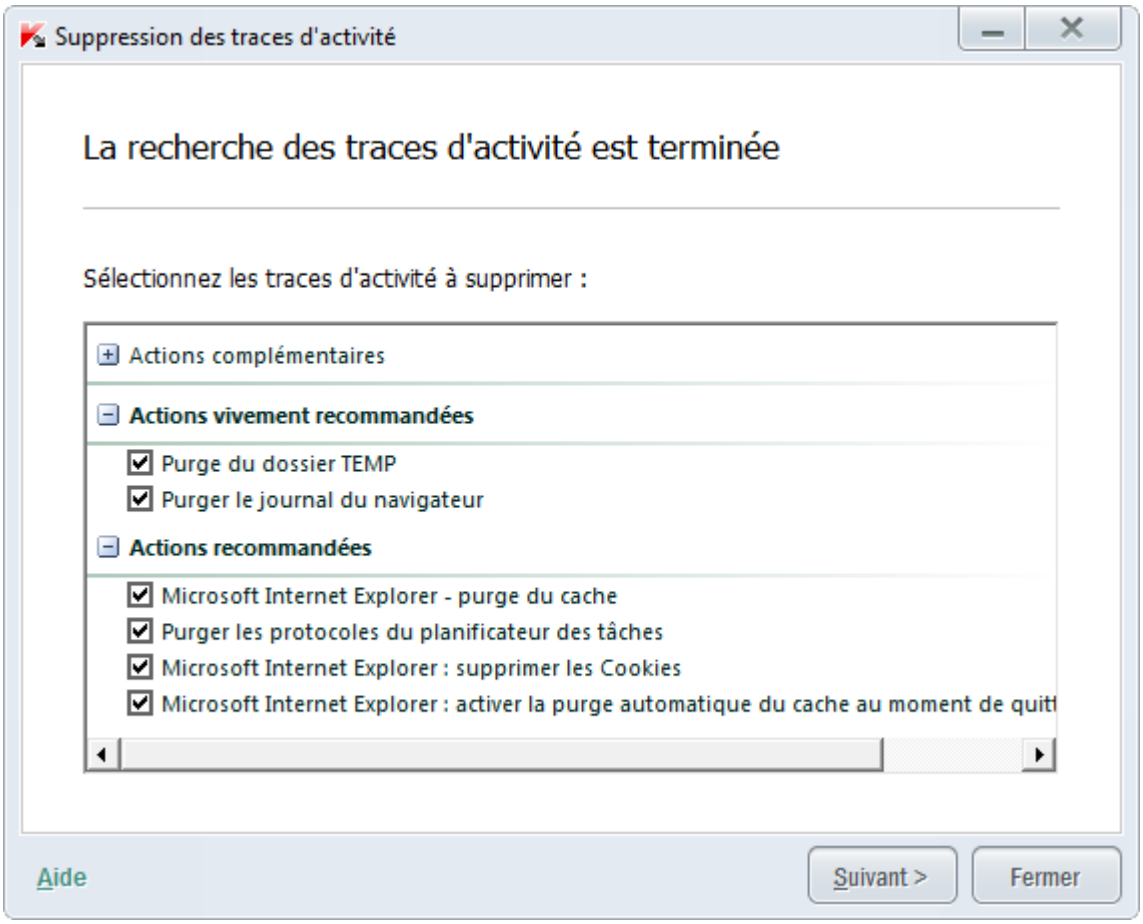


*Illustration 12. Traces d'activité détectées et recommandations pour leur suppression*

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

Pour que l'Assistant effectue 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, décochez la case en regard de celle-ci.

Il est déconseillé de décochez les cases sélectionnées par défaut. Cela pourrait créer des menaces contre la sécurité de votre 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 supprimées, 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 PURE, cochez la case **Supprimer les traces d'activité à chaque arrêt de Kaspersky PURE** 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, ne cochez pas cette case.

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

# SAUVEGARDE

La protection principale contre la perte de données importantes est la création de copies de sauvegarde sur un support fiable. Kaspersky PURE permet de créer automatiquement des copies de sauvegarde des données sélectionnées dans le stockage indiqué selon un horaire prédéfini ou manuellement.

Grâce à Mon Réseau (cf. section "Administration à distance de la protection du réseau domestique" à la page 41), vous pouvez lancer la tâche de sauvegarde sur les ordinateurs du réseau domestique et suivre l'état de l'exécution de ces tâches.

Vous pouvez utiliser les supports suivants pour la création de copies de sauvegarde :

- disque local ;
- disque amovible (par exemple, un disque dur externe) ;
- disque réseau ;
- serveur FTP ;
- stockage en ligne.

## DANS CETTE SECTION



# COPIE DE SAUVEGARDE DES DONNEES

*Pour créer une copie de sauvegarde, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Sauvegardes**.
2. Dans la fenêtre **Sauvegardes** qui s'ouvre, cliquez sur le bouton **Créer une tâche de sauvegarde**.

   L'Assistant de création d'une tâche de sauvegarde est lancé.

   Examinons en détails les étapes de l'Assistant.

   a. Dans la fenêtre de sélection du type de données, effectuez une des opérations suivantes :

   - Pour une configuration rapide, choisissez un des types de données prédéfinis (fichiers des dossiers Mes documents et Bureau, vidéo, photos, fichiers musicaux).
   - Choisissez l'option **Fichiers sélectionné** si vous souhaitez sélectionner manuellement les fichiers dont vous souhaitez créer une copie de sauvegarde.

b. Si vous aviez choisi l'option **Fichiers sélectionnés** à l'étape précédente, désignez dans la fenêtre de sélection des fichiers les fichiers ou la catégorie de fichiers dont il faut créer une copie de sauvegarde.

Lors de la création de copies de sauvegarde à l'aide du Stockage en ligne, Kaspersky PURE ne crée pas de copies de sauvegarde pour les données soumises aux restrictions des règles d'utilisation de Dropbox (cf. section "Utilisation du stockage en ligne" à la page 63)

c. Dans la fenêtre de sélection du stockage, effectuez une des opérations suivantes :

- Sélectionnez un des stockages proposés dans lequel les copies de sauvegarde vont être créées.

  Par défaut, Kaspersky PURE permet de créer des copies de sauvegarde sur les disques locaux et de réseaux ainsi que dans la Sauvegarde en ligne.

  Avant de pouvoir utiliser le Stockage en ligne pour la création de copies de sauvegarde de vos données, il faut l'activer (cf. section "Utilisation du stockage en ligne" à la page 63).

- Sélectionnez un stockage réseau existant.

- Cliquez sur le bouton **Ajouter un stockage** pour créer un stockage réseau.

  Pour garantir la sécurité des données, il est conseillé d'utiliser la Sauvegarde en ligne ou de créer le stockage des copies de sauvegarde sur un disque amovible.

d. Dans la fenêtre de programmation, définissez les conditions de lancement de la tâche.

Si vous souhaitez réaliser une copie de sauvegarde ponctuelle, ne cochez pas la case **Lancer automatiquement selon la programmation**.

e. Saisissez dans la fenêtre **Récapitulatif** le nom de la nouvelle tâche, cochez la case **Lancer la tâche à la fin de l'assistant**, puis cliquez sur **Terminer**.

# RESTAURATION DES INFORMATIONS AU DEPART DE LA COPIE DE SAUVEGARDE

*Pour restaurer des données depuis la sauvegarde, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Sauvegardes**.
2. Choisissez la section **Restauration des données**.
3. Sélectionnez le stockage qui contient les sauvegardes requises, puis cliquez sur **Restaurer les données**.

   La fenêtre **Restauration des données depuis le stockage** s'ouvre.
4. Dans la fenêtre qui s'ouvre, procédez comme suit :

   a. Sélectionnez dans la liste déroulante **Tâche de sauvegarde** la tâche qui a permis de créer les copies de sauvegarde requises.

   b. Dans la liste déroulante **Date**, sélectionnez la date et l'heure de création des copies de sauvegarde requises.

   c. Dans la liste déroulante **Catégorie**, sélectionnez le type de fichier à restaurer.

5. Dans la liste des fichiers de la partie inférieure de la fenêtre, sélectionnez les fichiers à restaurer. Pour ce faire, cochez la case en regard des fichiers qui vous intéressent.

   Kaspersky PURE ne permet pas la restauration de données depuis le Stockage en ligne si celles-ci ont été supprimées via l'interface Internet de Dropbox.

6. Cliquez sur le bouton **Restaurer les données**.

   La fenêtre **Restauration** s'ouvre.

7. Indiquez, dans la fenêtre **Restauration**, l'emplacement où seront enregistrés les fichiers restaurés (dans le dossier d'origine ou dans un dossier sélectionné).

8. Cliquez sur le bouton **Restaurer les données sélectionnées**.

   Les fichiers sélectionnés pour la restauration seront restaurés et enregistrés dans le dossier indiqué.

   En cas de détection d'une autre version d'un des fichiers sélectionnés pour la restauration, l'application propose de remplacer le fichier actuel par la copie de sauvegarde ou d'enregistrer les deux fichiers.

# UTILISATION DU STOCKAGE EN LIGNE

Le Stockage en ligne permet d'enregistrer les copies de sauvegarde de vos données sur un serveur distant. via le service Dropbox.

L'utilisation du Stockage en ligne requiert la création d'un compte sur le site du fournisseur de stockage en ligne Dropbox.

Vous pouvez utiliser le même compte utilisateur Dropbox pour conserver dans un seul Stockage en ligne les données de divers périphériques dotés de Kaspersky PURE.

Un compte standard sur Dropbox permet de stocker un maximum de 2 Go de données sur le disque distant. Le cas échéant, vous pouvez augmenter l'espace de la Sauvegarde en ligne selon les conditions définies par le fournisseur des services de sauvegarde. Vous trouverez de plus amples informations sur les conditions d'utilisation du service sur le site de Dropbox.

Avant de pouvoir utiliser le Stockage en ligne pour créer des copies de sauvegarde de vos données, il faut l'activer.

*Pour activer le Stockage en ligne, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Sauvegardes**.

2. Dans la fenêtre **Sauvegardes** qui s'ouvre, cliquez sur le bouton **Créer une tâche de sauvegarde**.

   L'Assistant de création d'une tâche de sauvegarde est lancé.

3. Dans la fenêtre de sélection du type de données, sélectionnez la catégorie de données ou désigner manuellement les fichiers dont vous souhaitez créer des copies de sauvegarde.

4. Dans la fenêtre de sélection du stockage, choisissez le Stockage en ligne, puis cliquez sur **Activer maintenant**.

   La fenêtre d'accès au compte Dropbox s'ouvre.

5. Exécutez une des opérations suivantes dans la fenêtre qui s'ouvre :

   a. Si vous ne possédez pas de compte Dropbox, ouvrez-en un maintenant.

   b. Si vous avez déjà votre compte Dropbox, saisissez vos données d'identification.

   Pour terminer l'activation de la Sauvegarde en ligne, confirmez que Kaspersky PURE peut utiliser votre compte Dropbox pour exécuter la sauvegarde et restaurer les informations. Kaspersky PURE va placer les copies de sauvegarde des données enregistrées dans un dossier séparés créé dans le dossier d'enregistrement des applications de Dropbox.

   Une fois l'activation de la Sauvegarde en ligne terminée, la fenêtre de sélection du stockage s'ouvre. La Sauvegarde en ligne pourra être sélectionnée. Le volume occupé et le volume disponible pour l'enregistrement d'informations sont indiqués pour la Sauvegarde en ligne activée.

# RESTRICTION DE L'ACCES AUX PARAMETRES DE KASPERSKY PURE A L'AIDE D'UN MOT DE PASSE

Il peut arriver que plusieurs personnes aux connaissances de l'outil informatique variées utilisent le même ordinateur. L'accès sans restriction de différents utilisateurs à l'administration de Kaspersky PURE et à ses paramètres peut déboucher sur une réduction du niveau de protection de l'ordinateur.

Pour limiter l'accès à l'application, vous pouvez définir un mot de passe d'administrateur et identifier les actions dont l'exécution ne pourra avoir lieu qu'après la saisie de ce mot de passe :

- configuration des paramètres de l'application ;
- gestion de la Sauvegarde ;
- administration à distance de la sécurité sur les ordinateurs du réseau domestique (le mot de passe doit être le même sur tous les ordinateurs ;
- administration du Contrôle Parental ;
- arrêt de l'application ;
- suppression de l'application.

*Pour protéger l'accès à Kaspersky PURE à l'aide d'un mot de passe, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Cliquez sur le lien **Configuration** dans le coin supérieur droit de la fenêtre.

   La fenêtre de configuration de l'application s'ouvre.

3. Dans la partie supérieure de la fenêtre de configuration de l'application, choisissez l'onglet **Mot de passe** (cf. ill. ci-après).

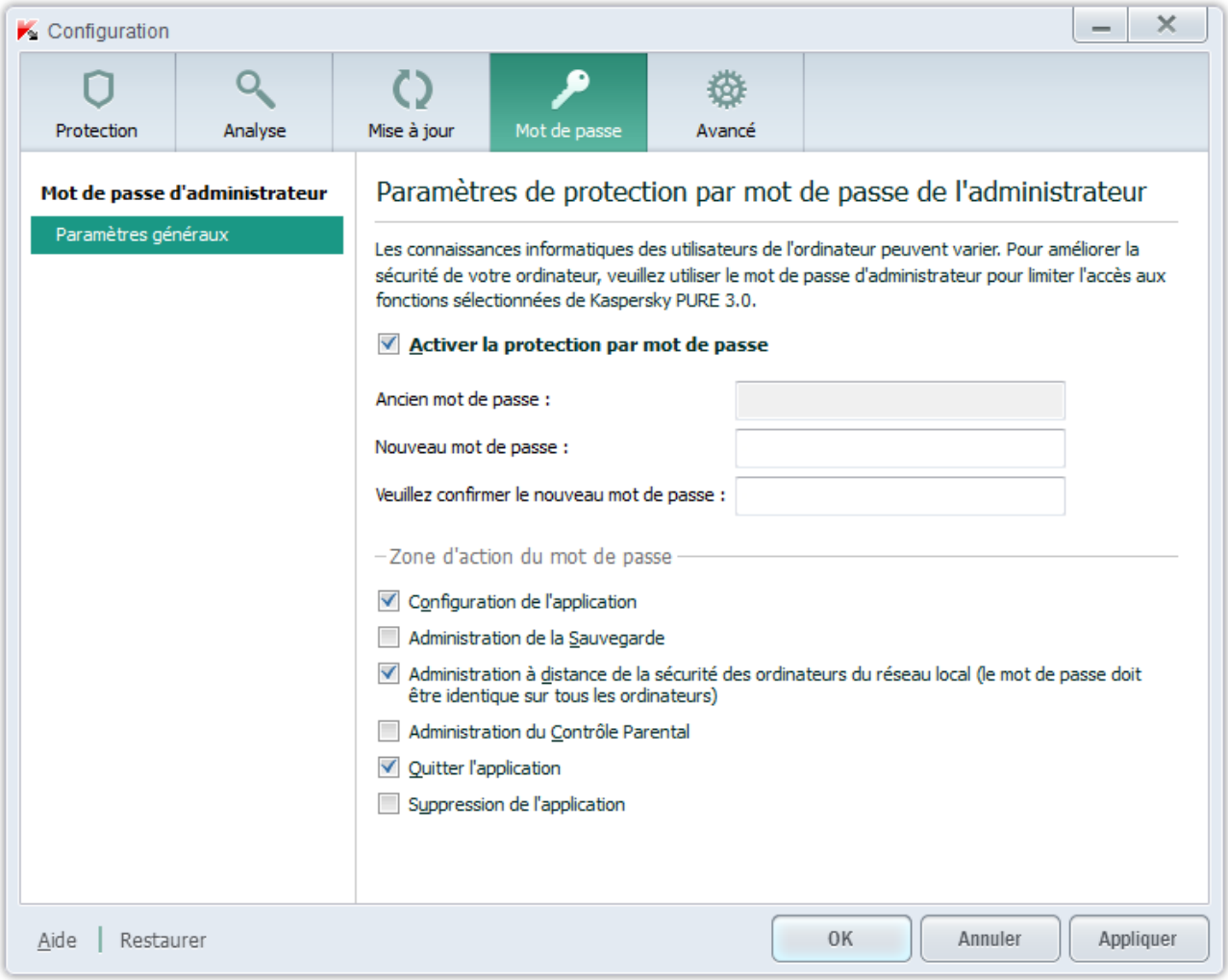


*Illustration 13. Fenêtre **Configuration**, section **Mot de passe***

4. Dans la partie droite de la fenêtre, cochez la case **Activer la protection par mot de passe**, puis remplissez les champs **Nouveau mot de passe** et **Confirmation du mot de passe**.

5. Si vous souhaitez modifier un mot de passe existant, saisissez-le dans le champ **Ancien mot de passe**.

6. Indiquez dans le groupe de paramètres **Zone d'action du mot de passe** les actions dont l'exécution ne pourra avoir lieu qu'après la saisie du mot de passe.

7. Cliquez sur le bouton **Appliquer** afin d'enregistrer les modifications introduites.

Il est impossible de récupérer un mot de passe oublié. Si vous oubliez votre mot de passe et que vous ne parvenez plus à accéder aux paramètres de Kaspersky PURE, il faut contacter le Support technique.

# UTILISATION DU CONTROLE PARENTAL

Le *Contrôle Parental* permet de contrôler les actions de différents utilisateurs sur l'ordinateur et sur le réseau. A l'aide du Contrôle Parental vous pouvez limiter l'accès aux ressources Internet et aux applications et 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. En utilisant l'ordinateur et Internet, les enfants sont confrontés à toute une série de menaces :

- la perte de temps et/ou d'argent lors des connexions aux messageries instantanés, aux jeux, aux boutiques en ligne, aux ventes aux enchères.
- l'accès à des sites Internet 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 ;
- le dommage corporel dû à une utilisation de longue durée de l'ordinateur.
- des contacts avec des inconnus qui, en se faisant passer pour des amis, peuvent obtenir des informations personnelles de l'enfant (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, le module possède les fonctions suivantes :

- restriction temporelle de l'utilisation de l'ordinateur et d'Internet ;
- 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 consultées ;
- 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 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 sur 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 différents utilisateurs. Des rapports sont rédigés pour chaque compte utilisateur. Ces rapports reprennent les événements des catégories contrôlées pour une période donnée.

### DANS CETTE SECTION



# CONFIGURATION DU CONTROLE PARENTAL

Si vous n'avez pas défini un mot de passe pour l'accès aux paramètres de Kaspersky PURE (cf. page 64), l'application vous propose, au premier lancement du Contrôle Parental, de définir un mot de passe pour éviter l'accès non autorisé aux paramètres du contrôle. Ensuite, vous pouvez configurer les restrictions d'utilisation de l'ordinateur et d'Internet pour tous les comptes utilisateur de l'ordinateur.

*Pour configurer le Contrôle Parental pour un compte utilisateur, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Contrôle Parental**.

   La fenêtre **Utilisateurs de l'ordinateur** s'ouvre. Elle affiche tous les comptes utilisateur créés sur l'ordinateur.

2. Cliquez sur le bouton **Sélectionnez le niveau de contrôle** pour le compte utilisateur requis.

3. Dans la fenêtre **Contrôle Parental** qui s'ouvre, réalisez une des opérations suivantes :

   - Sélectionnez un des niveaux de contrôle prédéfinis (**Collecte des statistiques**, **Profil "Enfant"** ou **Profil "Adolescent"**).

   - Définissez les restrictions manuellement :

     a. Sélectionnez l'option **Restrictions personnalisées**.

     b. Cliquez sur le bouton **Configuration**.

        La fenêtre **Contrôle Parental** s'ouvre.

     c. Sous l'onglet **Configuration** de la fenêtre qui s'ouvre, sélectionnez le type de restriction dans la partie gauche de la fenêtre, puis définissez les paramètres du contrôle dans la partie droite de la fenêtre.

     d. Cliquez sur le bouton **OK** pour enregistrer les paramètres du contrôle après la configuration.

4. Cliquez sur le bouton **OK** dans la fenêtre **Contrôle Parental**.

## CONSULTATION DU RAPPORT 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.

2. Dans la partie inférieure de la fenêtre, sélectionnez la section **Contrôle Parental**.

3. Dans la fenêtre qui s'ouvre, cliquez sur le bouton dans le groupe contenant le compte utilisateur  .

   La fenêtre **Contrôle Parental** s'ouvre.

4. Sélectionnez l'onglet **Rapports**.

5. Dans la partie gauche de la fenêtre, sélectionnez la section 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.

# SUSPENSION ET RESTAURATION DE LA PROTECTION DE L'ORDINATEUR

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

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

1. Choisissez l'option **Suspendre la protection** dans le menu contextuel de l'icône de l'application dans la zone de notification.

   La fenêtre **Suspension de la protection** s'ouvre (cf. ill. ci-dessous).

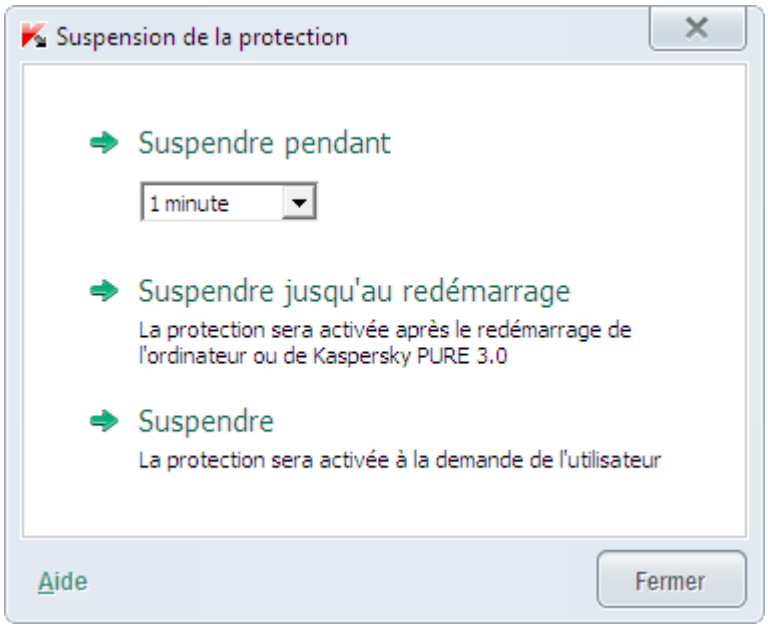


*Illustration 14. Fenêtre **Suspension de la protection***

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

   - **Suspendre pendant la période indiquée** : la protection sera activée à l'issue de l'intervalle défini dans la liste déroulante ci-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).
   - **Reprendre manuellement** : la protection sera activée lorsque vous déciderez de la rétablir.

*Pour restaurer la protection de l'ordinateur,*

sélectionnez l'option **Réactiver la protection** dans le menu contextuel de l'icône de l'application dans la zone de notifications.

# CONSULTATION DU RAPPORT SUR LA PROTECTION DE L'ORDINATEUR

Kaspersky PURE génère des rapports sur le fonctionnement de chaque module de protection. Ce rapport donne des données statistiques sur la protection de l'ordinateur (par exemple, nombre d'objets malveillants détectés et neutralisés pendant la période indiquée, nombre de fois que l'application a été actualisée, nombre de messages non sollicités détectés, etc.)

*Pour consulter le rapport sur la protection de l'ordinateur, procédez comme suit :*

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Protection de l'ordinateur**.

   La fenêtre **Protection de l'ordinateur** s'ouvre.

2. Cliquez sur le lien **Rapports** dans la partie supérieure de la fenêtre afin d'ouvrir la fenêtre des rapports sur la protection de l'ordinateur.

   Les rapports sur la protection de l'ordinateur sont présentés sous la forme de diagrammes dans la fenêtre **Rapports**.

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

   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.

# RESTAURATION DES PARAMETRES STANDARD DU FONCTIONNEMENT DE L'APPLICATION

A tout moment, vous pouvez restaurer les paramètres du fonctionnement de Kaspersky PURE recommandés par Kaspersky Lab. La restauration des paramètres s'opère à l'aide de l'Assistant de configuration de l'application.

A la fin de l'Assistant, le niveau de protection *Recommandé* sera sélectionné pour tous les modules de protection. Lors de la restauration du niveau de protection recommandé, vous pouvez enregistrer sélectivement les paramètres configurés auparavant pour les modules de l'application.

*Pour restaurer les paramètres de fonctionnement recommandés de l'application, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.

2. Cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.

3. Dans la fenêtre **Configuration** qui s'ouvre, lancez l'Assistant de configuration de l'application d'une des méthodes suivantes :

   - Cliquez sur le lien **Restaurer** dans le coin inférieur gauche de la fenêtre.

- Dans la partie supérieure de la fenêtre, choisissez la section **Paramètres avancés**, sous-section **Administration des paramètres**, puis cliquez sur le bouton **Restaurer** dans le groupe **Restauration des paramètres par défaut** (cf. ill. ci-après).

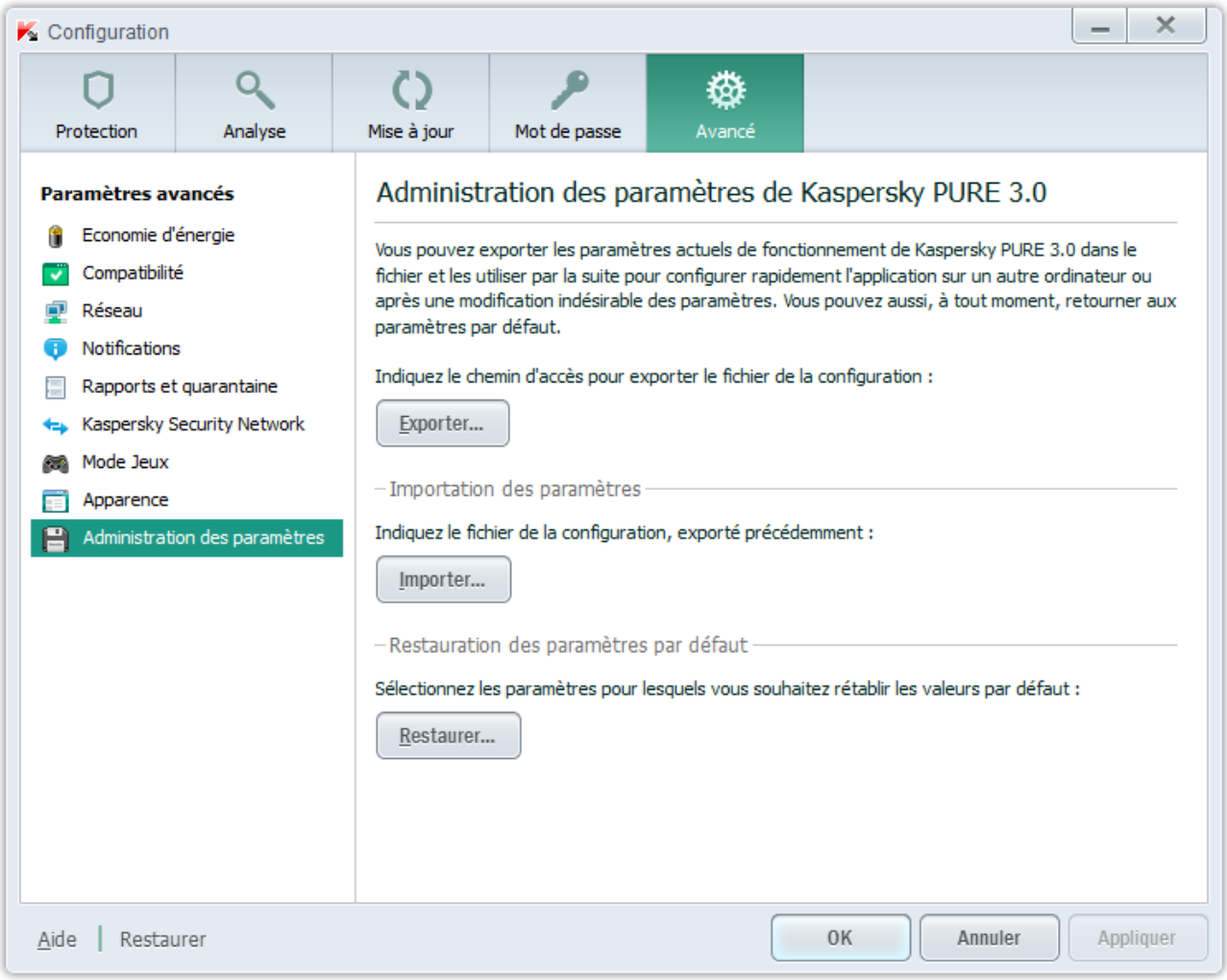


*Illustration 15. Fenêtre **Configuration**, sous-section **Administration des paramètres***

Examinons en détails les étapes de l'Assistant.

## Etape 1. Début de l'Assistant

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

## Etape 2. Restauration des paramètres

Cette fenêtre de l'Assistant reprend les modules de la protection de Kaspersky PURE dont les paramètres ont été modifiés par l'utilisateur ou assimilés par Kaspersky PURE durant l'entraînement des modules de la protection Pare-feu et Anti-Spam. Si des paramètres uniques ont été définis pour un module quelconque, ils figureront également dans la fenêtre (cf. ill. ci-après).

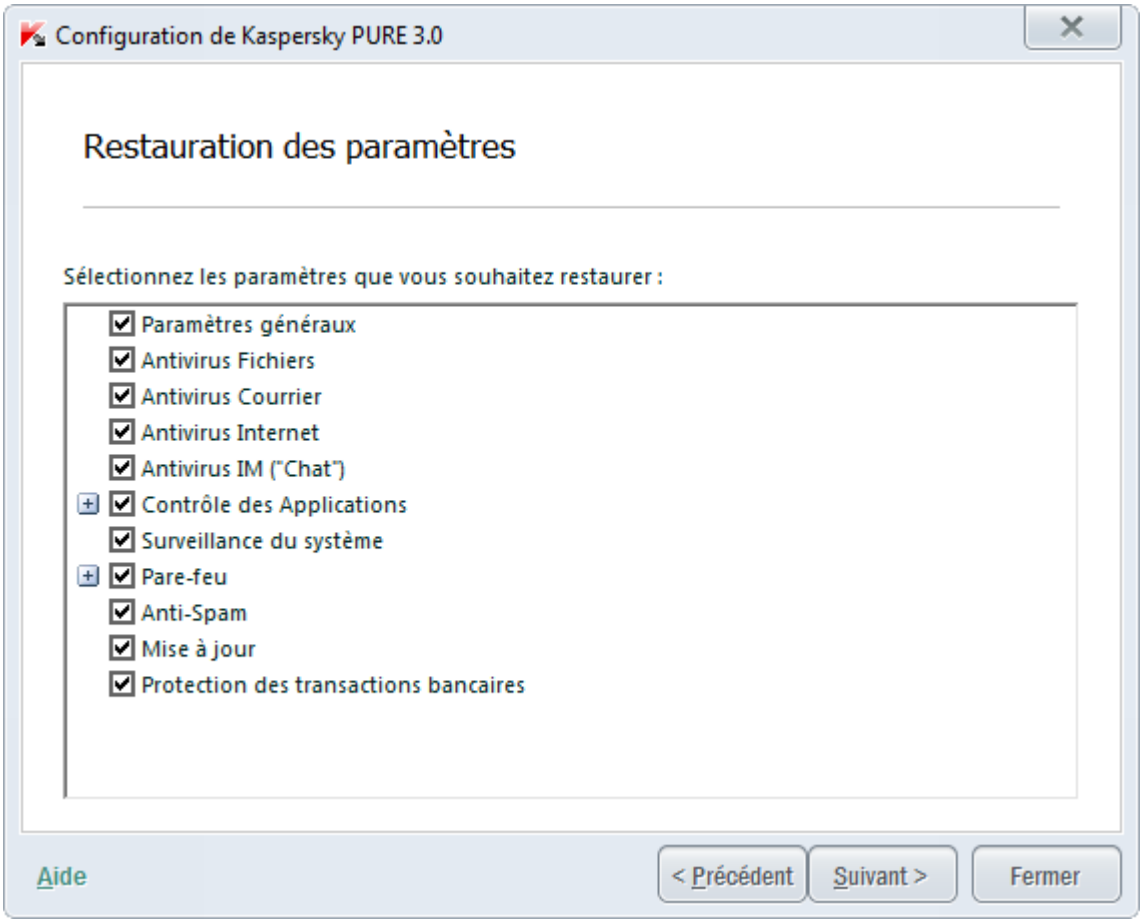


*Illustration 16. Fenêtre **Restauration des paramètres***

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

Les paramètres uniques sont définis pendant l'utilisation de Kaspersky PURE et tiennent compte des tâches individuelles et des exigences de sécurité. Kaspersky Lab recommande d'enregistrer les paramètres uniques lors de la restauration des paramètres initiaux de l'application.

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**.

# IMPORTATION DES PARAMETRES DE L'APPLICATION VERS KASPERSKY PURE INSTALLE SUR UN AUTRE ORDINATEUR

Après avoir configuré l'application, vous pouvez appliquer ses paramètres de fonctionnement à une version de Kaspersky PURE 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 PURE sur votre ordinateur chez vous et au bureau.

Le transfert des paramètres de Kaspersky PURE d'un ordinateur vers un autre s'effectue en trois étapes :

1. Exportation des paramètres de l'application dans le fichier de configuration.
2. Transfert du fichier de configuration vers un autre ordinateur (par exemple, par courrier électronique ou via support amovible).
3. Application des paramètres du fichier de configuration au programme installé sur l'autre ordinateur.

*Pour enregistrer les paramètres de l'application Kaspersky PURE dans un fichier de configuration, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
3. Dans la partie supérieure de la fenêtre **Configuration**, sélectionnez la sous-section **Administration des paramètres** dans la section **Avancé**.
4. Dans la sous-section **Administration des paramètres**, cliquez sur le bouton **Exporter**.
5. Saisissez le nom du fichier de configuration dans la fenêtre qui s'ouvre et indiquez le dossier de sauvegarde.
6. Cliquez sur le bouton **OK**.

*Pour appliquer les paramètres du fichier de configuration à une application installée sur un autre ordinateur, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
3. Dans la partie supérieure de la fenêtre **Configuration**, sélectionnez la sous-section **Administration des paramètres** dans la section **Avancé**.
4. Dans la sous-section **Administration des paramètres**, cliquez sur le bouton **Importer**.
5. Dans la fenêtre qui s'ouvre, sélectionnez le fichier à utiliser pour importer les paramètres de Kaspersky PURE.
6. Cliquez sur le bouton **OK**.

# CREATION ET UTILISATION DU DISQUE DE DEPANNAGE

Le disque de dépannage correspond à l'application Kaspersky Rescue Disk enregistrée sur le support amovible (CD ou périphérique USB).

Vous pouvez utiliser Kaspersky Rescue Disk pour analyser et réparer l'ordinateur infecté lorsque sa réparation est impossible par un autre moyen (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 au format ISO) avec la version actuelle de l'application Kaspersky Rescue Disk et à l'enregistrer sur un support amovible.

L'image du disque de départ peut être téléchargée à partir 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 et d'enregistrement de Kaspersky Rescue Disk. 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\AVP13\Data\Rdisk\ ;
- Sous Microsoft Windows Vista, Microsoft Windows 7 et Microsoft Windows 8 dans le dossier : ProgramData\Kaspersky Lab\AVP12\Data\Rdisk\.

*Pour créer un disque de dépannage, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre, sélectionnez la section **Outils complémentaires**.
3. Dans la fenêtre **Kaspersky Rescue Disk** qui s'ouvre, cliquez sur le bouton **Créer**.

   La fenêtre **Assistant de création d'un disque de dépannage** s'ouvre.

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**.

Examinons en détails les étapes de l'Assistant.

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

La première fenêtre de l'Assistant reprend les informations sur l'application Kaspersky Rescue Disk.

Si l'Assistant découvre un fichier d'image de disque dans le dossier prévu à cet effet (cf. ci-dessus), alors la case **Utiliser l'image de disque existante** apparaît dans la première fenêtre. Cochez la case pour utiliser le fichier découvert en guise d'image source pour le disque et passez directement à l'étape **Mise à jour de l'image du disque** (cf. ci-après). Si vous ne voulez pas utiliser l'image du disque trouvée, décochez cette case. L'Assistant passera 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**, cette étape est ignorée.

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

- Sélectionnez l'option **Copier l'image depuis le disque local ou depuis un disque réseau** si vous possédez déjà un disque de dépannage ou son image (fichier au format ISO) et qu'il 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 l'image du disque de dépannage afin de la 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**, cette étape est ignorée.

Si à l'étape précédente vous aviez choisi l'option **Copier l'image depuis le disque local ou depuis un disque réseau**, 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 à l'étape précédente vous aviez choisi l'option **Télécharger l'image depuis le serveur de Kaspersky Lab**, alors la progression du téléchargement s'affichera directement.

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

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

La procédure de mise à jour du fichier de l'image du disque reprend les actions suivantes :

- la mise à jour des bases de l'application ;

- la mise à jour des fichiers de configuration.

Les fichiers de configuration déterminent la possibilité de charger l'ordinateur depuis un support amovible (par exemple, CD/DVD ou périphérique USB avec Kaspersky Rescue Disk) créé à l'aide de l'Assistant.

Lors de la mise à jour des bases de l'application, les bases obtenues suite à la mise à jour la plus récente de Kaspersky PURE sont utilisées. Si les bases sont dépassées, il est conseillé de réaliser une mise à jour, de relancer l'Assistant de création et d'enregistrement de Kaspersky Rescue Disk.

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 du disque sur un support

Cette étape de l'Assistant vous informera que la création de l'image du disque a réussi et proposera d'enregistrer l'image du disque sur un support.

Désignez le support d'enregistrement de Kaspersky Rescue Disk :

- Pour enregistrer sur un CD/DVD, sélectionnez l'option **Enregistrer sur un disque CD/DVD** et indiquez le disque sur lequel vous souhaitez enregistrer l'image du disque.

- Pour enregistrer sur un périphérique USB, sélectionnez l'option **Enregistrer sur un périphérique USB** et indiquez le périphérique sur lequel enregistrer l'image du disque.

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 smartphone, un téléphone mobile, un ordinateur de poche ou un lecteur MP3. L'enregistrement de l'image de disque sur de tels périphériques pourrait nuire au fonctionnement ultérieur de ceux-ci.

- Pour enregistrer sur le disque dur de votre ordinateur ou sur un autre ordinateur auquel vous avez accès via le réseau, sélectionnez l'option **Enregistrer l'image dans le fichier sur le disque local ou réseau** et indiquez le dossier dans lequel enregistrer l'image du disque, et le nom du fichier au format ISO.

### Etape 6. Fin de l'Assistant

Pour quitter l'Assistant, cliquez sur **Terminer**. Vous pouvez utiliser le disque de dépannage créé pour démarrer l'ordinateur (cf. page 75), si, suite aux actions des virus et des programmes malveillants, il n'est pas possible de démarrer l'ordinateur et de lancer Kaspersky PURE en mode normal.

## 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 périphérique USB contenant le programme Kaspersky Rescue Disk (cf. section "Création d'un disque de dépannage" à la page 73).

Le lancement de l'ordinateur depuis un support amovible n'est pas toujours possible. C'est le cas par exemple s'il s'agit d'un ancien modèle d'ordinateur. Avant d'éteindre l'ordinateur en vue de le redémarrer depuis un support amovible, vérifiez si cette option est prise en charge par l'ordinateur.

*Pour démarrer l'ordinateur à l'aide du disque de dépannage, procédez comme suit :*

1. Dans les paramètres BIOS, activez le chargement depuis un CD/DVD ou depuis un périphérique USB (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 périphérique USB contenant l'application Kaspersky Rescue Disk.
3. Redémarrez l'ordinateur.

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

# CONTACTER LE SUPPORT TECHNIQUE

Cette section reprend les informations sur les différentes méthodes d'obtention du Support Technique et les conditions à remplir pour pouvoir bénéficier de l'aide du Support Technique.

### DANS CETTE SECTION



## MODES D'OBTENTION DE L'ASSISTANCE TECHNIQUE

Si vous ne trouvez pas la solution à votre problème dans la documentation de l'application ou dans une des sources d'informations relatives à l'application (cf. section "Sources d'information sur l'application "à la page 9), nous vous conseillons de contacter le Support Technique de Kaspersky Lab. Les experts du Support Technique répondront à vos questions sur l'installation et l'utilisation de l'application.

Avant de contacter le Support Technique, veuillez lire les règles d'obtention de l'assistance technique (http://support.kaspersky.com/fr/support/rules).

Vous pouvez contacter les experts du Support Technique d'une des manières suivantes :

- Via téléphone. Vous pouvez contacter les experts du Support Technique en France.
- En envoyant une demande depuis Mon Espace Personnel sur le site Internet du Support Technique. Cette méthode permet de contacter les experts du Support Technique via un formulaire.

Le Support technique est uniquement accessible aux utilisateurs qui ont acheté une licence commerciale pour l'application. Les détenteurs de licences d'évaluation n'ont pas droit au Support technique.

## SUPPORT TECHNIQUE PAR TELEPHONE

Si vous êtes confronté à un problème que vous ne parvenez pas à résoudre, vous pouvez contacter les experts francophones du Support Technique (http://support.kaspersky.com/fr/support/international).

Avant de contacter le service du Support Technique, veuillez prendre connaissances des Règles d'octroi du Support Technique (http://support.kaspersky.com/support/details). Ceci permettra nos experts à vous venir en aide le plus vite possible.

# OBTENTION DE L'ASSISTANCE TECHNIQUE VIA MON ESPACE PERSONNEL

*Mon Espace Personnel* est un espace qui vous est réservé (https://my.kaspersky.com/fr) sur le site du Support Technique.

Pour pouvoir accéder à Mon Espace Personnel, vous devez vous inscrire sur la page d'enregistrement (https://my.kaspersky.com/fr/registration). Vous devrez saisir votre adresse de messagerie et un mot de passe d'accès à Mon Espace Personnel.

Mon Espace Personnel permet de réaliser les opérations suivantes :

- envoyer des demandes au Support Technique et au Laboratoire d'étude des virus ;
- Communiquer avec le Support 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.
- Obtenir une copie du fichier clé en cas de perte ou de suppression de celui-ci.

### Demande adressée par email au Support Technique

Vous pouvez envoyer une demande par email au Support Technique en anglais et en français.

Vous devez fournir les informations suivantes dans les champs du formulaire :

- type de demande ;
- nom et numéro de version de l'application ;
- texte de la demande ;
- numéro de client et mot de passe ;
- adresse de messagerie.

L'expert du Support Technique répond via Mon Espace Personnel et en envoyant un message électronique à l'adresse indiquée dans la demande.

### Demande électronique adressée au Laboratoire d'étude des virus

Certaines demandes ne sont pas envoyées au Support Technique mais au Laboratoire d'étude des virus.

Vous pouvez envoyer les types de demandes suivantes au Laboratoire d'étude des virus :

- *Programme malveillant inconnu* : vous soupçonnez le fichier de contenir un virus mais Kaspersky PURE ne détecte aucune infection.

  Les experts du Laboratoire d'étude des virus analysent le code malveillant envoyé et en cas de découverte d'un virus inconnu jusque-là, ils ajoutent sa définition à la base des données accessible lors de la mise à jour des logiciels antivirus.

- *Faux positif du logiciel antivirus* : Kaspersky PURE 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 découvert par Kaspersky PURE sur la base du nom de ce virus.

Vous pouvez également envoyer une demande au laboratoire d'étude des virus depuis le formulaire de demande (http://support.kaspersky.ru/virlab/helpdesk.html?LANG=fr) sans vous enregistrer dans Mon Espace Personnel. Dans ce cas, vous ne devez pas indiquer le code d'activation de l'application.

# CREATION D'UN RAPPORT SUR L'ETAT DU SYSTEME ET UTILISATION DU SCRIPT AVZ

Une fois le problème signalé aux experts du Support Technique, ces derniers peuvent vous demander de composer un rapport reprenant les informations relatives au système d'exploitation et de l'envoyer au Support Technique. Les experts du Service de Support Technique peuvent également vous demander de créer un fichier contenant des informations techniques sur le fonctionnement du système. Ce fichier permet de suivre le processus d'exécution des instructions de l'application pas à pas et de découvrir à quel moment l'erreur survient.

L'analyse des données que vous envoyez permet aux experts du Support Technique de créer et de vous envoyer un script AVZ. L'exécution de scripts AVZ permet d'analyser les processus exécutés et de rechercher la présence d'un code malveillant, d'un code malveillant dans le système, de réparer ou de supprimer les fichiers infectés ou de composer des rapports sur les résultats de l'analyse du système.

### DANS CETTE SECTION



## CREATION D'UN RAPPORT SUR L'ETAT DU SYSTEME

*Pour créer un rapport sur l'état du système, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Cliquez sur le lien **Support Technique** situé dans la partie inférieure de la fenêtre principale afin d'ouvrir la fenêtre **Support Technique**.

   Cliquez sur le bouton **Outils de support**.
3. Dans la fenêtre **Outils de support** qui s'ouvre, cliquez sur le bouton **Créer un rapport sur le 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.
2. Cliquez sur le lien **Support Technique** situé dans la partie inférieure de la fenêtre principale afin d'ouvrir la fenêtre **Support Technique**.

   Cliquez sur le bouton **Outils de support**.
3. Dans la fenêtre **Outils de support** qui s'ouvre, cliquez sur le bouton **Consulter le rapport**.
4. Ouvrez l'archive sysinfo.zip contenant le fichier du rapport.

## COLLECTE D'INFORMATIONS TECHNIQUES SUR LE FONCTIONNEMENT DE L'APPLICATION

L'enregistrement des événements permet de collecter des informations techniques sur le fonctionnement de l'application et le système d'exploitation. Le rapport sur les événements enregistrés permet aux experts du Service de Support Technique d'analyser le problème survenu pendant l'utilisation de l'application.

*Afin de collecter et d'enregistrer les informations relatives au fonctionnement de l'application, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Cliquez sur le lien **Support Technique** situé dans la partie inférieure de la fenêtre principale afin d'ouvrir la fenêtre **Support Technique**.
3. Dans la fenêtre **Support Technique**, cliquez sur le bouton **Outils de support**.
4. Dans la liste déroulante **Enregistrer les événements** de la section **Outils de support**, sélectionnez le niveau d'importance des événements.

   Vous avez le choix entre les options suivantes pour le niveau d'importance des événements enregistrés dans le rapport :

   - Importants. Kaspersky PURE conserve dans le rapport les informations sur les événements potentiellement importants pour assurer la protection de l'ordinateur (par exemple : détection d'un objet potentiellement infecté ou d'une activité suspecte dans le système).
   - Recommandés. Kaspersky PURE conserve dans le rapport les informations sur les événements importants et sur les événements qui ne sont pas d'importance primordiale pour assurer la protection de l'ordinateur.
   - Tous. Kaspersky PURE compose le rapport détaillé sur tous les événements qui peuvent être utilisés pour diagnostiquer le fonctionnement de l'application.
5. Afin de lancer l'enregistrement des événements, cliquez sur le bouton **Activer l'enregistrement**.
6. Fermez la fenêtre **Support technique**, puis reproduisez la situation dans laquelle le problème survient.
7. Une fois que vous avez reproduit la situation, revenez à la section **Outils de support** dans la fenêtre **Support technique** puis cliquez sur le bouton **Désactiver l'enregistrement**.

   Kaspersky PURE arrête d'enregistrer les informations techniques sur le fonctionnement de l'application et l'ensemble du système d'exploitation.

Une fois les informations de service sur le fonctionnement de l'application recueillies, vous pouvez les envoyer au Service de Support Technique de Kaspersky Lab.

## ENVOI DES FICHIERS DE DONNEES

Une fois que la collecte de données techniques sur le fonctionnement de l'application est terminée et que le rapport sur l'état du système a été créé, il faut les envoyer aux experts du Support Technique de Kaspersky Lab.

Pour charger les fichiers de données sur le serveur du Support Technique, il faut obtenir un numéro de requête. Ce numéro est accessible dans Mon Espace Personnel sur le site Internet du Support Technique lorsque des requêtes actives sont présentes.

*Pour télécharger les fichiers de données sur le serveur du Support Technique, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Cliquez sur le lien **Support Technique** situé dans la partie inférieure de la fenêtre afin d'ouvrir la fenêtre **Support Technique**.
3. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Surveillance des problèmes**.

   La fenêtre **Surveillance des problèmes** s'ouvre.
4. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Envoyer les informations de service au Support Technique**.

   La fenêtre **Envoi du rapport** s'ouvre.
5. Cochez les cases en regard des données que vous souhaitez envoyer au Support Technique, puis cliquez sur **Envoyer**.

   La fenêtre **Saisissez le numéro de requête** s'ouvre.
6. Indiquez le numéro attribué à votre demande lors de la prise de contact avec le Support 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 Support 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.
2. Cliquez sur le lien **Support Technique** situé dans la partie inférieure de la fenêtre afin d'ouvrir la fenêtre **Support Technique**.
3. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Surveillance des problèmes**.
4. La fenêtre **Surveillance des problèmes** s'ouvre.
5. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Envoyer les informations de service au Service du Support technique**.

   La fenêtre **Envoi du rapport** s'ouvre.
6. Cochez les cases en regard des données que vous souhaitez envoyer au Support Technique, puis cliquez sur **Envoyer**.

   La fenêtre **Saisissez le numéro de requête** s'ouvre.
7. 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.
8. Saisissez le nom de l'archive et confirmez l'enregistrement.

Vous pouvez envoyer l'archive créée au Support Technique via Mon Espace Personnel.

# EXECUTION DU SCRIPT AVZ

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 (cf. section "Modes d'obtention de l'assistance technique" à la page 76).

*Pour exécuter le script AVZ, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Cliquez sur le lien **Support Technique** situé dans la partie inférieure de la fenêtre afin d'ouvrir la fenêtre **Support Technique**.
3. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Surveillance des problèmes**.

   La fenêtre **Surveillance des problèmes** s'ouvre.
4. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Exécuter le script**.

   La fenêtre **Exécution du script AVZ** s'ouvre.
5. Copiez le texte du script, reçu des experts du Support Technique, insérez-le dans le champ de saisie dans la fenêtre qui s'ouvre et cliquez sur le bouton **Suivant**.

   L'exécution du script sera lancée.

Si l'exécution du script réussit, l'Assistant termine. Si une erreur se produit durant l'exécution du script, l'Assistant affiche le message correspondant.

# GLOSSAIRE

## A

### Activation de l'application

L'application devient entièrement fonctionnelle. L'utilisateur effectue l'activation pendant ou après l'installation de l'application. Pour pouvoir activer l'application, l'utilisateur doit disposer d'un code d'activation.

### Analyse du trafic

Analyse en temps réel des objets transitant par tous les protocoles (exemple : HTTP, FTP et autres), à l'aide de la dernière version des bases.

### Analyseur heuristique

Technologie de détection des menaces dont les définitions ne figurent pas encore dans les bases de Kaspersky Lab. L'analyseur heuristique permet de détecter les objets dont le comportement dans le système peut représenter une menace pour la sécurité. Les objets identifiés à l'aide de l'analyseur heuristique sont considérés comme potentiellement infectés. Ainsi, un objet potentiellement infecté peut être un objet qui contient une séquence d'instructions caractéristiques des programmes malveillants (ouverture d'un fichier, écriture dans un fichier).

### Application incompatible

Application antivirus d'un autre éditeur ou application de Kaspersky Lab qui ne peut être administrée via Kaspersky PURE.

### 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 malveillantes

Liste des d'adresses des sites Internet 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

Bases de données contenant les informations relatives aux menaces informatiques connues de Kaspersky Lab au moment de la publication des bases. Les entrées des bases permettent de détecter le code malveillant dans les objets analysés. Ces bases sont créées par les experts de Kaspersky Lab et mises à jour toutes les heures.

### Blocage d'un objet

Interdiction de l'accès à l'objet pour les applications tiers. L'objet bloqué ne peut être lu, exécuté, modifié ou supprimé.

## C

### Centre de protection

Module de l'application qui assure la protection complexe de l'ordinateur contre différentes menaces. Le Centre de protection protège l'ordinateur contre les virus et contre le courrier indésirable et les attaques de réseau. Ce module contient les modules Mise à jour, Surveillance du système et Quarantaine.

### COFFRE-FORT

Objet crypté prévu pour la conservation de données confidentielles. Le coffre-fort est un disque virtuel amovible protégé par un mot de passe sur lequel des dossiers et des fichiers sont enregistrés.

La manipulation des coffres-forts requiert l'installation de Kaspersky PURE.

### COURRIER INDESIRABLE

Envoi massif non autorisé de messages électroniques, le plus souvent à caractère publicitaire.

### COURRIER POTENTIELLEMENT INDESIRABLE

Message qui ne peut être considéré comme courrier indésirable de manière certaine mais qui possède certaines caractéristiques du courrier indésirable (par exemple, certains types d'envois et de messages publicitaires).

## D

### DEGRE D'IMPORTANCE DE L'EVENEMENT

Caractéristique de l'événement consigné dans l'application de Kaspersky Lab. Il existe 4 degrés d'importance :

- Critique.
- Erreur.
- Avertissement.
- Message d'information.

Les événements du même type peuvent avoir différents degrés de gravité, en fonction du moment où l'événement s'est produit.

### DEGRE DE MENACE

Indice de probabilité que le programme présente une menace pour le système d'exploitation. Le degré de menace est calculé à l'aide de l'analyse heuristique sur la base de deux types de critères :

- statiques (par exemple, les informations sur le fichier exécutable de l'application : la taille du fichier, la date de création, etc.) ;
- dynamiques qui sont appliqués pendant la simulation du fonctionnement de l'application dans l'environnement virtuel (l'analyse des fonctions de système appelées par l'application).

Le degré de menace permet d'identifier le comportement typique aux applications malveillantes. Plus le degré de menace est bas, plus le nombre d'actions autorisées pour l'application est élevé.

### DUREE DE VALIDITE DE LA LICENCE

Période au cours de laquelle vous pouvez utiliser les fonctions de l'application et les services complémentaires.

## E

### EN-TETE

Informations contenues dans le début du fichier ou du message et qui offrent des données de faible niveau sur l'état et le traitement du fichier (message). Ainsi, l'en-tête du courrier électronique contient des renseignements tels que les données de l'expéditeur, du destinataire et la date.

### ENREGISTREUR DE FRAPPES

Sous-module 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.

### ETAT DE PROTECTION

Etat actuel de la protection qui définit le niveau de protection de l'ordinateur.

## F

### FAUX POSITIF

Situation où un objet sain est considéré comme infecté par l'application de Kaspersky Lab car son code évoque celui d'un virus.

### FICHIER COMPACTE

Fichier d'archivage contenant un programme de décompactage ainsi que des instructions du système d'exploitation nécessaires à son exécution.

## K

### KASPERSKY SECURITY NETWORK (KSN)

L'infrastructure des services en ligne et des services offrant l'accès à la base opérationnelle de connaissance de Kaspersky Lab sur la réputation des fichiers, des ressources Internet et du logiciel. L'utilisation des données de Kaspersky Security Network assure une vitesse de réaction plus élevée des applications de Kaspersky Lab face aux menaces inconnues, augmente l'efficacité de fonctionnement de certains modules de la protection et réduit la possibilité de faux positifs.

## M

### MASQUE DE FICHIER

Représentation du nom d'un fichier par des caractères génériques. Les caractères principaux utilisés à cette fin sont * et ? (où * représente n'importe quel nombre de n'importe quel caractère et ? représente un caractère unique).

### 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.

### MISE A JOUR

Procédure de remplacement/d'ajout de nouveaux fichiers (bases ou modules de l'application), récupérés sur les serveurs de mises à jour de Kaspersky Lab.

### MISE A JOUR DES BASES

Fonction de l'application de Kaspersky Lab qui permet de maintenir la protection de l'ordinateur à jour. Pendant la mise à jour, l'application copie la mise à jour des bases et des modules de l'application depuis les serveurs de mise à jour de Kaspersky Lab sur l'ordinateur et les installe et les applique automatiquement.

### MISE A JOUR DISPONIBLE

Ensemble des mises à jour des modules de l'application de Kaspersky Lab qui reprend les mises à jour urgentes rassemblées au cours d'une période définie 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.

### MODULES DE L'APPLICATION

Fichiers qui font partie de la distribution d'une application de Kaspersky Lab et qui sont responsables de la réalisation des tâches principales. Chaque type de tâche exécutée par l'application (Protection en temps réel, Analyse à la demande, Mise à jour) a son propre module exécutable. En lançant l'analyse complète de votre ordinateur depuis la fenêtre principale, vous démarrez le module lié à cette tâche.

### MOT DE PASSE PRINCIPAL

Mot de passe unique qui intervient dans la protection de la base du Gestionnaire de mots de passe et qui permet d'accéder aux données.

## N

### NAVIGATEUR PROTEGE

Navigateur lancé en mode Protection des transactions bancaires. Le lancement du navigateur protégé s'opère quand un site de transactions bancaires en ligne est sollicité, ce qui permet à l'application de garantir la protection des données de l'utilisateur contre le vol. Dans ce cas, le navigateur normal, utilisé pour la connexion au site Internet, affiche un message de lancement du navigateur protégé.

### NIVEAU DE PROTECTION

Le niveau de protection est l'ensemble des paramètres prédéfinis de fonctionnement du module de l'application.

## O

### OBJET INFECTE

Objet dont un segment de code correspond parfaitement à un segment de code d'un programme dangereux connu. Les experts de Kaspersky Lab déconseillent l'utilisation de tels objets.

### OBJET POTENTIELLEMENT INFECTE

Objet dont le code contient un extrait modifié de code d'un programme dangereux connu ou un objet dont le comportement évoque un tel programme.

### OBJETS DE DEMARRAGE

Ensemble d'applications indispensables au lancement et au fonctionnement correct du système d'exploitation et du logiciel de votre ordinateur. Le système d'exploitation lance ces objets à chaque démarrage. Il existe des virus capables d'infecter les objets de démarrage, ce qui peut entraîner, par exemple, le blocage du lancement du système d'exploitation.

### OUTIL DE DISSIMULATION D'ACTIVITE

Programme ou ensemble de programmes qui permet de dissimuler la présence de l'individu malintentionné ou du programme malveillant dans le système.

Dans les systèmes Windows, tout programme qui s'infiltre dans le système et intercepte les fonctions système (Windows API) est considéré comme un rootkit (outil de dissimulation d'activité). L'interception et la modification de fonctions API de bas niveau permet avant tout à ce genre de programme de bien masquer sa présence dans le système. De plus, en général, un rootkit masque la présence dans le système de n'importe quel processus, dossier ou fichier sur le disque ou clé de registre décrit dans sa configuration. De nombreux rootkits installent leurs pilotes et services dans le système (ils sont aussi invisibles).

## P

### PAQUET DE MISE A JOUR

Paquet de fichiers pour la mise à jour des modules de l'application. L'application de Kaspersky Lab copie les paquets de mise à jour depuis les serveurs de mises à jour de Kaspersky Lab, puis les installe et les applique automatiquement.

### 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 quarantaine.

### PARAMETRES DE LA TACHE

Les paramètres de fonctionnement de l'application, spécifiques à chaque type de tâches.

### 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.

### PROTECTION DES TRANSACTIONS BANCAIRES

Module de l'application servant à protéger les données confidentielles saisies par l'utilisateur sur les sites Internet des banques ou des systèmes de paiement et servant à prévenir le vol d'argent lors des paiements en ligne.

### 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. Le objets sains sont ignorés par l'utilisateur, tandis que les objets infectés ou potentiellement infectés sont traités conformément aux paramètres de la tâche (réparer, supprimer, etc.).

### 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, FTP et NNTP.

### 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 tout en conservant une IPv4 relativement limitée.

## Q

### QUARANTAINE

Stockage spécial dans lequel l'application place les copies de sauvegarde des fichiers, modifiés ou supprimés lors de la réparation. Les copies des fichiers sont conservées sous un format spécial et ne représentent aucun danger pour l'ordinateur.

## R

### RESTAURATION

Déplacement d'un objet original depuis le dossier de quarantaine ou de sauvegarde vers l'emplacement où il était avant sa mise en quarantaine, sa réparation ou sa suppression ou vers un dossier spécifié par l'utilisateur.

### REPARATION D'OBJETS

Mode de traitement des objets infectés qui débouche sur la restauration complète ou partielle des données. Certains objets infectés ne peuvent pas être réparés.

### 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.

## S

### SAUVEGARDE EN LIGNE

Mode d'enregistrement des informations sur des serveurs distants, souvent répartis entre différents pays. La Sauvegarde en ligne simplifie la synchronisation des données entre les différents ordinateurs et les périphériques mobiles. L'utilisation de la Sauvegarde en ligne requiert une connexion à Internet.

### SCRIPT

Petit programme informatique ou partie indépendante d'un programme (fonction) écrit, en règle générale, pour exécuter une 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 Internet.

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 de 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 peuvent être modifiées par le serveur proxy à des fins déterminées.

### SERVEURS DE MISES A JOUR DE KASPERSKY LAB

Serveurs HTTP de Kaspersky Lab sur lesquels l'application de Kaspersky Lab récupère la mise à jour des bases et des modules de l'application.

### SERVICE DE NOMS DE DOMAINE (DNS)

Système distribué de traduction du nom d'hôte (ordinateur ou autre périphérique réseau) en adresse IP. Le DNS fonctionne dans les réseaux TCP/IP. Dans certains cas particuliers, le DNS peut enregistrer et traiter les requêtes de retour et définir le nom de l'hôte en fonction de son IP (enregistrement PTR). La résolution du nom DNS est généralement l'œuvre d'applications réseau et non pas des utilisateurs.

### SIGNATURE NUMERIQUE

Bloc de données chiffrées qui fait partie d'un document ou d'une application. La signature numérique permet d'identifier l'auteur du document ou de l'application. Afin de pouvoir créer une signature numérique, l'auteur du document ou de l'application doit posséder un certificat numérique qui confirme l'identité de l'auteur.

La signature numérique permet de vérifier la source et l'intégrité des données et offre une protection contre les faux.

### STOCKAGE DES COPIES DE SAUVEGARDE

Espace disque ou support d'informations réservé pour la création de copies de sauvegarde de fichiers lors de l'exécution de la tâche de sauvegarde.

### SUPPRESSION D'UN MESSAGE

Mode de traitement d'un message électronique considéré comme indésirable. Il se caractérise par la suppression physique du message. Ce mode doit être appliqué aux messages dont vous êtes convaincu à 100 % qu'ils appartiennent au courrier indésirable ou qu'ils contiennent un objet malveillant. Une copie du message supprimé est conservée dans la quarantaine (à condition 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 détecté par l'application (disque dur, dossier, ressource réseau). Ce mode de traitement est recommandé pour les objets dangereux dont la réparation est impossible pour une raison quelconque.

## T

### TECHNOLOGIE ICHECKER

Technologie qui permet d'accélérer l'analyse antivirus en excluant les objets qui n'ont pas été modifiés depuis l'analyse antérieure à condition que les paramètres de l'analyse (bases de l'application 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 possédiez 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 de l'application, l'archive sera analysée de nouveau.

Limitations de la technologie **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 ;
- Cette technologie prend en charge un nombre limité de formats.

### TACHE

Fonctions exécutées par l'application de Kaspersky Lab sous la forme des tâches, par exemple : Protection en temps réel des fichiers, Analyse complète de l'ordinateur, Mise à jour des bases.

## V

### VIRUS INCONNU

Nouveau virus au sujet duquel aucune information ne figure dans les bases. En général, l'application détecte les virus inconnus dans les objets à l'aide de l'analyse heuristique. Ces objets obtiennent l'état potentiellement infecté.

# KASPERSKY LAB

Kaspersky Lab est un éditeur de renommée mondiale spécialisé dans les systèmes de protection contre les menaces informatiques : virus et autres programmes malveillants, courrier indésirable, attaques réseau et attaques de pirates.

En 2008, Kaspersky Lab a fait son entrée dans le Top 4 des leaders mondiaux du marché des solutions de sécurité informatique pour les utilisateurs finaux (classement "IDC Worldwide Endpoint Security Revenue by Vendor"). Selon les résultats d'une étude réalisée par KomKon TGI-Russia 2009, Kaspersky Lab est l'éditeur de système de protection préféré des utilisateurs particuliers en Russie.

Kaspersky Lab a vu le jour en Russie en 1997. Aujourd'hui, Kaspersky Lab est devenu un groupe international de sociétés dont le siège principal est basé à Moscou. La société compte cinq filiales régionales qui gèrent les activités de la société en Russie, en Europe de l'Ouest et de l'Est, au Moyen Orient, en Afrique, en Amérique du Nord et du Sud, au Japon, en Chine et dans d'autres pays de la région Asie-Pacifique. La société emploie plus de 2 000 experts qualifiés.

**Produits**. Les produits développés par Kaspersky Lab protègent aussi bien les ordinateurs des particuliers que les ordinateurs des réseaux d'entreprise.

La gamme de logiciels pour particuliers reprend des logiciels antivirus pour ordinateurs de bureau et ordinateurs portables ainsi que des applications pour la protection des ordinateurs de poche, des smartphones et d'autres appareils nomades.

La société propose des applications et des services pour la protection des postes de travail, des serveurs de fichiers et Internet, des passerelles de messagerie et des pare-feu. L'utilisation de ces solutions combinée à des outils d'administration centralisés permet de mettre en place et d'exploiter une protection efficace automatisée de l'organisation contre les menaces informatiques. Les logiciels de Kaspersky Lab ont obtenu les certificats des plus grands laboratoires d'essai. Ils sont compatibles avec les applications de nombreux éditeurs et sont optimisés pour de nombreuses plateformes matérielles.

Les experts de la lutte antivirus de Kaspersky Lab travaillent 24h/24. Chaque jour, ils trouvent des centaines de nouvelles menaces informatiques, développent les outils d'identification et de neutralisation de ces menaces et les ajoutent aux bases utilisées par les applications de Kaspersky Lab. *Les bases antivirus de Kaspersky Lab sont actualisées toutes les heures*, tandis que *les bases antispam* sont actualisées *toutes les 5 minutes*.

**Technologies**. Kaspersky Lab est à l'origine de nombreuses technologies sans lesquelles il est impossible d'imaginer un logiciel antivirus moderne. Ce n'est donc pas un hasard si le moteur logiciel de Kaspersky Anti-Virus est intégré aux logiciels de plusieurs autres éditeurs : citons notamment SafeNet (É-U), Alt-N Technologies (É-U), Blue Coat Systems (É-U), Check Point Software Technologies (Israël), Clearswift (R-U), CommuniGate Systems (É-U), Critical Path (Irlande), D-Link (Taïwan), M86 Security (É-U), GFI (Malte), IBM (É-U), Juniper Networks (É-U), LANDesk (É-U), Microsoft (É-U), NETASQ (France), NETGEAR (É-U), Parallels (Russie), SonicWALL (USA), WatchGuard Technologies (É-U), ZyXEL Communications (Taïwan). De nombreuses technologies novatrices développées par la société sont brevetées.

**Réalisations**. Au cours de ces années de lutte contre les menaces informatiques, Kaspersky Lab a décroché des centaines de récompenses. Ainsi, en 2010, Kaspersky Anti-Virus a obtenu plusieurs hautes distinctions Advanced+ à l'issue de tests réalisés par le célèbre laboratoire antivirus autrichien AV-Comparatives. Mais la récompense la plus importante de Kaspersky Lab, c'est la fidélité de ses utilisateurs à travers le monde. Les produits et les technologies de la société protègent plus de 300 millions d'utilisateurs. Elle compte également plus de 200 000 entreprises parmi ses clients.

| | |
|---|---|
| Site de Kaspersky Lab : | http://www.kaspersky.com/fr |
| Encyclopédie Virus : | http://www.securelist.com/fr/ |
| Laboratoire d'étude des virus : | newvirus@kaspersky.com (uniquement pour l'envoi d'objets suspects sous forme d'archive) |
| | http://support.kaspersky.ru/virlab/helpdesk.html?LANG=fr |
| | (pour les questions posées aux experts de la lutte contre les virus) |
| Forum de Kaspersky Lab : | http://forum.kaspersky.fr |

# INFORMATIONS SUR LE CODE TIERS

Les informations sur le code tiers sont reprises dans le fichier legal_notices.txt situé dans le dossier d'installation de l'application.

# NOTICE SUR LES MARQUES DE COMMERCE

Les autres noms et marques déposés appartiennent à leurs propriétaires respectifs.

Google Chrome est une marque de Google, Inc.

Intel, Pentium et Atom sont des marques déposées de Intel Corporation aux États-Unis et dans d'autres pays.

Microsoft, Windows, Windows Vista et Internet Explorer sont des marques déposées de Microsoft Corporation aux Etats-Unis et/ou dans d'autres pays.

Mozilla et Firefox sont des marques de Mozilla Foundation.

# INDEX

## L



## M



## O



## P



## Q



## R



## S



## T