Kaspersky Small Office Security

Manuel de l'utilisateur

VERSION DE L'APPLICATION : 4.0

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.

Attention ! Ce document demeure la propriété de Kaspersky Lab ZAO (ci-après, Kaspersky Lab) et il est protégé par les législations de la Fédération de Russie et les accords internationaux sur les droits d'auteur. Toute copie ou diffusion illicite de ce document, intégrale ou partielle, est passible de poursuites civiles, administratives ou judiciaires, conformément aux lois applicables.

La copie sous un format quelconque et la diffusion, y compris la traduction, de n'importe quel document ne sont admises que par autorisation écrite de Kaspersky Lab.

Ce document et les illustrations qui l'accompagnent peuvent être utilisés uniquement à des fins personnelles, non commerciales et à titre d'information.

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.

Kaspersky Lab ne peut être tenu responsable du contenu, de la qualité, de l'actualité et de l'exactitude des textes utilisés dans ce manuel et dont les droits appartiennent à d'autres entités. Kaspersky Lab n'assume pas non plus de responsabilité en cas de dommages liés à l'utilisation de ces textes.

Date d'édition : 01/12/2014

© 2014 Kaspersky Lab ZAO. Tous droits réservés.

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

TABLE DES MATIERES

PRESENTATION DU GUIDE

Ce document est le guide de l'utilisateur de Kaspersky Small Office Security 4 (ci-après Kaspersky Small Office Security).

Pour tirer le meilleur parti de l'utilisation de Kaspersky Small Office Security, l'utilisateur doit connaître l'interface du système d'exploitation utilisé, maîtriser ses principaux procédés et savoir utiliser le courrier électronique et Internet.

Ce guide poursuit les objectifs suivants :

- Aider à installer Kaspersky Small Office Security, à activer l'application et à l'utiliser.
- Offrir un accès rapide aux informations pour répondre aux questions liées à l'utilisation de Kaspersky Small Office Security.
- Présenter des sources d'informations complémentaires sur l'application et les modes d'obtention de l'assistance technique.

DANS CETTE SECTION

DANS CE DOCUMENT

Ce document contient les sections suivantes.

Sources d'informations sur l'application (à la page 12)

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 Small Office Security (à la page 14)

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. Cette section fournit des informations sur la configuration matérielle et logicielle requise pour l'installation de l'application.

Installation et suppression de l'application (à la page 23)

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

Licence de l'application (à la page 32)

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

Utilisation des notifications de l'application (à la page 37)

Cette section contient des informations sur l'utilisation des notifications de l'application.

Analyse de l'état de protection de l'ordinateur et suppression des problèmes de sécurité (à la page 38)

Cette section contient des informations sur la manière de vérifier l'état de protection de l'ordinateur et d'éliminer les problèmes de sécurité.

Mise à jour de ma protection (à la page 39)

Cette section contient les instructions, étape par étape, sur la mise à jour des bases et des modules d'application.

Analyse de l'ordinateur (à la page 40)

Cette section contient les instructions, étape par étape, sur l'analyse de l'ordinateur à la recherche des virus, programmes malveillants et vulnérabilités.

Restauration de l'objet réparé ou supprimé par l'application (à la page 43)

Cette section contient les instructions, étape par étape, comment restaurer l'objet réparé ou supprimé.

Restauration du système d'exploitation après l'infection (à la page 44)

Cette section contient les informations sur la restauration du système d'exploitation après une infection par des virus.

Protection du courrier électronique (à la page 46)

Cette section contient les informations sur la protection du courrier électronique contre le courrier indésirable, les virus et d'autres applications présentant une menace.

Protection des données personnelles dans Internet (à la page 48)

Cette section contient des informations sur la sécurité de l'utilisation d'Internet et sur la protection de vos données contre le vol.

Protection contre les bannières lors des visites des sites Internet (à la page 61)

Cette section contient les informations sur le blocage des bannières sur les sites Internet à l'aide de Kaspersky Small Office Security.

Elimination des traces d'utilisation de l'ordinateur et d'Internet (à la page 63)

Cette section contient les informations sur la suppression des traces d'activité de l'utilisateur depuis l'ordinateur.

Contrôle d'utilisation de l'application sur l'ordinateur et dans Internet (à la page 65)

Cette section contient les informations sur le contrôle des actions des utilisateurs sur l'ordinateur et sur Internet à l'aide de Kaspersky Small Office Security.

Administration à distance de la protection de l'ordinateur (à la page 72)

Cette section contient les informations sur l'administration à distance de la protection de votre ordinateur via le portail Centre d'administration de Kaspersky Small Office Security.

Utilisation des programmes inconnus (à la page 74)

Cette section contient les informations sur la prévention des actions interdites des programmes sur l'ordinateur.

Suppression des données sans la possibilité de les restaurer (à la page 80)

Cette section contient les informations sur la suppression des données à l'aide de Kaspersky Small Office Security pour empêcher des individus malintentionnés de les restaurer.

Suppression des données non utilisées (à la page 82)

Cette section contient les informations sur la suppression des fichiers temporaires et non utilisés.

Sauvegarde des données (à la page 84)

Cette section contient les informations sur l'exécution de la sauvegarde des données à l'aide de Kaspersky Small Office Security.

Conservation des données dans les coffres-forts (à la page 90)

Cette section contient les informations sur la protection des fichiers et des dossiers sur votre ordinateur à l'aide des coffres-forts.

Protection de l'accès à l'administration de Kaspersky Small Office Security par mot de passe (à la page 92)

Cette section contient les instructions sur la protection des paramètres de l'application à l'aide d'un mot de passe.

Suspension et restauration de la protection de l'ordinateur (à la page 93)

Cette section explique, étape par étape, comment activer et désactiver l'application.

Restauration des paramètres standards d'utilisation de l'application (à la page 94)

Cette section contient les instructions sur la manière de restaurer les paramètres standard de fonctionnement de l'application.

Consultation du rapport sur l'utilisation de l'application (à la page 96)

Cette section contient les instructions pour consulter les rapports de fonctionnement de l'application.

Application des paramètres de l'application sur un autre ordinateur (à la page 97)

Cette section contient les informations sur la manière d'exporter les paramètres de l'application et de les appliquer sur un autre ordinateur.

Participation à Kaspersky Security Network (à la page 98)

Cette section contient les informations sur Kaspersky Security Network et expliquer comment participer au programme KSN.

Utilisation de l'application depuis la ligne de commande (à la page 100)

Cette section contient les informations sur l'administration de l'application à l'aide de la ligne de commande.

Contacter le Support Technique de Kaspersky Lab (à la page 101)

Cette section contient des informations sur les méthodes de contact du Support Technique de Kaspersky Lab.

Restrictions et avertissements (à la page 108)

Cette section contient les informations sur les restrictions non critiques pour le fonctionnement de l'application.

Glossaire (à la page 111)

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

Kaspersky Lab" (à la page 117)

Cette section contient des informations sur Kaspersky Lab ZAO.

Informations sur le code tiers (à la page 118)

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 d'éléments de sens sur lesquels nous attirons votre attention : avertissements, conseils, exemples.

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

Tableau 1. Conventions

EXEMPLE DE TEXTE	DESCRIPTION DE LA CONVENTION
N'oubliez pas que...	Les avertissements apparaissent en rouge et sont encadrés. Les avertissements contiennent les informations sur les actions potentiellement indésirables qui peuvent amener à la perte d'informations ou à la perturbation du fonctionnement du matériel ou du système d'exploitation.
Il est conseillé d'utiliser...	Les remarques sont encadrées. 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 : ...	Les exemples sont présentés sur un fond jaune sous le titre "Exemple".

EXEMPLE DE TEXTE	DESCRIPTION DE LA CONVENTION
La *mise à jour*, c'est ... L'événement *Bases dépassées* survient.	Les éléments de sens suivants sont en italique : • nouveaux termes ; • noms des états et des événements de l'application.
Appuyez sur la touche **ENTER**. Appuyez sur la combinaison de touches **ALT+F4**.	Les noms des touches du clavier sont en caractères mi-gras et en lettres majuscules. Deux noms de touche unis par le caractère "+" représentent une combinaison de touches. 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 planifier une tâche, procédez comme suit :*	Les phrases d'introduction des instructions sont en italique et possèdent l'icône "flèche".
Dans la ligne de commande, saisissez le texte `help` Les informations suivantes s'affichent : `Indiquez la date au format JJ:MM:AA.`	Les types de texte suivants apparaissent dans un style spécial : • texte de la ligne de commande ; • texte des messages affichés sur l'écran par l'application ; • 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 chevrons sont omis.

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 101).

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 spécifique pour chaque application.

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

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

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

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

La Base de connaissance permet de trouver les articles qui contiennent des informations utiles, des recommandations et des réponses aux questions fréquemment posées sur l'achat, l'installation et l'utilisation de l'application sur le serveur de fichier (http://support.kaspersky.com/fr/ksos4fs) et sur l'ordinateur personnel (http://support.kaspersky.com/fr/ksos4pc).

Les articles peuvent répondre à des questions en rapport non seulement avec Kaspersky Small Office Security, mais également avec d'autres applications de Kaspersky Lab. De plus, ils peuvent présenter les actualités du Support Technique.

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 principales tâches pour l'utilisateur.

Documentation

Le manuel de l'utilisateur contient les informations sur l'installation, sur l'activation, sur la configuration des paramètres, ainsi que les informations pour utiliser l'application. Le document décrit l'interface graphique et décrit l'exécution des tâches les plus fréquentes impliquées dans l'utilisation de l'application.

DISCUSSION SUR LES LOGICIELS DE KASPERSKY LAB DANS 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.

KASPERSKY SMALL OFFICE SECURITY

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. Cette section fournit des informations sur la configuration matérielle et logicielle requise pour l'installation de l'application.

DANS CETTE SECTION

NOUVEAUTES

Les fonctionnalités suivantes ont été introduites dans Kaspersky Small Office Security :

- La licence de Kaspersky Small Office Security a été améliorée :
  - La protection des périphériques sur la base Mac® OS a été ajoutée.
  - L'administration de la licence dans Internet a été ajoutée.
- L'interface graphique de l'utilisateur a été améliorée.
- La prise en charge des dernières versions des navigateurs Internet populaires a été ajoutée : maintenant, les modules de protection (par exemple, Clavier virtuel) prennent en charge les navigateurs Internet Mozilla™ Firefox™ depuis la version 25.x jusqu'à la version 34.x, Google Chrome™ depuis la version 33.x jusqu'à la version 38.x.
- La prise en charge du fonctionnement du navigateur Google Chrome pour le système d'exploitation de 64 bits a été ajoutée.
- La possibilité d'accès rapide aux tâches principales (par exemple, la tâche d'analyse, la tâche de mise à jour) a été ajoutée depuis la barre des tâches dans les systèmes d'exploitation qui prennent en charge les listes des passages.
- L'affichage du processus d'exécution des tâches, exécutées par l'application Kaspersky Small Office Security, sous forme de l'indicateur d'exécution dans la barre des tâches a été ajoutée.
- La rapidité de l'application a été augmentée et la consommation des ressources de l'ordinateur a été optimisée.
- Le temps de lancement de l'application a été réduit considérablement.
- Le processus de mise à jour de l'application a été amélioré.

- L'utilisation du module Surveillance du système a été améliorée : réalisation de la protection contre les crypteurs. Si le crypteur tente d'exécuter le chiffrement du fichier, Kaspersky Small Office Security crée automatiquement une copie de sauvegarde de ce fichier avant qu'il sera chiffré par un crypteur malveillant. Les copies de sauvegarde sont enregistrées dans le dossier système de conservation des fichiers temporaires. Si le crypteur a chiffré un fichier, Kaspersky Small Office Security le restaure automatiquement depuis la copie de sauvegarde. La fonctionnalité est soumise à des restrictions (cf. section "Restrictions et avertissements" à la page 108).

- La notification de l'utilisateur sur la connexion au réseau Wi-Fi non sécurisé a été ajoutée.

- La fonctionnalité de blocage d'accès non autorisé à la webcam a été ajoutée. Bloque l'accès au flux vidéo de la webcam.

- La fonction de protection des données du presse-papiers contre le vol et l'interception a été ajoutée.

- La possibilité d'administration à distance de la protection de vos périphériques via le portail Centre d'administration de Kaspersky Small Office Security a été ajoutée.

- La protection contre la capture d'écran non autorisée a été améliorée. Kaspersky Small Office Security protège maintenant contre la capture d'écran à l'aide de DirectX® et OpenGL.

- La fonctionnalité du Contrôle Internet a été améliorée : la liste des sites Internet pour lesquels la recherche sécurisée fonctionne a été élargie.

- La configuration des paramètres du Contrôle Internet, de la Protection bancaire, des Sauvegardes et des Coffres-forts virtuels a été simplifiée.

- Le fonctionnement du module Protection bancaire a été amélioré : l'enregistrement dans le journal des événements des événements liés à la baisse de la protection durant l'utilisation de la Protection bancaire a été ajouté. L'analyse de la connexion de confiance sécurisée avec les services de Kaspersky Lab et avec les sites Internet des banques en ligne et des systèmes de paiement à l'aide de l'analyse des certificats des ressources Internet correspondantes a été aussi ajoutée.

A PROPOS DE L'APPLICATION KASPERSKY SMALL OFFICE SECURITY

Kaspersky Small Office Security assure une protection complexe des ordinateurs personnels et des serveurs de fichiers. La protection complète inclut la protection de l'ordinateur, la protection des données des utilisateurs ainsi que l'administration à distance des fonctions de Kaspersky Small Office Security sur tous les postes du réseau. Pour exécuter les tâches liées à la protection complète, Kaspersky Small Office Security propose différents fonctions et modules de protection.

L'installation de l'application sur le serveur de fichier ne diffère pas de l'installation sur l'ordinateur personnel. Si Kaspersky Small Office Security est installé sur le serveur de fichier (par exemple, Microsoft® Windows Server® 2012), l'application a un ensemble limité des fonctions. Pour plus d'informations sur les fonctions de l'application selon la version, veuillez lire la section "Comparaison des fonctions de l'application selon le type de système d'exploitation" (à la page 18).

Protection de l'ordinateur

Les *modules de la protection* ont été développés pour protéger les ordinateurs contre les menaces connues ou non, les attaques réseau, les escroqueries, les messages non sollicités. Chaque type de menace est pris en charge par un module 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 assurée par les modules de protection, il est conseillé de réaliser une *recherche* systématique d'éventuels virus et autres programmes dangereux sur votre ordinateur. Cette opération s'impose pour exclure la possibilité de propager des programmes malveillants qui n'auraient pas été détectés par les modules de la protection en raison, par exemple, d'un niveau de protection faible ou pour toute autre raison.

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

Certaines tâches spécifiques qui requièrent une exécution épisodique (par exemple, la suppression des traces d'activité de l'utilisateur dans le système d'exploitation), sont exécutées à l'aide des *outils et assistants complémentaires*.

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 Small Office Security 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 Small Office Security intercepte toute tentative d'envoi d'une requête vers un fichier et recherche dans ce fichier la présence éventuelle de virus connus et d'autres applications présentant une menace. L'utilisation ultérieure 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. De plus, la copie du fichier sera placée en quarantaine. Si à la place du fichier supprimé vous placez un fichier infecté avec le même nom, uniquement la copie de ce dernier fichier est enregistrée dans la quarantaine. La copie du fichier précédent avec le même nom n'est pas enregistrée.

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. Ce 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.

Contrôle des Applications

Le Contrôle des Applications enregistre les actions effectuées par les applications dans le système d'exploitation et règlemente l'activité des applications sur la base des groupes dans lesquels le module a placé 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 toute activité réseau selon des règles de deux types : *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.

Surveillance du système

Le module Surveillance du système permet d'annuler les actions des programmes malveillants dans le système d'exploitation.

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 Small Office Security 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 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 bancaire

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

Saisie sécurisée des données

La protection des données saisies au clavier assure une protection des informations personnelles saisies sur les sites Internet contre les enregistreurs de frappe. Le clavier virtuel permet d'éviter l'interception des données saisies au clavier et protège les données personnelles contre l'interception par capture d'écran.

Contrôle Internet

Les fonctions du Contrôle Internet visent à protéger les employés des menaces auxquelles ils pourraient être confrontés sur l'ordinateur et sur Internet.

Le Contrôle Internet permet d'établir des restrictions souples d'accès aux ressources Internet et aux applications pour des utilisateurs différents de l'ordinateur. De plus, le Contrôle Internet permet de consulter des statistiques sur les actions des utilisateurs soumis aux contrôles.

Sauvegarde

La fonction de sauvegarde est conçue pour protéger vos données contre la perte suite aux échecs de fonctionnement du matériel. Kaspersky Small Office Security permet d'exécuter une sauvegarde programmée sur les disques amovibles et dans les stockages réseau ou en ligne. Vous pouvez copier les fichiers par catégorie et indiquer le nombre de versions conservées d'un même fichier.

Coffres-forts virtuels

Les coffres-forts virtuels sont conçus pour protéger vos données confidentielles contre tout accès non autorisé. Il est impossible d'ouvrir le coffre-fort et de consulter les données sans avoir saisi le mot de passe.

Centre d'administration

Si l'ordinateur possède l'application Kaspersky Small Office Security, l'administrateur de Kaspersky Small Office Security a un compte sur le portail My Kaspersky (http://center.kaspersky.com) et la licence de Kaspersky Small Office Security est enregistrée sur ce portail. L'administrateur peut gérer à distance la protection de l'ordinateur sur le portail Centre d'administration de Kaspersky Small Office Security.

COMPARAISON DES FONCTIONS DE L'APPLICATION SELON LE TYPE DE SYSTEME D'EXPLOITATION

Le tableau ci-dessous affiche la comparaison des fonctions de Kaspersky Small Office Security selon le type de système d'exploitation (ordinateur personnel ou serveur de fichier).

Tableau 2. Comparaison des fonctions de Kaspersky Small Office Security

FONCTIONNALITE	ORDINATEUR PERSONNEL	SERVEUR DE FICHIER
Antivirus Fichiers	oui	oui
Antivirus Courrier	oui	non
Antivirus Internet	oui	non
Antivirus IM ("Chat")	oui	non
Contrôle des Applications	oui	oui
Surveillance du système	oui	non
Pare-feu	oui	oui, désactivé par défaut
Prévention des intrusions	oui	oui, désactivée par défaut
Anti-Spam	oui	non
Anti-bannière	oui	non
Protection bancaire	oui	non
Clavier virtuel	oui	non
Protection des données saisies au clavier	oui	non
Sauvegarde	oui	oui
Coffres-forts virtuels	oui	oui
Suppression définitive des données	oui	oui
Suppression des données non utilisées	oui	oui
Protection Cloud	oui	oui
Contrôle Internet	oui	non
Centre d'administration	oui	oui
Protection d'accès à la webcam	oui	non
Protection dans le réseau Wi-Fi	oui	non
Restauration du système	oui	oui
Disque de dépannage	oui	oui
Configuration du navigateur	oui	oui
Suppression des traces d'activité	oui	oui

Les modules principaux de l'application sont accessibles dans la fenêtre principale (cf. ill. ci-après).

Illustration 1. Fenêtre principale de Kaspersky Small Office Security sur l'ordinateur personnel

Illustration 2. Fenêtre principale de Kaspersky Small Office Security sur le serveur de fichier

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 du site d'un partenaire.
- **Via les partenaires**. La société partenaire vous offre un paquet de licence qui contient le code d'activation.

Si vous achetez le produit dans une 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 ;
- manuel rapide 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 commercialisée.

Si vous achetez Kaspersky Small Office Security 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.

Si vous achetez Kaspersky Small Office Security chez nos partenaires, les partenaires vous transmettent les instructions sur l'installation de l'application et vous activez l'application à l'aide du code d'activation qui fait partie du paquet de licence.

Lors de l'achat d'une licence de Kaspersky Small Office Security, vous pouvez utiliser les applications : Kaspersky Internet Security for Mac, Kaspersky Internet Security for Android™, Kaspersky Password Manager. Pour plus d'informations sur ces applications, cf. *Manuel de l'utilisateur de Kaspersky Internet Security for Mac*, *Manuel de l'utilisateur de Kaspersky Internet Security for Android*, *Manuel de l'utilisateur de Kaspersky Password Manager*. Les applications et les manuels peuvent être téléchargés sur le site de Kaspersky Lab.

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 ;
- assistance 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 sur l'apparition de nouveaux virus ou le déclenchement d'épidémies de virus. Pour bénéficier de ce service, vous devez être abonné aux 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 LOGICIELLES ET MATERIELLES

Recommandations d'ordre général :

- Espace disponible sur le disque dur : 480 Mo.
- CD-/DVD-ROM (pour l'installation à partir d'un CD d'installation).
- Connexion à Internet (pour l'activation de l'application et la mise à jour des bases ou modules de l'application).
- Internet Explorer® 8.0 ou suivant.
- Microsoft® Windows® Installer 3.0 ou suivantes.
- Microsoft .NET Framework 4 ou suivant.
- La protection contre l'accès non autorisé à la webcam est offerte uniquement pour les modèles de webcams compatibles http://support.kaspersky.com/fr/10978.

Lors de l'installation sur l'ordinateur personnel

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 1 GHz ou supérieur ;
- 512 Mo de mémoire vive disponible.

Exigences pour les systèmes d'exploitation Microsoft Windows Vista® Home Basic (Service Pack 1 ou suivant), Microsoft Windows Vista Home Premium (Service Pack 1 ou suivant), Microsoft Windows Vista Business (Service Pack 1 ou suivant), Microsoft Windows Vista Enterprise (Service Pack 1 ou suivant), Microsoft Windows Vista Ultimate (Service Pack 1 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, Microsoft Windows 8 Enterprise, Microsoft Windows 8.1 (Windows 8.1 Update), Windows 8.1 Pro (Windows 8.1 Update), Windows 8.1 Enterprise (Windows 8.1 Update) :

- processeur 1 GHz ou supérieur ;
- 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 tablettes :

- Microsoft Tablet PC ;
- processeur Intel® Celeron® 1.66 GHz ou supérieur ;
- 1000 Mo de mémoire vive disponible.

Exigences pour les netbooks :

- processeur Intel Atom™ 1600 MHz ou supérieur ;
- 1024 Mo de mémoire vive disponible ;
- écran 10.1 pouces avec résolution 1024x600 ;
- carte graphique Intel GMA 950.

Lors de l'installation sur le serveur de fichier

L'application Kaspersky Small Office Security n'est pas prévue pour l'installation sur le serveur de fichier fonctionnant en mode Server Core.

Les exigences pour les systèmes d'exploitation Microsoft Windows Server 2012 R2 Foundation/Essentials/Standard, Microsoft Windows Server 2012 Foundation/Essentials/Standard :

- Processeur de 64 bits (x64), 1.4 GHz ou supérieur.
- 4 Go de mémoire vive disponible.

Les exigences pour le système d'exploitation Microsoft Windows Server 2008 R2 Foundation/Standard/Enterprise Service Pack 1 ou supérieur :

- Processeur de 64 bits (x64), 1.4 GHz ou processeur à deux noyaux 1.4 Ghz ou supérieur.
- 512 Mo de mémoire vive disponible.

Les exigences pour le système d'exploitation Microsoft Windows Small Business Server 2008 Standard x64 Edition Service Pack 2 ou supérieur :

- Processeur de 64 bits (x64), 2 GHz ou supérieur.
- 4 Go de mémoire vive disponible.

Les exigences pour les systèmes d'exploitation Microsoft Windows Small Business Server 2011 Essentials Service Pack 1 ou supérieur, Microsoft Windows Small Business Server 2011 Standard Service Pack 1 ou supérieur :

- Processeur de 64 bits (x64), 2 GHz ou supérieur.
- 8 Go de mémoire vive disponible.

INSTALLATION ET SUPPRESSION DE L'APPLICATION

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

DANS CETTE SECTION

PROCEDURE D'INSTALLATION STANDARD

L'installation de Kaspersky Small Office Security s'effectue de manière interactive à l'aide d'un Assistant d'installation.

L'installation sur le serveur de fichier et sur l'ordinateur personnel s'exécute depuis un paquet 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 arrêter l'Assistant à n'importe quelle étape d'installation, il faut fermer la fenêtre de l'Assistant.

Si l'application doit protéger plus d'un ordinateur (le nombre maximal d'ordinateurs protégés est défini par les conditions du Contrat de licence), la procédure d'installation sera identique sur tous les ordinateurs.

- *Pour installer Kaspersky Small Office Security sur votre ordinateur,*

  lancez le fichier du paquet d'installation (fichier avec extension exe) sur le CD d'installation.

Pour installer Kaspersky Small Office Security, vous pouvez également utiliser le paquet d'installation obtenu via Internet. De plus, l'Assistant d'installation affiche quelques étapes complémentaires d'installation pour certaines langues de localisation.

Si Kaspersky Small Office Security s'installe sur l'ordinateur personnel, les extensions pour les navigateurs Internet, assurant un fonctionnement protégé dans Internet, sont installées avec l'application.

DANS CETTE SECTION

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

Avant l'installation, l'Assistant d'installation recherche la présence d'une version de Kaspersky Small Office Security plus récente sur les serveurs de mises à jour de Kaspersky Lab.

Si l'Assistant d'installation ne détecte pas sur le serveur des mises à jour de Kaspersky Lab une version plus récente de l'application, il lancera l'installation de la version actuelle.

Si l'Assistant d'installation détecte sur les serveurs de mises à jour de Kaspersky Lab une version plus récente de Kaspersky Small Office Security, il vous proposera de la télécharger et de l'installer sur votre ordinateur. Il est conseillé d'installer une nouvelle version de l'application afin de bénéficier des nouvelles améliorations. Ces améliorations permettent de protéger votre ordinateur de manière plus efficace. Si vous refusez d'installer la nouvelle version, l'Assistant lancera l'installation de la version actuelle de l'application. Si vous acceptez d'installer la nouvelle version, l'Assistant d'installation copiera les fichiers du paquet d'installation sur votre ordinateur et lancera l'installation de la nouvelle version.

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 conclu entre vous et Kaspersky Lab et vous propose également de participer au programme Kaspersky Security Network.

ETAPE 3. CONSULTATION DU CONTRAT DE LICENCE

Cette étape de l'Assistant d'installation s'affiche pour certaines langues de localisation lors de l'installation de Kaspersky Small Office Security à partir du paquet d'installation obtenu via Internet.

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

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

Si les conditions du Contrat de licence ne sont pas acceptées, l'installation de l'application n'a pas lieu.

ETAPE 4. RÈGLEMENT 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, ZAO d'informations sur les nouvelles menaces détectées sur l'ordinateur, sur les applications exécutées, sur les applications signées et les informations relatives au système d'exploitation. Vos données personnelles ne sont ni recueillies, ni traitées, ni enregistrées.

Lisez le Règlement de Kaspersky Security Network. Si vous êtes d'accord avec tous les points, cliquez sur le bouton **Accepter** dans la fenêtre de l'Assistant.

Si vous ne voulez pas participer à Kaspersky Security Network, cliquez sur le bouton **Refuser**.

Après avoir accepté ou refusé la participation à Kaspersky Security Network, l'installation de l'application se poursuivra.

ETAPE 5. INSTALLATION

Pour certaines versions de Kaspersky Small Office Security diffusées par abonnement, il faut saisir le mot de passe fourni par le prestataire de services avant l'installation.

Après la saisie du mot de passe, l'installation de l'application commence.

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 Small Office Security effectue une série de vérifications. Après ces analyses, les problèmes suivants peuvent être détectés :

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

  - correspondance du système d'exploitation et des paquets des mises à jour (Service Pack) 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, une notification apparaîtra.

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

- *Présence de programmes malveillants sur l'ordinateur*. En cas de détection de programmes malveillants 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 acceptez d'installer l'utilitaire, l'Assistant le téléchargera sur les serveurs de Kaspersky Lab. Ensuite, l'installation de l'utilitaire sera lancée 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 étape de l'Assistant vous signale la fin de l'installation de l'application. Pour commencer à utiliser Kaspersky Small Office Security immédiatement, assurez-vous que la case **Lancer Kaspersky Small Office Security** est cochée, puis cliquez sur le bouton **Terminer**.

Si vous avez décoché la case **Lancer Kaspersky Small Office Security** avant la fermeture de l'Assistant, l'application devra être lancée manuellement.

Dans certains cas, le redémarrage du système d'exploitation peut être requis pour terminer l'installation.

ETAPE 7. ACTIVATION DE L'APPLICATION

Au premier lancement de Kaspersky Small Office Security, l'Assistant d'activation de l'application se lance.

L'administration à distance de la licence et de la protection des périphériques connectés est accessible uniquement après la création d'un compte du chef de l'entreprise ou d'un compte administrateur sur le portail My Kaspersky (http://center.kaspersky.com). Après la création du compte, il faut enregistrer la licence de Kaspersky Small Office Security sur le portail My Kaspersky. Après cela, le portail peut être utilisé comme le Centre d'administration de Kaspersky Small Office Security.

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

Vous avez le choix entre les options suivantes pour activer Kaspersky Small Office Security :

- **Activer l'application**. Sélectionnez cette option et saisissez le code d'activation si vous avez acheté une licence d'utilisation de l'application.
- **Activer la version d'évaluation de l'application**. Sélectionnez cette option si vous souhaitez installer une version d'évaluation du logiciel avant de décider d'acheter une licence. Vous allez pouvoir utiliser toutes les fonctions de l'application pendant une courte période de présentation. Une fois la licence expirée, vous ne pourrez plus activer la version d'évaluation de l'application.

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

Pendant l'activation de l'application, l'enregistrement sur le portail My Kaspersky (http://center.kaspersky.com) peut être requis.

ETAPE 8. ENREGISTREMENT DE LA LICENCE

Cette étape n'est pas disponible dans toutes les versions de Kaspersky Small Office Security.

Pour administrer à distance la licence et la protection des périphériques connectés, il faut enregistrer la licence de Kaspersky Small Office Security sur le portail My Kaspersky (http://center.kaspersky.com) sous le compte du chef de l'entreprise ou sous le compte administrateur. Ce compte sera utilisé pour installer Kaspersky Small Office Security sur les ordinateurs et les périphériques mobiles des employés de l'entreprise et pour administrer à distance la protection de tous les périphériques.

Les employés de l'entreprise peuvent aussi créer des comptes sur le portail My Kaspersky (http://center.kaspersky.com) pour usage personnel.

ETAPE 9. FIN DE L'ACTIVATION

L'Assistant vous signale la réussite de l'activation de Kaspersky Small Office Security. De plus, la fenêtre reprend les informations sur la licence valide : expiration de la licence et nombre d'ordinateurs couverts par cette licence.

En cas d'abonnement, les informations sur l'état de l'abonnement sont fournies à la place de la date d'expiration de la licence.

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

INSTALLATION DE L'APPLICATION DE LA LIGNE DE COMMANDE

Vous pouvez installer Kaspersky Small Office Security à l'aide de la ligne de commande.

Syntaxe de la ligne de commande :

```
<chemin d'accès au fichier du paquet d'installation> [paramètres]
```

Les instructions détaillées et la liste des paramètres d'installation de l'application sur le serveur de fichier (http://support.kaspersky.com/fr/11635) et sur l'ordinateur personnel (http://support.kaspersky.com/fr/11636).

MISE A JOUR D'UNE VERSION ANTERIEURE DE L'APPLICATION

Installation de Kaspersky Small Office Security 4 par-dessus Kaspersky Small Office Security 3 et Kaspersky Small Office Security 2

Si votre ordinateur possède déjà l'application Kaspersky Small Office Security 3 ou Kaspersky Small Office Security 2, vous pouvez mettre à jour l'application jusqu'à Kaspersky Small Office Security 4. Si vous possédez une licence valide de Kaspersky Small Office Security 3 ou Kaspersky Small Office Security 2, il n'est pas nécessaire d'activer l'application : l'Assistant d'installation reçoit automatiquement les informations sur la licence et l'appliquera pendant l'installation de Kaspersky Small Office Security 4.

Installation de Kaspersky Small Office Security par-dessus Kaspersky Small Office Security 1

Si vous installez Kaspersky Small Office Security 4 sur l'ordinateur avec l'application Kaspersky Small Office Security 1 déjà installée, Kaspersky Small Office Security 4 propose de supprimer Kaspersky Small Office Security 1.

Après la suppression de Kaspersky Small Office Security 1, les types suivants des données ne seront pas accessibles :

- les bases de l'Anti-Spam ;
- les fichiers en quarantaine.

L'installation de Kaspersky Small Office Security s'effectue de manière interactive à l'aide d'un Assistant d'installation.

L'installation sur le serveur de fichier et sur l'ordinateur personnel s'exécute depuis un paquet 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 arrêter l'Assistant à n'importe quelle étape d'installation, il faut fermer la fenêtre de l'Assistant.

Si l'application doit protéger plus d'un ordinateur (le nombre maximal d'ordinateurs protégés est défini par les conditions du Contrat de licence), la procédure d'installation sera identique sur tous les ordinateurs.

Pour installer Kaspersky Small Office Security sur votre ordinateur,

lancez le fichier du paquet d'installation (fichier avec extension exe) sur le CD d'installation.

Pour installer Kaspersky Small Office Security, vous pouvez également utiliser le paquet d'installation obtenu via Internet. De plus, l'Assistant d'installation affiche quelques étapes complémentaires d'installation pour certaines langues de localisation.

Si Kaspersky Small Office Security s'installe sur l'ordinateur personnel, les extensions pour les navigateurs Internet, assurant un fonctionnement protégé dans Internet, sont installées avec l'application.

Kaspersky Small Office Security est incompatible avec une suite des applications de Kaspersky Lab. Vous pouvez prendre connaissance de la liste des applications incompatibles dans la section Restrictions et avertissements (à la page 108).

DANS CETTE SECTION

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

Avant l'installation, l'Assistant d'installation recherche la présence d'une version de Kaspersky Small Office Security plus récente sur les serveurs de mises à jour de Kaspersky Lab.

Si l'Assistant d'installation ne détecte pas sur le serveur des mises à jour de Kaspersky Lab une version plus récente de l'application, il lancera l'installation de la version actuelle.

Si l'Assistant d'installation détecte sur les serveurs de mises à jour de Kaspersky Lab une version plus récente de Kaspersky Small Office Security, il vous proposera de la télécharger et de l'installer sur votre ordinateur. Il est conseillé d'installer une nouvelle version de l'application afin de bénéficier des nouvelles améliorations. Ces améliorations permettent de protéger votre ordinateur de manière plus efficace. Si vous refusez d'installer la nouvelle version, l'Assistant lancera l'installation de la version actuelle de l'application. Si vous acceptez d'installer la nouvelle version, l'Assistant d'installation copiera les fichiers du paquet d'installation sur votre ordinateur et lancera l'installation de la nouvelle version.

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 conclu entre vous et Kaspersky Lab et vous propose également de participer au programme Kaspersky Security Network.

ETAPE 3. CONSULTATION DU CONTRAT DE LICENCE

Cette étape de l'Assistant d'installation s'affiche pour certaines langues de localisation lors de l'installation de Kaspersky Small Office Security à partir du paquet d'installation obtenu via Internet.

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

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

Si les conditions du Contrat de licence ne sont pas acceptées, l'installation de l'application n'a pas lieu.

ETAPE 4. RÈGLEMENT 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, ZAO d'informations sur les nouvelles menaces détectées sur l'ordinateur, sur les applications exécutées, sur les applications signées et les informations relatives au système d'exploitation. Vos données personnelles ne sont ni recueillies, ni traitées, ni enregistrées.

Lisez le Règlement de Kaspersky Security Network. Si vous êtes d'accord avec tous les points, cliquez sur le bouton **Accepter** dans la fenêtre de l'Assistant.

Si vous ne voulez pas participer à Kaspersky Security Network, cliquez sur le bouton **Refuser**.

Après avoir accepté ou refusé la participation à Kaspersky Security Network, l'installation de l'application se poursuivra.

ETAPE 5. INSTALLATION

Pour certaines versions de Kaspersky Small Office Security diffusées par abonnement, il faut saisir le mot de passe fourni par le prestataire de services avant l'installation.

Après la saisie du mot de passe, l'installation de l'application commence.

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 Small Office Security effectue une série de vérifications. Après ces analyses, les problèmes suivants peuvent être détectés :

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

  - correspondance du système d'exploitation et des paquets des mises à jour (Service Pack) 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, une notification apparaîtra.

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

- *Présence de programmes malveillants sur l'ordinateur*. En cas de détection de programmes malveillants 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 acceptez d'installer l'utilitaire, l'Assistant le téléchargera sur les serveurs de Kaspersky Lab. Ensuite, l'installation de l'utilitaire sera lancée 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 Small Office Security** est cochée, l'application sera lancée automatiquement après le redémarrage.

Si vous avez décoché la case **Lancer Kaspersky Small Office Security** avant la fermeture de l'Assistant, l'application doit être lancée manuellement.

SUPPRESSION DE L'APPLICATION

Suite à la suppression de Kaspersky Small Office Security, l'ordinateur et vos données personnelles ne seront plus protégés.

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

Pour lancer l'Assistant,

ouvrez le menu **Démarrer** et sélectionnez l'option **Toutes les applications** → **Kaspersky Small Office Security** → **Supprimer Kaspersky Small Office Security**.

DANS CETTE SECTION

ETAPE 1. SAISIE DU MOT DE PASSE POUR SUPPRIMER L'APPLICATION

Pour supprimer Kaspersky Small Office Security, vous devez saisir le mot de passe d'accès aux paramètres de l'application. Si pour quelconque raison, vous ne pouvez pas indiquer le mot de passe, la suppression de l'application ne sera pas possible.

Cette étape s'affiche uniquement si le mot de passe de suppression de l'application a été établi.

ETAPE 2. ENREGISTREMENT DE DONNEES POUR UNE REUTILISATION

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

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

Pour enregistrer les données en vue d'une utilisation ultérieure, cochez les cases en regard des données à enregistrer :

- **Informations 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.
- **Fichiers de quarantaine** : fichiers analysés par l'application et placés en quarantaine.

  Lors de la suppression de Kaspersky Small Office Security de l'ordinateur, les fichiers en quarantaine seront inaccessibles. Pour pouvoir à nouveau utiliser ces fichiers, il faut installer Kaspersky Small Office Security.

- **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.

  Vous pouvez aussi exporter les paramètres de protection à l'aide d'une ligne de commande, en utilisant la commande :

  ```
  avp.com EXPORT <nom_du_fichier>
  ```

- **Données iChecker** : fichiers contenant les informations sur les objets déjà analysés à l'aide de la technologie iChecker.
- **Bases Anti-Spam** : les bases qui contiennent les images des messages non sollicités ajoutés par l'utilisateur.
- **Coffres-forts virtuels** : les fichiers que vous avez entreposé dans les Coffres-forts virtuels.

ETAPE 3. CONFIRMATION DE LA SUPPRESSION DE L'APPLICATION

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 4. 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.

Après la suppression de Kaspersky Small Office Security, vous pouvez indiquer les causes de la suppression de l'application sur le site Internet de Kaspersky Lab. Pour ce faire, il faut accéder au site Internet de Kaspersky Lab à l'aide du bouton **Remplir le formulaire**.

Cette fonctionnalité peut être inaccessible dans certaines régions.

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 rallumé.

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 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 selon 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 Small Office Security.

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 20).

Pour utiliser l'application, vous devez acheter une licence d'utilisation de l'application.

La licence présente une durée de validité limitée. A l'expiration de la licence, l'application continue à fonctionner, mais en mode de fonctionnalité limitée (par exemple, la mise à jour et l'utilisation de Kaspersky Security Network ne sont pas disponibles). Vous pouvez toujours utiliser tous les modules de l'application et soumettre l'ordinateur à une analyse antivirus de 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 Small Office Security, la licence doit être renouvelée.

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

Avant d'acheter une licence, vous pouvez vous familiariser gratuitement avec la version d'évaluation de Kaspersky Small Office Security. La version d'évaluation de Kaspersky Small Office Security exécute ses fonctions sur une période de présentation limitée. Au terme de la période de présentation, Kaspersky Small Office Security met fin à l'exécution de ses fonctions. Pour pouvoir continuer à utiliser l'application, il faut acheter une licence.

La licence de Kaspersky Small Office Security vous permet d'utiliser les applications suivantes :

- Kaspersky Small Office Security 4 Personal Computer ;
- Kaspersky Small Office Security 4 File Server ;
- Kaspersky Internet Security for Mac ;
- Kaspersky Internet Security for Android ;
- Kaspersky Password Manager.

Vous obtenez aussi l'accès au compte spécial sur le portail My Kaspersky (http://center.kaspersky.com) pour administrer la licence de Kaspersky Small Office Security.

A PROPOS DU CODE D'ACTIVATION

Le *code d'activation* est un code que vous obtenez lors de l'achat d'une licence Kaspersky Small Office Security. 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 de l'une des manières suivantes :

- Si vous avez acheté Kaspersky Small Office Security en magasin, le code d'activation figure dans la documentation présente dans la boîte contenant le cédérom d'installation ou sur la boîte elle-même.
- Si vous avez acheté Kaspersky Small Office Security en ligne, le code d'activation est envoyé à l'adresse électronique que vous avez indiquée lors de la commande.

Le point du départ de la durée de validité de la licence commence à partir de la date d'activation de l'application ou à partir de la date de délivrance de la licence. Si vous avez acheté une licence autorisant l'utilisation de Kaspersky Small Office Security sur plusieurs appareils, le décompte de la durée de validité de la licence 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 à http://www.kaspersky.com/fr/support pour le récupérer.

A PROPOS DES DONNEES

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

- les informations sur les sommes de contrôle des fichiers traités (MD5, sha256) ;
- les informations pour définir la réputation des URL ;
- les statistiques d'utilisation des notifications de l'application ;
- les données statistiques pour la protection contre le courrier indésirable ;
- les données sur l'activation et sur la version utilisée de Kaspersky Small Office Security ;
- les informations sur la licence de la version installée de Kaspersky Small Office Security ;
- les informations sur les types de menaces détectées ;
- les informations sur les certificats numériques utilisés et les informations nécessaires pour vérifier leur authenticité ;
- les données relatives au fonctionnement de l'application et à la licence indispensables pour configurer l'affichage du contenu des sites de confiance.

Si l'ordinateur est équipé d'un module TPM (Trusted Platform Module), 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 Small Office Security, vous acceptez de fournir automatiquement à Kaspersky Lab les informations sur le code de l'erreur, sur le paquet d'installation utilisé et sur l'ordinateur.

Si vous participez à programme Kaspersky Security Network (cf. section "Participation à Kaspersky Security Network (KSN)" à la page 98), vous acceptez d'envoyer à Kaspersky Lab en mode automatique des informations suivantes obtenues lors du fonctionnement de Kaspersky Small Office Security sur l'ordinateur :

- les informations sur le logiciel et le matériel installé ;
- les informations sur l'état de la protection antivirus de l'ordinateur, ainsi que sur tous les objets potentiellement infectés et les décisions prises vis-à-vis de ces objets ;
- les informations sur les programmes téléchargés et lancés ;
- les informations sur les erreurs et sur l'utilisation de l'interface utilisateur de Kaspersky Small Office Security ;
- les informations relatives à l'application, y compris sa version, les informations relatives aux fichiers des modules d'application chargés et à la version des bases de l'application utilisées ;
- les statistiques des mises à jour et des connexions aux serveurs de Kaspersky Lab ;
- les informations relatives à l'utilisation de la connexion sans fil de l'ordinateur ;
- les statistiques des retards induits par Kaspersky Small Office Security lors du travail de l'utilisateur avec les applications installées sur l'ordinateur ;
- les fichiers qui pourraient être utilisés par des individus malintentionnés pour nuire à l'ordinateur ou à ses composants, dont les fichiers détectés après avoir cliqué sur un lien malveillant.

Les informations à transmettre à Kaspersky Lab seront conservées 30 jours maximum à partir de leur création sur l'ordinateur. Cette conservation a lieu dans un stockage interne protégé. Le volume maximal de données conservées s'élève à 30 Mo.

De plus, vous acceptez d'envoyer automatiquement à Kaspersky Lab pour analyse complémentaire les fichiers (ou leurs composants) qui risquent d'être utilisés par des individus malintentionnés pour nuire à l'ordinateur ou aux données existantes.

Kaspersky Lab protège les informations obtenues conformément aux dispositions juridiques en vigueur. 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 de données personnelles ou d'autres informations confidentielles. Les informations d'origine obtenues sont enregistrées sous forme chiffrée 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.

ACHAT D'UNE LICENCE

Si vous avez installé Kaspersky Small Office Security sans avoir acheté une licence au préalable, vous pouvez l'acheter après l'installation de l'application. A l'achat d'une licence, vous recevez le code d'activation requis pour activer l'application (cf. section "Activation de l'application" à la page 35).

Pour acheter une licence, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.

2. Cliquez sur le lien **Licence** situé dans la partie inférieure de la fenêtre principale de l'application pour ouvrir la fenêtre **Licence**.

3. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Acheter le code d'activation**.

   La page Internet de la boutique en ligne de Kaspersky Lab ou de la société partenaire où vous pourrez acheter la licence s'ouvrira.

ACTIVATION DE L'APPLICATION

L'administration à distance de la licence et de la protection des périphériques connectés est accessible uniquement après la création d'un compte du chef de l'entreprise ou d'un compte administrateur sur le portail My Kaspersky (http://center.kaspersky.com). Après la création du compte, il faut enregistrer la licence de Kaspersky Small Office Security sur le portail My Kaspersky.

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

Pour activer l'application Kaspersky Small Office Security, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.

2. Le lien **Saisir le code d'activation**, situé dans la partie inférieure de la fenêtre principale de l'application, permet d'ouvrir la fenêtre **Activation**.

3. La fenêtre **Activation** permet de saisir le code d'activation dans le champ de saisie et de cliquer sur le bouton **Activer**.

   La demande d'activation de l'application sera exécutée.

4. Saisissez les données d'enregistrement de l'utilisateur.

   Selon les conditions d'utilisation, l'application peut exiger une authentification sur le portail My Kaspersky. Si vous n'êtes pas un utilisateur enregistré, remplissez les champs du formulaire d'enregistrement pour obtenir d'autres possibilités.

Les utilisateurs enregistrés peuvent exécuter les actions suivantes :

- envoyer des demandes au Support Technique et au Laboratoire d'étude des virus ;
- gérer les codes d'activation ;
- recevoir des informations sur les nouvelles applications et sur les offres spéciales de Kaspersky Lab.

Cette étape n'est pas disponible dans toutes les versions de Kaspersky Small Office Security.

5. Cliquez sur le bouton **Terminer** dans la fenêtre **Activation** pour terminer le processus d'activation.

RENOUVELLEMENT DE LA DUREE DE VALIDITE DE LA LICENCE

Vous pouvez renouveler la licence si sa durée de validité arrive à échéance. Pour ce faire, vous pouvez indiquer un code d'activation de réserve sans attendre l'expiration de la licence. A l'issue de la période de validité de la licence, Kaspersky Small Office Security sera activé automatiquement à l'aide du code d'activation de réserve.

Pour indiquer le code d'activation de réserve pour un renouvellement automatique de la licence, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Cliquez sur le lien **Licence** situé dans la partie inférieure de la fenêtre principale de l'application pour ouvrir la fenêtre **Licence**.
3. Dans la liste déroulante dans le groupe **Code d'activation de réserve**, cliquez sur le bouton **Saisir le code d'activation**.
4. Saisissez le code d'activation dans les champs correspondants, puis cliquez sur **Ajouter**.

   Kaspersky Small Office Security enverra les données au serveur d'activation de Kaspersky Lab pour vérification.
5. Cliquez sur le bouton **Terminer**.

Le code d'activation de réserve sera affiché dans la fenêtre **Licence**.

L'application est automatiquement activée à l'aide du code d'activation de réserve à l'expiration de la licence. Vous pouvez aussi activer vous-même l'application à l'aide du code d'activation de réserve, en cliquant sur le bouton **Activer maintenant**. Le bouton est accessible si l'application n'a pas été activée automatiquement. Le bouton n'est pas accessible jusqu'à l'expiration de la licence.

Si en tant que code d'activation de réserve, vous avez indiqué un code d'activation déjà utilisé auparavant sur cet ordinateur ou sur un autre, lors du renouvellement de la licence, la date de la première activation de l'application à l'aide de ce code d'activation sera considérée comme la date d'activation de l'application.

UTILISATION DES NOTIFICATIONS DE L'APPLICATION

Les notifications de l'application qui apparaissent dans la zone de notification de la barre des tâches signalent les événements survenus pendant l'utilisation de l'application et nécessitant votre attention. En fonction de l'importance 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 : détection d'un objet malveillant ou d'une activité dangereuse dans le système d'exploitation). 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 : détection d'un objet potentiellement infecté ou d'une activité suspecte dans le système d'exploitation). Les fenêtres des notifications et des messages contextuels importants sont en jaune.

- *Informatifs* : signalent des événements qui ne sont pas essentiels pour assurer la protection de l'ordinateur. Les fenêtres des notifications et des messages contextuels informatifs 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 sélectionnée par défaut. La notification peut être fermée automatiquement lors du redémarrage de l'ordinateur, lors de la fermeture de Kaspersky Small Office Security ou en mode Connected Standby sous Windows 8. En cas de fermeture automatique de la notification, Kaspersky Small Office Security exécutera l'action recommandée par défaut.

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

L'indicateur situé dans la partie supérieure de la fenêtre principale de l'application signale les problèmes qui pourraient survenir dans la protection de l'ordinateur. La couleur verte de l'indicateur signifie que l'ordinateur est protégé, la couleur jaune signale un problème de protection, la couleur rouge indique une menace sérieuse pour la sécurité de l'ordinateur. Il est conseillé d'éliminer immédiatement les problèmes et les menaces pour la sécurité.

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

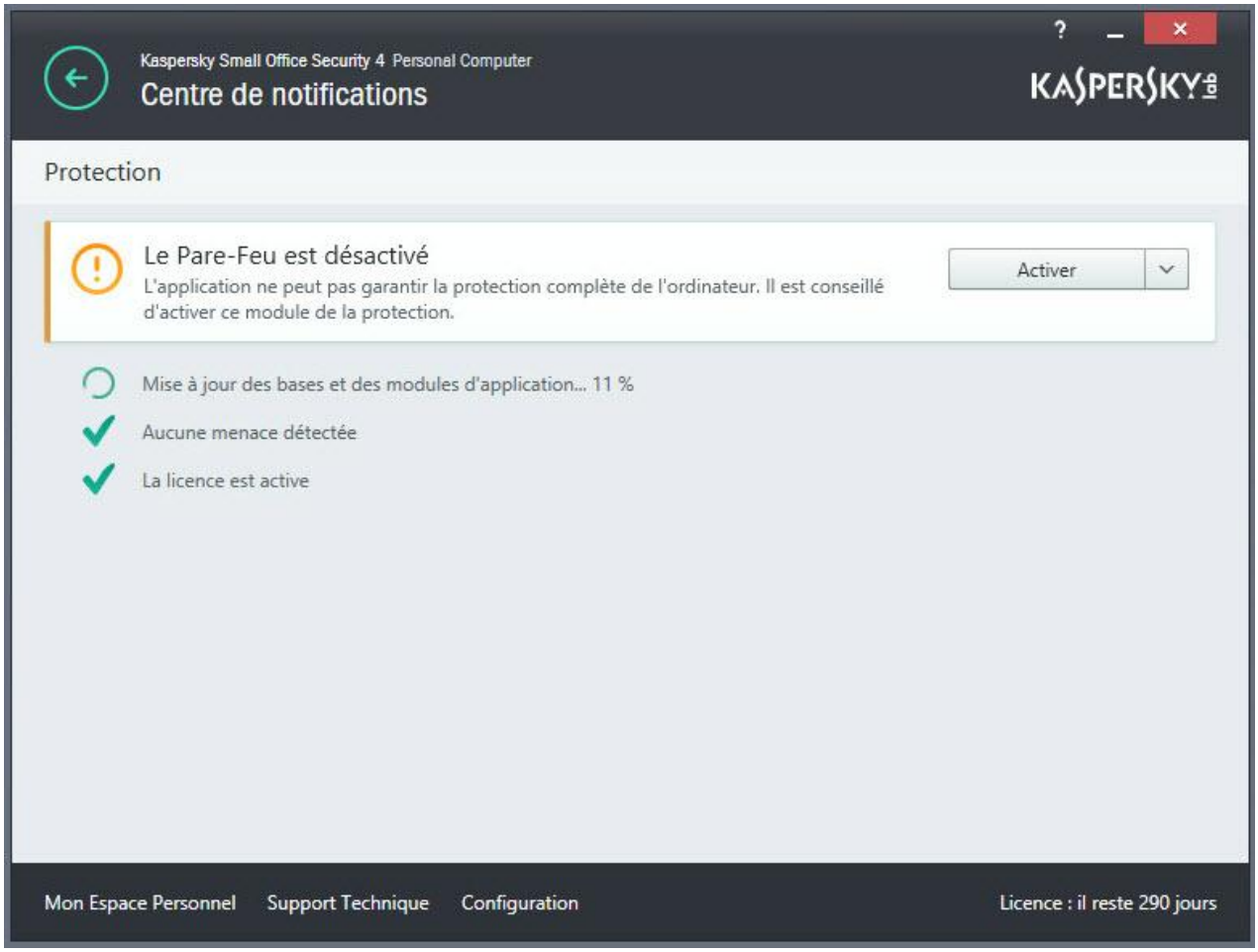


Illustration 3. Fenêtre Centre de notifications

Les problèmes de protection sont regroupés selon les catégories auxquelles ils appartiennent. Des actions que vous pouvez exécuter sont proposées pour résoudre chaque problème.

MISE A JOUR DES BASES ET DES MODULES D'APPLICATION

Kaspersky Small Office Security vérifie automatiquement la présence du paquet des mises à jour sur les serveurs de mises à jour de Kaspersky Lab. Si le serveur héberge un nouveau paquet des mises à jour, Kaspersky Small Office Security les télécharge et les installe en arrière-plan. Vous pouvez lancer la mise à jour de Kaspersky Small Office Security 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 du paquet de mises à jour depuis les serveurs de mise à jour de Kaspersky Lab requiert une connexion Internet.

En cas d'utilisation du système d'exploitation Microsoft Windows 8, le téléchargement des paquets des mises à jour ne se passe pas si la connexion à haut débit à Internet est utilisée et si une restriction du trafic avec ce type de connexion est configurée dans l'application. Pour exécuter le téléchargement du paquet des mises à jour, il faut désactiver manuellement la restriction dans la sous-section **Réseau** de la fenêtre de configuration de l'application.

- *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 et cliquez sur le bouton **Mise à jour**.

     La fenêtre **Mise à jour** s'ouvre.

  2. Dans la fenêtre **Mise à jour**, cliquez sur le bouton **Mettre à jour**.

ANALYSE DE L'ORDINATEUR

Cette section contient des informations sur l'analyse de l'ordinateur à la recherche de la présence de virus et d'autres programmes présentant une menace.

DANS CETTE SECTION

ANALYSE COMPLETE

Pendant l'analyse complète, Kaspersky Small Office Security analyse par défaut les objets suivants :

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

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

Pour lancer l'analyse complète, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Cliquez sur le bouton **Analyse**.

   La fenêtre **Analyse** s'ouvre.
3. Dans la fenêtre **Analyse**, sélectionnez la section **Analyse complète**.
4. Dans le groupe **Analyse complète**, cliquez sur le bouton **Lancer l'analyse**.

Kaspersky Small Office Security lancera une analyse complète de l'ordinateur.

ANALYSE PERSONNALISEE

L'analyse personnalisée vous permet d'analyser le fichier, le dossier ou le disque sur les virus et sur d'autres programmes présentant une menace.

Il est possible de lancer l'analyse personnalisée à l'aide des moyens suivants :

- à partir du menu contextuel de l'objet ;
- à partir de la fenêtre principale de l'application.

Pour lancer l'analyse personnalisée depuis le menu contextuel de l'objet, procédez comme suit :

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

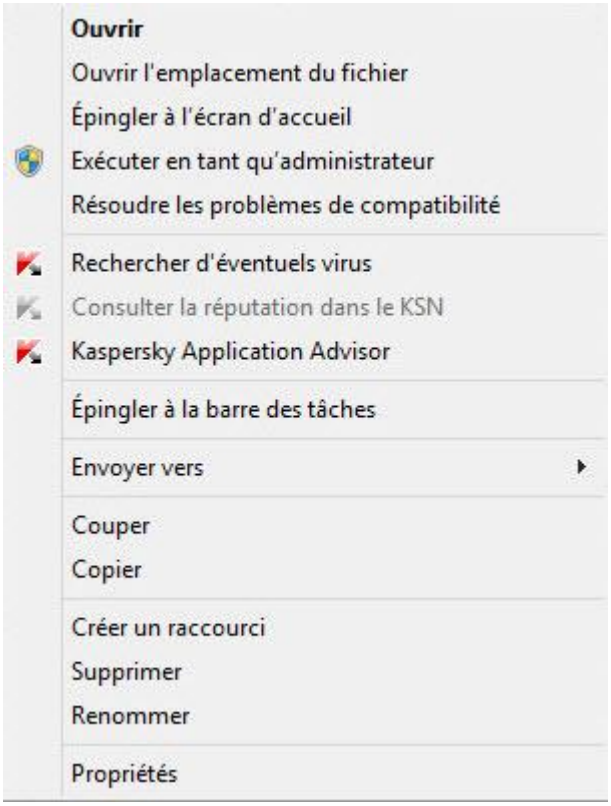


Illustration 4. Menu contextuel de l'objet

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

1. Ouvrez la fenêtre principale de l'application.
2. Cliquez sur le bouton **Analyse**.

   La fenêtre **Analyse** s'ouvre.
3. Dans la fenêtre **Analyse**, sélectionnez la section **Analyse personnalisée**.
4. Indiquez les objets à analyser à l'aide d'une des méthodes suivantes :
   - Déplacez les objets dans la fenêtre **Analyse personnalisée**.
   - Cliquez sur le bouton **Ajouter** et indiquez l'objet dans la fenêtre de sélection du fichier ou du dossier.
5. Cliquez sur le bouton **Lancer l'analyse**.

ANALYSE RAPIDE

Pendant l'analyse rapide, Kaspersky Small Office Security analyse par défaut les objets suivants :

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

Pour lancer l'analyse rapide, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Cliquez sur le bouton **Analyse**.

   La fenêtre **Analyse** s'ouvre.
3. Dans la fenêtre **Analyse**, sélectionnez la section **Analyse rapide**.
4. Dans le groupe **Analyse rapide**, cliquez sur le bouton **Lancer l'analyse**.

Kaspersky Small Office Security lancera une analyse rapide de l'ordinateur.

RECHERCHE DE VULNERABILITES

Une *vulnérabilité* est un endroit non protégé dont le code est utilisé par les individus malintentionnés, par exemple pour copier les données utilisées par l'application au code non protégé. La recherche de vulnérabilités sur votre ordinateur permet d'identifier les "points faibles" de la protection de votre ordinateur. Il est conseillé de supprimer les vulnérabilités détectées.

Pour lancer la recherche de vulnérabilités, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Le lien **Afficher les outils complémentaires**, situé dans la partie inférieure de la fenêtre principale, permet d'ouvrir la fenêtre **Outils**.
3. Dans la partie gauche de la fenêtre **Outils** à l'aide du lien **Recherche de Vulnérabilités**, ouvrez la fenêtre **Recherche de Vulnérabilités**.
4. Dans le groupe **Recherche de Vulnérabilités**, cliquez sur le bouton **Lancer l'analyse**.

Kaspersky Small Office Security commence à rechercher la présence éventuelle de vulnérabilités sur votre ordinateur.

RESTAURATION DE L'OBJET 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 objet supprimé ou réparé s'effectue à partir de sa copie de sauvegarde créée par l'application lors de l'analyse.

Kaspersky Small Office Security ne répare pas les applications de la Boutique Windows. Si une de ces applications est considérée comme dangereuse à l'issue de l'analyse, elle sera supprimée de l'ordinateur.

En cas de suppression d'applications de la Boutique Windows, Kaspersky Small Office Security ne crée pas de copie de sauvegarde. Pour restaurer ce type d'objets, il faut utiliser les outils de restauration du système d'exploitation (pour plus d'informations, veuillez consulter la documentation du système d'exploitation de votre ordinateur) ou mettre à jour les applications via la Boutique Windows.

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

1. Ouvrez la fenêtre principale de l'application.
2. Dans la liste déroulante **Afficher les outils complémentaires**, sélectionnez l'élément **Quarantaine**.
3. Dans la fenêtre **Quarantaine** qui s'ouvre, sélectionnez le fichier requis dans la liste et cliquez sur le bouton **Restaurer**.

RESTAURATION DU SYSTEME D'EXPLOITATION

Cette section contient les informations sur la restauration du système d'exploitation après une infection par des virus.

DANS CETTE SECTION

A PROPOS DE LA 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 de programmes malveillants ou suite à une erreur système, utilisez l'*Assistant de restauration après infection* qui supprime les traces des objets malveillants dans le système d'exploitation. 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 d'exploitation a été modifié d'une manière ou d'une autre : blocage de l'accès à l'environnement réseau, modification des extensions de formats de fichiers connus, blocage du panneau de, configuration, etc. Les causes de ces dégâts sont multiples. Il peut s'agir de l'activité de programmes malveillants, d'une mauvaise configuration du système d'exploitation, de pannes du système ou de l'utilisation d'applications d'optimisation du système d'exploitation qui ne fonctionnent pas correctement.

Une fois l'étude terminée, l'Assistant analyse les informations recueillies afin d'identifier les dommages dans le système d'exploitation nécessitant 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 par catégorie selon la gravité des problèmes identifiés.

RESTAURATION DU SYSTEME D'EXPLOITATION A L'AIDE DE L'ASSISTANT DE RESTAURATION

- *Pour lancer l'Assistant de restauration après infection, procédez comme suit :*

  1. Ouvrez la fenêtre principale de l'application.
  2. Dans la liste déroulante **Afficher les outils complémentaires**, sélectionnez l'élément **Restauration du système**.

  La fenêtre de l'Assistant de restauration après infection 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 d'exploitation

Assurez-vous que l'option **Exécuter la recherche d'endommagements liés à l'activité de programmes malveillants** est sélectionnée dans la fenêtre de l'Assistant, puis cliquez sur le bouton **Suivant**.

Etape 2. Recherche de problèmes

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

Etape 3. Sélection des actions pour éliminer les endommagements

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 les éliminer. Trois groupes d'actions ont été désignés :

- Les *actions vivement recommandées* permettent de supprimer les corruptions qui constituent un problème sérieux. Il est conseillé d'exécuter toutes les actions de ce groupe.
- Les *actions recommandées* visent à supprimer les corruptions qui peuvent présenter un danger. L'exécution des actions de ce groupe est également recommandée.
- Les *actions complémentaires* permettent de supprimer les corruptions du système d'exploitation 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 l'icône ▸ 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 sélectionnées par défaut car vous pourriez mettre en danger la sécurité de l'ordinateur.

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

Etape 4. Elimination des endommagements

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

Etape 5. Fin de l'Assistant

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

PROTECTION DU COURRIER ELECTRONIQUE

Cette section contient les informations sur la protection du courrier électronique contre le courrier indésirable, les virus et d'autres applications présentant une menace.

DANS CETTE SECTION

CONFIGURATION DE L'ANTIVIRUS COURRIER

Kaspersky Small Office Security 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 est lancé 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 configurer l'Antivirus Courrier, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Cliquez sur le lien **Configuration** dans la partie inférieure de la fenêtre.
3. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le module **Antivirus Courrier**.

   Cette fenêtre affiche les paramètres de l'Antivirus Courrier.
4. Confirmez que le bouton d'activation de l'Antivirus Courrier dans la partie supérieure de la fenêtre est bien en position Activé.
5. Sélectionnez le niveau de protection :

   - **Recommandé**. A ce niveau, l'Antivirus Courrier analyse le courrier entrant et sortant ainsi que les archives jointes.
   - **Faible**. A ce niveau, l'Antivirus Courrier analyse uniquement le courrier entrant, mais pas les archives jointes.
   - **Elevé**. A ce niveau, l'Antivirus Courrier analyse le courrier entrant et sortant ainsi que les archives jointes. Si vous choisissez le niveau élevé, l'analyse heuristique opère une analyse détaillée.
6. Dans la liste déroulante **Action en cas de détection d'une menace**, sélectionnez l'action que l'Antivirus Courrier exécutera en cas de détection d'un objet infecté (par exemple, réparer).

Si aucune menace n'a été détectée dans le message ou si les objets infectés ont été réparés, le message peut être utilisé. Si l'objet infecté ne peut pas être réparé, l'Antivirus Courrier renomme ou supprime l'objet du message et place dans l'objet du message une notification indiquant que le message a été traité par Kaspersky Small Office Security. Dans le cas de suppression de l'objet, Kaspersky Small Office Security crée sa copie de sauvegarde et place en quarantaine (cf. section "Restauration de l'objet supprimé ou réparé par l'application" à la page 43).

Cette fonctionnalité est inaccessible si l'application Kaspersky Small Office Security est installée sur le serveur de fichier.

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 inférieure de la fenêtre pour accéder à la section **Configuration**.
3. Dans la partie gauche de la fenêtre, sélectionnez la section **Protection**.
4. Dans la partie droite de la section **Protection**, sélectionnez le module **Anti-Spam**.

   La fenêtre reprend les paramètres de l'Anti-Spam.
5. Activez l'Anti-Spam à l'aide du bouton dans la partie droite de la fenêtre.
6. Assurez-vous que le niveau **Recommandé** est défini dans le groupe **Niveau de protection**.

Cette fonctionnalité est inaccessible si l'application Kaspersky Small Office Security est installée sur le serveur de fichier.

PROTECTION DES DONNEES PERSONNELLES SUR INTERNET

Cette section contient des informations sur la sécurité de l'utilisation d'Internet et sur la protection de vos données contre le vol.

DANS CETTE SECTION

A PROPOS DE LA PROTECTION DES DONNEES PERSONNELLES SUR INTERNET

Kaspersky Small Office Security protège vos données personnelles contre le vol :

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

Kaspersky Small Office Security 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.

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.

Le Clavier virtuel et la protection des données saisies au clavier permettent d'empêcher l'interception des données saisies au clavier.

Pour supprimer les informations sur les actions de l'utilisateur sur l'ordinateur, il y a l'Assistant de suppression des traces d'activité.

Pour la protection des données lors de l'utilisation des services de banque en ligne et pour les paiements sur les boutiques en ligne, il y a la Protection bancaire.

Pour la protection contre l'envoi des données personnelles via Internet, un des outils du Contrôle Internet (cf. section "Utilisation du Contrôle Internet" à la page 65) est prévu.

Cette fonctionnalité est inaccessible si l'application Kaspersky Small Office Security est installée sur le serveur de fichier.

A PROPOS DU CLAVIER VIRTUEL

Lors 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 d'une banque en ligne.

Il y a un risque que ces données soient interceptées à l'aide d'outils d'interception ou d'enregistreurs de frappes. Le clavier virtuel permet d'éviter l'interception des données saisies au clavier.

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

Le clavier virtuel possède les particularités suivantes :

- Il faut appuyer sur les touches du Clavier virtuel 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. Une deuxième pression sur une touche équivaut au relâchement d'une touche sur le clavier.
- 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 **LEFT ALT**+**MAJ**, il faudra cliquer sur la touche **LEFT ALT** avec le bouton gauche de la souris, puis cliquer avec le bouton droit sur la touche **MAJ**).

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

L'utilisation du Clavier virtuel possède les restrictions suivantes :

- 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, 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 (versions 10 et 11) de style Windows 8, ainsi que dans le navigateur Microsoft Internet Explorer (versions 10 et 11) 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 Small Office Security.
- 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.
- Le clavier virtuel n'empêche pas la capture d'écran à l'aide de la touche **PRINT SCREEN** et d'autres combinaisons de touches définies dans les paramètres du système d'exploitation.
- Lors du lancement du Clavier virtuel dans le navigateur Microsoft Internet Explorer, la fonction de remplissage automatique des champs de saisie arrête de fonctionner parce que ce système permet aux individus malintentionnés d'intercepter les données saisies.
- Kaspersky Small Office Security ne protège pas contre les captures d'écran dans le système d'exploitation Microsoft Windows 8 et 8.1 (uniquement les 64 bits) si la fenêtre du Clavier virtuel est ouvert, mais le processus de la Navigation sécurisée n'est pas lancé.
- Dans certains navigateurs (par exemple, Google Chrome), la protection des données saisies de type quelconque peut ne pas fonctionner (par exemple, des adresses du courrier électronique ou des chiffres).

La liste ci-dessus cite les restrictions principales dont la fonctionnalité de protection des données saisies possède. La liste complète des restrictions est reprise dans l'article sur le site Internet du Support Technique de Kaspersky Lab (http://support.kaspersky.com/fr/11603).

LANCEMENT DU CLAVIER VIRTUEL

Pour ouvrir le Clavier virtuel, vous disposez des méthodes suivantes :

- via le menu contextuel de l'icône de l'application dans la zone de notification ;
- à partir de la fenêtre principale de l'application ;
- à partir de la fenêtre du navigateur Microsoft Internet Explorer, Mozilla Firefox ou Google Chrome à l'aide de l'icône d'accès rapide au Clavier virtuel ;
- à l'aide de l'icône d'accès rapide au Clavier virtuel dans les champs 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 (cf. section "Configuration d'affichage de l'icône du Clavier virtuel" à la page 51).

  Lors de l'utilisation du Clavier virtuel, Kaspersky Small Office Security désactive la fonction de remplissage automatique des champs de saisie sur les sites Internet.

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

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).

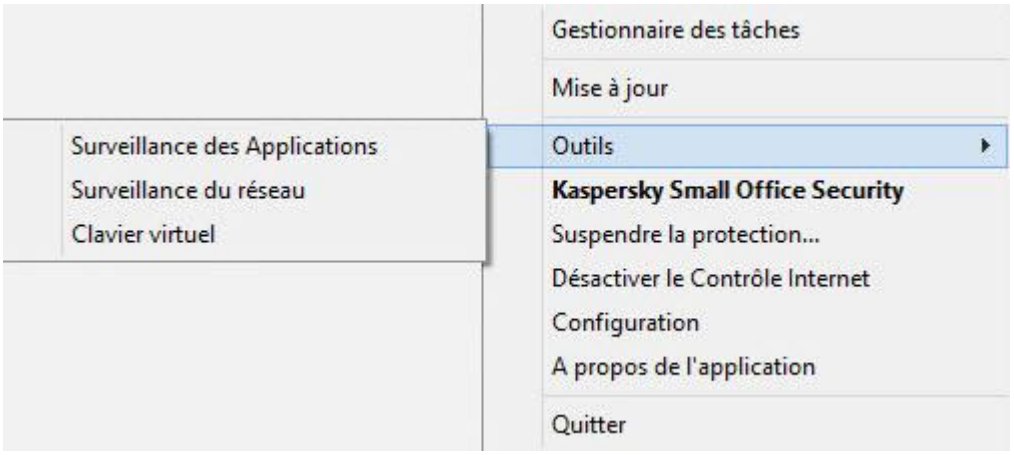


Illustration 5. Menu contextuel de Kaspersky Anti-Virus

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

1. Ouvrez la fenêtre principale de l'application.
2. Le lien **Afficher les outils complémentaires**, situé dans la partie inférieure de la fenêtre principale, permet d'ouvrir la fenêtre **Outils**.
3. Dans la gauche de la fenêtre **Outils** à l'aide du lien **Clavier virtuel**, ouvrez la fenêtre Clavier virtuel.

- *Pour ouvrir le Clavier virtuel depuis la fenêtre du navigateur Microsoft Internet Explorer ou Mozilla Firefox,*

  cliquez sur le bouton  **Clavier virtuel** dans la barre d'outils du navigateur.

- *Pour ouvrir le Clavier virtuel depuis la fenêtre du navigateur Google Chrome,*

  1. cliquez sur le bouton  **Kaspersky Protection** dans la barre d'outils du navigateur.
  2. Dans le menu déroulant, sélectionnez l'option  **Clavier virtuel**.

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

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

CONFIGURATION D'AFFICHAGE DE L'ICONE DU CLAVIER VIRTUEL

- *Pour configurer l'affichage de l'icône d'accès rapide au 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 inférieure de la fenêtre.
  3. Dans la fenêtre qui s'ouvre **Configuration** dans la section **Avancé**, sélectionnez la sous-section **Saisie sécurisée des données**.

     Les paramètres de la configuration de la saisie sécurisée des données s'affichent dans la fenêtre.
  4. S'il faut, cochez la case **Ouvrir le Clavier virtuel via la combinaison de touches CTRL+ALT+MAJ+P** dans le groupe **Clavier virtuel**.
  5. Si vous voulez que l'icône d'appel du Clavier Virtuel s'affiche dans les champs de saisie, cochez la case **Afficher l'icône d'accès rapide dans les champs de saisie**.
  6. Si vous voulez que l'icône d'accès au Clavier virtuel s'affiche uniquement lors de l'ouverture de sites Internet précis, procédez comme suit :

     a. Dans le groupe **Clavier virtuel** à l'aide du lien **Modifier les catégories**, ouvrez la fenêtre **Paramètres de la Saisie sécurisée des données**.

     b. Cochez les cases pour les catégories de sites Internet sur lesquels il faut afficher l'icône d'accès rapide dans les champs de saisie.

        L'icône d'accès au Clavier virtuel sera affichée lors de l'ouverture du site Internet lié à une des catégories sélectionnées.

     c. Si vous voulez activer ou désactiver l'affichage de l'icône d'accès au Clavier virtuel sur le site Internet défini, procédez comme suit :

        a. A l'aide du lien **Configuration des exclusions**, ouvrez la fenêtre **Exclusions pour le Clavier virtuel**.

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

           La fenêtre d'ajout d'une exclusion pour le Clavier virtuel s'ouvre.

        c. Saisissez l'adresse du site Internet dans le champ **Masque de l'adresse Internet**.

d. Si vous voulez que l'icône d'appel du Clavier virtuel s'affiche (ou ne s'affiche pas) uniquement sur la page Internet indiquée, dans le groupe **Zone d'application**, sélectionnez **Appliquer à la page indiquée**.

e. Dans le groupe **Icône du Clavier virtuel**, indiquez si l'icône d'accès au Clavier virtuel doit s'afficher sur la page Internet indiquée.

f. Cliquez sur le bouton **Ajouter**.

Le site Internet renseigné apparaît dans la liste de la fenêtre **Exclusions pour le Clavier virtuel**.

Lors de l'ouverture du site Internet, l'icône d'accès au Clavier virtuel sera affichée dans les champs de saisie conformément aux paramètres configurés.

PROTECTION DES DONNEES SAISIES AU CLAVIER

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

La protection des données saisies au clavier possède les restrictions suivantes :

- 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 de la saisie des données est inaccessible dans le navigateur Microsoft Internet Explorer depuis la boutique en ligne de Windows.
- La protection des données saisies au clavier ne peut protéger vos données si le site Internet demandant la saisie de ces données a été compromis car dans ce cas, les données tombent directement entre les mains des individus malintentionnés.
- Dans certains navigateurs (par exemple, Google Chrome), la protection des données saisies de type quelconque peut ne pas fonctionner (par exemple, des adresses du courrier électronique ou des chiffres).

La liste ci-dessus cite les restrictions principales dont la fonctionnalité de protection des données saisies possède. La liste complète des restrictions est reprise dans l'article sur le site Internet du Support Technique de Kaspersky Lab (http://support.kaspersky.com/fr/11603).

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

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 inférieure de la fenêtre pour accéder à la section **Configuration**.
3. Dans la section **Avancé**, sélectionnez la sous-section **Saisie sécurisée des données**.

   Les paramètres de la saisie sécurisée des données s'affichent.
4. Dans le groupe **Protection des données saisies au clavier** situé dans la partie inférieure de la fenêtre, cochez la case **Protéger les données saisies au clavier**.
5. Définissez la zone de protection des données saisies au clavier :

   a. Ouvrez la fenêtre **Paramètres de la Saisie sécurisée des données** à l'aide du lien **Modifier les catégories** dans la partie inférieure du groupe **Protection des données saisies au clavier**.

   b. Cochez les cases pour les catégories des sites Internet sur lesquels il faut protéger les données saisies au clavier.

c. Si vous voulez activer la protection des données saisies au clavier sur un site Internet défini, procédez comme suit :

   a. Ouvrez la fenêtre **Exclusions pour la protection des données saisies au clavier** à l'aide du lien **Configuration des exclusions**.

   b. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Ajouter**.

      La fenêtre d'ajout d'une exclusion pour la protection des données saisies au clavier s'ouvre.

   c. Dans la fenêtre qui s'ouvre, saisissez l'URL du site dans le champ **Masque de l'adresse Internet**.

   d. Sélectionnez une des options de protection des données saisies sur ce site Internet (**Appliquer à la page Internet indiquée** ou **Appliquer à tout le site Internet**).

   e. Sélectionnez l'action de la protection des données saisies sur ce site (**Protéger** ou **Ne pas protéger**).

   f. Cliquez sur le bouton **Ajouter**.

Le site Internet renseigné apparaît dans la liste de la fenêtre **Exclusions pour la protection des données saisies au clavier**. Quand vous ouvrirez ce site, les données saisies seront protégées conformément aux paramètres définis.

CONFIGURATION DES NOTIFICATIONS SUR LES VULNERABILITES DU RESEAU WI-FI

Pendant l'utilisation du réseau Wi-Fi, vos données confidentielles peuvent être volées si le réseau Wi-Fi n'est pas assez protégé. Kaspersky Small Office Security vérifie le réseau Wi-Fi à chaque fois que vous vous connectez au réseau Wi-Fi. Si le réseau Wi-Fi n'est pas sécurisé (par exemple, un protocole de cryptage vulnérable est utilisé ou le nom du réseau Wi-Fi (SSID) n'est pas assez populaire), l'application affiche une notification indiquant que vous vous connectez à un réseau Wi-Fi non sécurisé. Le lien dans la fenêtre de notification permet de savoir comment se protéger lors de l'utilisation du réseau Wi-Fi.

Pour configurer les notifications sur les vulnérabilités du réseau Wi-Fi, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Cliquez sur le lien **Configuration** dans la partie inférieure de la fenêtre pour accéder à la section **Configuration**.
3. Dans la partie gauche de la fenêtre, sélectionnez la section **Protection**.
4. Dans la partie droite de la section **Protection**, sélectionnez la sous-section **Pare-feu**.

   Cette fenêtre affiche alors les paramètres du module Pare-feu.
5. Cochez la case **Signaler les vulnérabilités lors de la connexion au réseau Wi-Fi** si elle a été décochée. Si vous ne souhaitez pas recevoir de notifications, décochez cette case. Cette case est cochée par défaut.
6. Si la case **Signaler les vulnérabilités lors de la connexion au réseau Wi-Fi** est cochée, vous pouvez configurer les paramètres complémentaires d'affichage des notifications :

   - Cochez la case **Interdire le transfert du mot de passe sur Internet sous forme non protégée et afficher une notification** pour bloquer le transfert du mot de passe sous forme texte non protégée lors du remplissage du champ **Mot de passe** sur Internet. Cette case est décochée par défaut.
   - A l'aide du lien **Restaurer des notifications masquées** rétablissez les paramètres d'affichage des notifications sur le transfert du mot de passe sous forme non protégée. Si vous avez bloqué auparavant l'affichage des notifications sur le transfert du mot de passe sous forme non protégée, ces notifications seront affichées de nouveau.

Cette fonctionnalité est inaccessible si l'application Kaspersky Small Office Security est installée sur le serveur de fichier.

PROTECTION DES OPERATIONS FINANCIERES ET DES ACHATS SUR INTERNET

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

La fonctionnalité de la Navigation sécurisée est inaccessible si l'application Kaspersky Small Office Security est installée sur le serveur de fichier.

La Navigation sécurisée est un mode spécial de fonctionnement du navigateur qui est utilisé pour protéger vos données lors d'utilisation des sites Internet des banques ou des systèmes de paiement. La Navigation sécurisée est lancée dans un environnement isolé pour qu'autres programmes ne puissent pas s'intégrer dans le processus de la Navigation sécurisée.

Lors de l'utilisation de la Navigation sécurisée, l'application offre une protection contre les types suivants des menaces :

- Modules douteux. L'analyse sur la présence des modules douteux est exécutée à chaque accès au site Internet de la banque ou du système de paiement.
- Rootkits. L'analyse sur la présence des rootkits est exécutée au lancement de la Navigation sécurisée.
- Vulnérabilités connues du système d'exploitation. L'analyse sur la présence des vulnérabilités du système d'exploitation est exécutée au lancement de la Navigation sécurisée.
- Certificats invalides des sites Internet des banques et de systèmes de paiement. L'analyse des certificats est exécutée lors de l'accès au site Internet de la banque ou du système de paiement. L'analyse des certificats est exécutée sur la base des certificats compromis.

Quand vous ouvrez le site Internet en Navigation sécurisée, un cadre s'affiche autour de la fenêtre du navigateur. La couleur du cadre signale l'état de la protection.

Les couleurs suivantes peuvent être utilisées dans le cadre de la fenêtre du navigateur :

- Cadre de couleur verte. Signifie que l'exécution de toutes les analyses a réussi. Vous pouvez poursuivre l'utilisation de la Navigation sécurisée.
- Cadre de couleur jaune. Signifie que des problèmes de sécurité à supprimer ont été détectés lors des analyses.

  L'application peut détecter les menaces suivantes, ainsi que les problèmes de sécurité :

  - Module douteux. L'analyse de l'ordinateur et la réparation sont requises.
  - Rootkit. L'analyse de l'ordinateur et la réparation sont requises.
  - Vulnérabilité du système d'exploitation. L'installation des mises à jour du système d'exploitation est requise.
  - Certificat invalide du site Internet de la banque ou du système de paiement.

  Si vous ne supprimez pas les menaces détectées, la sécurité de la session de connexion au site Internet de la banque ou du système de paiement n'est pas garantie. Les événements, liés au lancement et l'utilisation de la Navigation sécurisée avec une protection basse, sont enregistrés dans le journal des événements Windows.

  La couleur jaune de l'icône peut aussi signifier que le lancement de la Navigation sécurisée est impossible à cause des restrictions techniques. Par exemple, l'hyperviseur de l'éditeur tiers est lancé ou votre ordinateur ne prend pas en charge la technologie de virtualisation matérielle.

Pour un fonctionnement correct de la Navigation sécurisée, il faut que les plug-ins du module Protection bancaire soient activés dans celle-ci. Les plug-ins sont automatiquement activés dans le navigateur lors de son premier lancement après l'installation de Kaspersky Small Office Security. Si le navigateur n'a pas été relancé après l'installation de Kaspersky Small Office Security, les plug-ins ne sont pas activés.

L'activation automatique des plug-ins possède les restrictions suivantes :

- Les plug-ins s'intègrent et s'activent uniquement dans les navigateurs pris en charge par l'application.

  Les navigateurs suivants prennent en charge les plug-ins de la Protection bancaire :

  - Internet Explorer versions 8.0, 9.0, 10.0, 11.0.

    Les navigateurs Internet Explorer 10 de style Modern UI et Internet Explorer 11 de style Windows 8 ne sont pas pris en charge.

  - Mozilla Firefox versions 19.x, 20.x, 21.x, 22.x, 23.x, 24.x, 25.x, 26.x, 27.x, 28.x, 29.x, 30.x, 31.x, 32.x, 33.x, 34.x.

  - Google Chrome versions 33.x, 34.x, 35.x, 36.x, 37.x, 38.x.

    Kaspersky Small Office Security prend en charge l'utilisation du navigateur Google Chrome versions 37.x et 38.x dans le système d'exploitation de 32 bits et de 64 bits.

    Dans Mozilla Firefox, les plug-ins ne sont pas activés automatiquement si un profil d'utilisateur n'a pas été créé dans le navigateur. Pour créer un profil de l'utilisateur, il faut redémarrer le navigateur.

    Lors du premier lancement de Google Chrome en mode sécurisé, le navigateur Internet vous proposera d'installer l'extension Kaspersky Protection Plugin qui active les plug-ins du module Protection bancaire. Dans le cas de refus d'installation de l'extension Kaspersky Protection Plugin, vous pourrez l'installer plus tard à l'aide du lien http://support.kaspersky.com/interactive/google/fr/kisplugin.

- Lors de la mise à jour du navigateur, les plug-ins ne sont pas activés automatiquement si la nouvelle version du navigateur prend en charge la même technologie d'activation des plug-ins que la version précédente du navigateur. Si la nouvelle version du navigateur prend en charge la même technologie d'activation des plug-ins que la version précédente du navigateur, les plug-ins sont activés automatiquement.

Si les plug-ins ne sont pas activés automatiquement lors du redémarrage du navigateur, il faut les activer manuellement. Les paramètres du navigateur permettent de voir si les plug-ins sont activés ou de les activer manuellement. Les informations sur l'activation des plug-ins sont à consulter dans l'aide du navigateur utilisé.

Vous pouvez activer ou désactiver l'activation automatique des plug-ins (cf. section "Activation de l'activation automatique des plug-ins de la Protection bancaire" à la page 57) dans la fenêtre de configuration de l'application.

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.

DANS CETTE SECTION

CONFIGURATION DES PARAMETRES DE LA PROTECTION BANCAIRE

Pour configurer la Protection bancaire, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Cliquez sur le lien **Configuration** dans la partie inférieure de la fenêtre principale de l'application pour accéder à la section **Configuration**.
3. Dans la partie gauche de la fenêtre, sélectionnez la section **Protection**.
4. Dans la partie droite de la section **Protection**, sélectionnez la sous-section **Protection bancaire**.

   Cette fenêtre affiche alors les paramètres du module Protection bancaire.
5. Activez le module Protection bancaire à l'aide du bouton dans la partie supérieure de la fenêtre.
6. Pour activer la notification sur les vulnérabilités détectées dans le système d'exploitation avant le lancement de la navigation sécurisée, cochez la case **Signaler les vulnérabilités dans le système d'exploitation**.

CONFIGURATION DE LA PROTECTION BANCAIRE POUR UN SITE INTERNET QUELCONQUE

Pour configurer la Protection bancaire pour un site Internet défini, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre principale qui s'ouvre, cliquez sur le bouton **Protection bancaire**.

   La fenêtre **Protection bancaire** s'ouvre.
3. Cliquez sur le bouton **Ajouter un site Internet à la Protection bancaire**.

   Les champs de saisie des informations relatives au site apparaissent dans la partie droite de la fenêtre.
4. Dans le champ **Site Internet pour la Protection bancaire**, saisissez l'adresse du site Internet à ouvrir en mode de Navigation sécurisée.

   Devant l'adresse du site Internet, le protocole https:// utilisé par la Navigation sécurisée par défaut doit s'afficher.
5. En cas de nécessité, saisissez le nom ou la description de ce site Internet dans le champ **Description**.
6. Sélectionnez le mode de lancement de la navigation sécurisée lors de l'ouverture de ce site Internet :
   - Si vous voulez que le site Internet s'ouvre automatiquement à chaque fois en Navigation sécurisée, sélectionnez l'option **Lancer la Navigation sécurisée**.
   - Si vous voulez que l'application Kaspersky Small Office Security vous demande l'action à exécuter lors de l'ouverture du site Internet, sélectionnez l'option **Confirmer l'action**.
   - Si vous voulez activer la Protection bancaire pour ce site Internet, sélectionnez l'option **Ne pas lancer la Navigation sécurisée**.
7. Dans la partie droite de la fenêtre, cliquez sur le bouton **Ajouter**.

Le site Internet s'affichera dans la liste dans la partie gauche de la fenêtre.

LANCEMENT DE L'ACTIVATION AUTOMATIQUE DES PLUG-INS DE LA PROTECTION BANCAIRE

Pour activer l'activation des plug-ins de la Protection bancaire dans les navigateurs, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Cliquez sur le lien **Configuration** dans la partie inférieure de la fenêtre principale de l'application pour accéder à la section **Configuration**.
3. Dans la partie gauche de la fenêtre, sélectionnez la section **Protection**.
4. Dans la partie droite de la section **Protection**, sélectionnez la section **Antivirus Internet**.
5. Dans la fenêtre **Paramètres de l'Antivirus Internet** qui s'ouvre, à l'aide du lien **Configuration avancée**, ouvrez la fenêtre **Paramètres avancés de l'Antivirus Internet**.
6. Dans le groupe **Extensions des navigateurs Internet**, cochez la case **Activer automatiquement les plug-ins de l'application dans tous les navigateurs Internet**.

A PROPOS DE LA PROTECTION CONTRE LES CAPTURES D'ECRAN

Kaspersky Small Office Security bloque la création non autorisée de captures d'écran par des logiciels espions, en protégeant vos données lors de l'utilisation des sites Internet protégés. La protection contre les captures d'écran est activée par défaut. Si la protection a été désactivée manuellement, vous pouvez l'activer dans la fenêtre de configuration de l'application (cf. section "Activation de la protection contre la création des images de l'écran" à la page 57).

Kaspersky Small Office Security utilise la technologie de l'hyperviseur pour protéger contre les captures d'écran. La fonctionnalité de protection contre les captures d'écran à l'aide de l'hyperviseur de Kaspersky Small Office Security possède les restrictions suivantes dans le système d'exploitation Microsoft Windows 8 x64 :

- La fonctionnalité n'est pas accessible au lancement de l'hyperviseur d'un programme tiers, par exemple, d'un programme de virtualisation de la société VMware™. Après l'utilisation de l'hyperviseur d'un programme tiers, la fonctionnalité de protection contre les captures d'écran devient de nouveau accessible.
- La fonctionnalité n'est pas accessible si le processeur central de votre ordinateur ne prend pas en charge la technologie de virtualisation matérielle. Pour savoir si le processeur de votre ordinateur prend en charge ou non la technologie de virtualisation matérielle, consultez la documentation technique de votre ordinateur ou rendez-vous sur le site Internet du fabricant du processeur.
- La fonctionnalité n'est pas accessible si au moment du lancement de la Navigation sécurisée, un hyperviseur actif d'un programme tiers a été détecté, par exemple, un programme de la société VMware.

ACTIVATION DE LA PROTECTION CONTRE LES CAPTURES D'ECRAN

Pour activer la protection contre les captures d'écran, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Cliquez sur le lien **Configuration** dans la partie inférieure de la fenêtre pour accéder à la section **Configuration**.
3. Dans la partie gauche de la fenêtre, sélectionnez la section **Protection**.
4. Dans la partie droite de la section **Protection**, sélectionnez la sous-section **Protection bancaire** et assurez-vous que le commutateur de la Protection bancaire est activé.

   La fenêtre **Paramètres de la Protection bancaire** s'ouvre.
5. Dans le groupe **Avancé**, cochez la case **Bloquer les captures d'écran lors de l'utilisation de la Navigation sécurisée**.

A PROPOS DES DONNEES DU PRESSE-PAPIERS

Kaspersky Small Office Security bloque l'accès non autorisé des applications au presse-papiers pendant les transactions bancaires, empêchant ainsi le vol de données par des individus malintentionnés. Le blocage agit uniquement dans le cas des tentatives des applications douteuses d'obtenir l'accès au presse-papiers. Si vous copiez manuellement les données depuis la fenêtre d'une application vers la fenêtre d'une autre application (par exemple, du Bloc-notes dans la fenêtre de l'éditeur de texte), l'accès au presse-papiers est autorisé. Si le navigateur Internet Explorer® ouvert en mode normal est une source des données pour la copie, uniquement les données depuis la ligne d'adresse du navigateur peuvent être placées dans le presse-papiers.

LANCEMENT DE L'APPLICATION DE PROTECTION DES MOTS DE PASSE KASPERSKY PASSWORD MANAGER

L'application Kaspersky Password Manager est conçue pour un remplissage automatique des champs de saisie des mots de passe et d'autres données personnelles sur les sites Internet et dans les applications Windows. Kaspersky Password Manager doit être installé indépendamment de Kaspersky Small Office Security. Après l'installation, vous pouvez lancer Kaspersky Password Manager depuis le menu **Démarrer** ou depuis la fenêtre de Kaspersky Small Office Security.

Pour utiliser l'application Kaspersky Password Manager, les exigences et les restrictions suivantes sont requises :

- L'application est accessible au téléchargement, à l'installation et au lancement via l'interface Kaspersky Small Office Security uniquement si l'application Kaspersky Small Office Security est installée sur l'ordinateur personnel et non pas sur le serveur de fichier.
- L'accès à Internet est requis pour utiliser l'application Kaspersky Password Manager. Les mots de passe et les autres données personnelles dans Kaspersky Password Manager sont conservés dans le stockage cloud.
- Après l'installation, l'application Kaspersky Password Manager doit être connectée au portail My Kaspersky à l'aide du compte de l'utilisateur qui va utiliser Kaspersky Password Manager.

  Sous réserve de cette exigence, les mots de passe, conservés dans Kaspersky Password Manager, seront accessibles uniquement à l'utilisateur de Kaspersky Password Manager.

Pour plus d'informations sur la connexion de Kaspersky Password Manager au portail My Kaspersky, cf. *Manuel de l'utilisateur de Kaspersky Password Manager*.

Pour lancer l'application de protection des mots de passe Kaspersky Password Manager, si elle est déjà installée, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application Kaspersky Small Office Security.
2. Cliquez sur le bouton **Gestionnaire de mots de passe**.

La fenêtre de l'application de protection des mots de passe Kaspersky Password Manager s'ouvre.

Pour télécharger l'application de protection des mots de passe Kaspersky Password Manager, si elle n'est pas encore installée, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Cliquez sur le bouton **Gestionnaire de mots de passe**.

   La fenêtre **Gestionnaire de mots de passe** s'ouvre.
3. Cliquez sur le bouton **Télécharger**.

   Vous allez être dirigés vers le site Internet de Kaspersky Lab. Ce site vous aidera à télécharger le paquet d'installation de Kaspersky Password Manager.

Les informations sur l'utilisation de l'application Kaspersky Password Manager sont reprises dans le *Manuel de l'utilisateur Kaspersky Password Manager*.

Cette fonctionnalité est inaccessible si l'application Kaspersky Small Office Security est installée sur le serveur de fichier.

VERIFICATION DE LA SECURITE DU SITE INTERNET

Kaspersky Small Office Security permet d'analyser la sécurité d'un site Internet avant de cliquer sur le lien vers ce site Internet. La vérification de la sécurité d'un site Internet est confiée à *l'URL Advisor* qui fait partie de l'Antivirus Internet.

Le module URL Advisor est inaccessible dans le navigateur Microsoft Internet Explorer (versions 10 et 11) de style Windows 8.

L'URL Advisor s'intègre dans les navigateurs Microsoft Internet Explorer, Google Chrome et Mozilla Firefox et analyse les liens figurant sur la page Internet ouverte dans le navigateur. A côté de chaque lien, Kaspersky Small Office Security 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, qui s'ouvre à l'aide du lien ;
-  – si la page Internet, qui s'ouvre à l'aide du lien, est dangereuse selon les données de Kaspersky Lab.

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

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

Pour configurer l'analyse des liens sur les sites Internet, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Cliquez sur le lien **Configuration** dans la partie inférieure de la fenêtre principale de l'application pour ouvrir la fenêtre **Configuration**.
3. Dans la section **Protection**, choisissez la sous-section **Antivirus Internet**.

   La fenêtre reprend les paramètres de l'Antivirus Internet.
4. Le lien **Configuration avancée** de la partie inférieure de la fenêtre ouvre la fenêtre des paramètres avancés de l'Antivirus Internet.
5. Dans le groupe **URL Advisor**, cochez la case **Analyser les liens**.
6. Pour que l'Antivirus Internet analyse le contenu de tous les sites Internet, choisissez l'option **Sur tous les sites Internet sauf les sites indiqués**.

   Le cas échéant, désignez les pages Internet auxquelles vous faites confiance à l'aide du lien **Configurer les exclusions**. L'Antivirus Internet ne va pas analyser le contenu des pages Internet indiquées, ainsi que les connexions chiffrées aux sites Internet indiqués.
7. Pour que l'Antivirus Internet analyse uniquement le contenu de certaines pages Internet, procédez comme suit :

   a. Choisissez l'option **Uniquement sur les sites Internet indiqués**.

   b. Cliquez sur le lien **Configurer les sites Internet vérifiés**.

c. Dans la fenêtre **Configurer les sites Internet vérifiés** qui s'ouvre, cliquez sur **Ajouter**.

d. Dans la fenêtre **Ajouter l'URL** qui s'ouvre, saisissez l'adresse de la page Internet dont le contenu devra être analysé.

e. Sélectionnez l'état d'analyse de la page Internet (*Actif* : l'Antivirus Internet analysera le contenu de la page Internet).

f. Cliquez sur le bouton **Ajouter**.

La page indiquée apparaît dans la liste de la fenêtre **URL analysées**. L'Antivirus Internet analysera les liens sur cette page.

8. Si vous souhaitez configurer d'autres paramètres d'analyse des liens, dans la fenêtre **Paramètres avancés de l'Antivirus Internet** du groupe **URL Advisor**, cliquez sur le lien **Configurer l'URL Advisor**.

La fenêtre **Configurer l'URL Advisor** s'ouvre.

9. Pour que l'Antivirus Internet vous alerte sur la sécurité des liens sur toutes les pages Internet, cochez la case **Tous les liens** dans le groupe **Liens à analyser**.

10. Pour que l'Antivirus Internet affiche les informations relatives à l'appartenance d'un lien à une catégorie de contenu définie (par exemple, *langage vulgaire*), procédez comme suit :

a. Cochez la case **Afficher les informations sur les catégories de contenu des sites Internet**.

b. Cochez les cases en regard des catégories de contenu dont les informations devront apparaître dans les commentaires.

L'Antivirus Internet analyse les liens sur les pages indiquées et affichera les informations relatives aux catégories conformément aux paramètres configurés.

PROTECTION CONTRE LES BANNIERES LORS DES VISITES DES SITES INTERNET

Le module Anti-bannière est conçu pour protéger contre les bannières dans Internet. Si le module est activé, vous pouvez désactiver l'affichage des bannières directement sur la page Internet ou indiquer l'adresse du site Internet ou le masque à l'aide duquel Kaspersky Small Office Security bloquera l'affichage des bannière sur ce site Internet. Par défaut, Kaspersky Small Office Security protège contre les types de bannières les plus répandus.

Cette fonctionnalité est inaccessible si l'application Kaspersky Small Office Security est installée sur le serveur de fichier.

DANS CETTE SECTION

ACTIVATION DU MODULE ANTI-BANNIERE

Pour activer le module Anti-bannière, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Le lien **Configuration** permet de passer à la fenêtre **Configuration**.
3. Sélectionnez la section **Protection**.
4. Activez le module **Anti-bannière**.

DESACTIVATION D'AFFICHAGE D'UNE BANNIERE SUR LE SITE INTERNET

Pour désactiver l'affichage d'une bannière sur le site Internet, procédez comme suit :

1. Placez le curseur de la souris sur la bannière dont vous voulez désactiver l'affichage.
2. Cliquez sur le touche **CTRL** sur le clavier.
3. Dans le menu apparu, sélectionnez l'option **Ajouter à l'Anti-bannière**.

   La fenêtre **URL interdites** s'ouvre.
4. Dans la fenêtre **URL interdites**, cliquez sur **Ajouter**.

   L'adresse de la bannière sera ajoutée à la liste des adresses Internet interdites.
5. Mettez à jour la page Internet dans le navigateur pour que la bannière ne s'affiche plus.

Lors du futur accès à cette page Internet, la bannière ne s'affichera pas.

DESACTIVATION D'AFFICHAGE DE TOUTES LES BANNIERES SUR LE SITE INTERNET

Vous pouvez désactiver l'affichage de toutes les bannières sur un site Internet particulier. Pour ce faire, il faut indiquer le masque de ce site Internet et l'ajouter à la liste des URL interdites.

Pour désactiver l'affichage de toutes les bannières sur le site Internet, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Le lien **Configuration** permet de passer à la fenêtre **Configuration**.
3. Sélectionnez la section **Protection**.
4. Sélectionnez le module **Anti-bannière**.

   La fenêtre **Paramètres de l'Anti-bannière** s'ouvre.
5. Dans la fenêtre **Paramètres de l'Anti-bannière** à l'aide du lien **Configurer les URL interdites**, ouvrez la fenêtre **URL interdites**.
6. Dans la fenêtre **URL interdites**, cliquez sur **Ajouter**.
7. Dans la fenêtre ouverte dans le champ **Masque d'adresse Internet (URL)**, saisissez le masque d'adresse du site Internet sur lequel vous voulez désactiver l'affichage des bannières. Par exemple : `http://example.com*`.
8. Indiquez **Actif** en tant que l'état pour ce site Internet.
9. Cliquez sur le bouton **Ajouter**.

Kaspersky Small Office Security bloquera les bannières sur le site http://example.com.

ELIMINATION DES TRACES D'UTILISATION DE L'ORDINATEUR ET D'INTERNET

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

- termes de recherche et 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 peuvent être accessibles aux individus malintentionnés et aux tiers.

Kaspersky Small Office Security comprend un Assistant de suppression des traces d'activité de l'utilisateur dans le système d'exploitation.

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

1. Ouvrez la fenêtre principale de l'application.
2. Le lien **Afficher les outils complémentaires**, situé dans la partie inférieure de la fenêtre principale, permet d'ouvrir la fenêtre **Outils**.
3. Dans la partie gauche de la fenêtre **Outils** à l'aide du lien **Suppression des traces d'activité**, lancez l'Assistant de suppression des traces d'activité.

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

Examinons en détails les étapes de l'Assistant.

Etape 1. Guide de démarrage de l'Assistant

Assurez-vous que l'option **Exécuter la recherche des 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 signale les traces d'activité détectées et les moyens proposés pour les éliminer (cf. ill. ci-après).

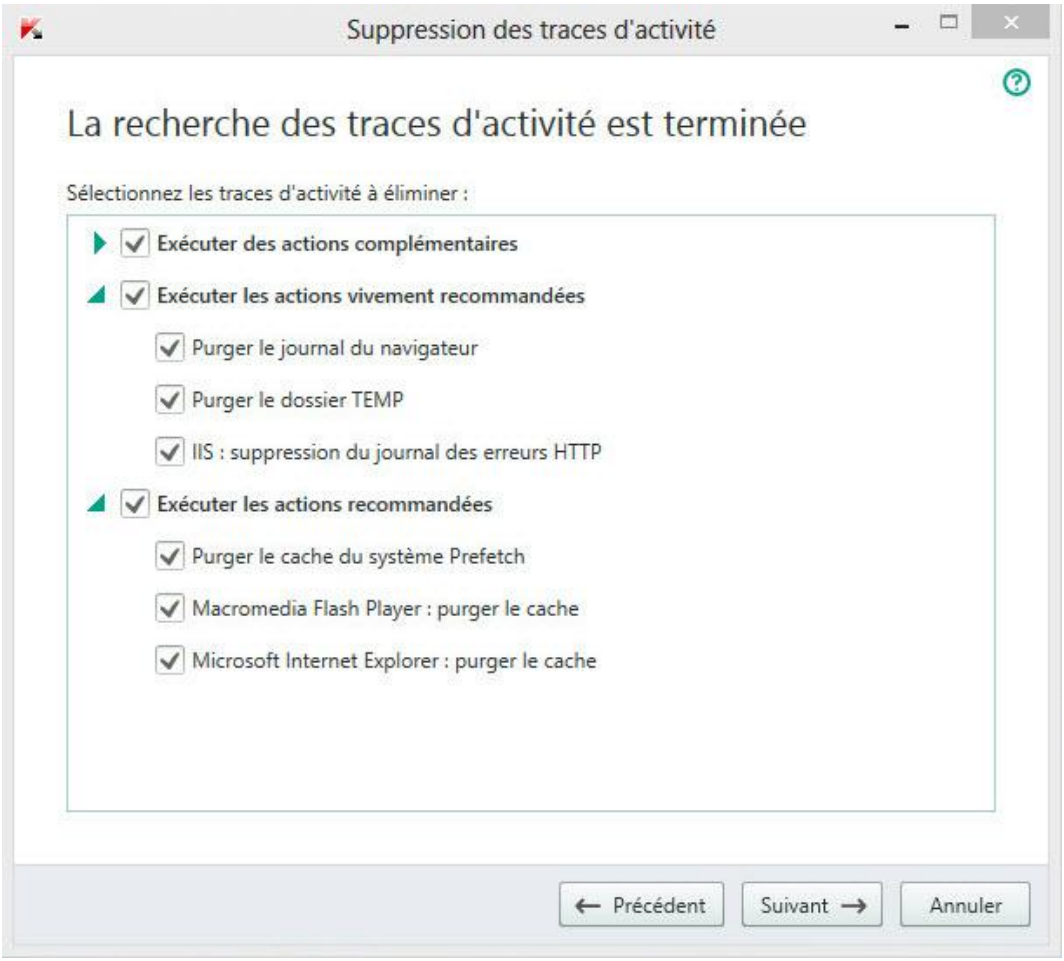


Illustration 6. Traces d'activité détectées et recommandations de suppression

Pour voir les actions reprises dans le groupe, cliquez sur l'icône ▸ 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 sélectionnées par défaut car vous pourriez mettre en danger la sécurité de l'ordinateur.

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

Etape 4. Suppression des traces d'activité

L'Assistant exécute les actions sélectionnées à l'étape précédente. La suppression des traces d'activité peut durer un certain temps. La suppression de certaines traces d'activité nécessitera peut-être le redémarrage de l'ordinateur. L'Assistant vous préviendra.

Une fois les traces d'activité supprimées, l'Assistant passe automatiquement à l'étape suivante.

Etape 5. Fin de l'Assistant

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

CONTROLE D'UTILISATION DE L'APPLICATION SUR L'ORDINATEUR ET SUR INTERNET

Cette section contient les informations sur le contrôle des actions des utilisateurs sur l'ordinateur et sur Internet à l'aide de Kaspersky Small Office Security.

DANS CETTE SECTION

UTILISATION DU CONTROLE INTERNET

Le Contrôle Internet permet de contrôler les actions de différents utilisateurs sur l'ordinateur et sur le réseau. A l'aide du Contrôle Internet, vous pouvez limiter l'accès aux ressources Internet et aux applications et consulter des rapports sur les actions des utilisateurs.

Les utilisateurs d'Internet sont heurtés à une suite des 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 avec le contenu pornographique, extrémiste, le contenu extrême faisant l'apologie des armes, de la drogue, de la violence, etc. ;
- le téléchargement de fichiers infectés par des programmes malveillants ;
- les contacts avec les individus malintentionnés qui peuvent obtenir captieusement ou autrement les informations des employés à ne pas révéler.

Le Contrôle Internet permet de diminuer les risques liés à l'utilisation de l'ordinateur et d'Internet. Pour ce faire, les fonctions suivantes du module sont utilisées :

- restriction de l'utilisation de l'ordinateur et d'Internet dans le temps ;
- composition de listes d'applications dont l'exécution est autorisée ou interdite et restriction temporaire sur l'exécution d'applications autorisées ;
- composition de listes de sites dont la visite est autorisée ou interdite et sélection de catégories de contenu ne pouvant être consulté ;

- activation du mode de recherche sécurisée à l'aide des moteurs de recherche (dans ce cas, les liens de sites au contenu douteux n'apparaissent pas dans les résultats de la recherche) ;
- restriction du téléchargement de fichiers sur 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 ;
- recherche de mots clés définis dans les communications.

Toutes les restrictions sont activées séparément, ce qui permet une administration flexible du Contrôle Internet pour différents utilisateurs. Des rapports sont rédigés pour chaque compte utilisateur. Ces rapports reprennent les événements des catégories contrôlées pour une période donnée.

Le Contrôle Internet est inaccessible si l'application Kaspersky Small Office Security est installée sur le serveur de fichier.

ACCES A LA CONFIGURATION DES PARAMETRES DU CONTROLE INTERNET

Pour accéder à la configuration des paramètres du Contrôle Internet, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la fenêtre principale de l'application, cliquez sur le bouton **Contrôle Internet**.
3. Lors de la première ouverture de la fenêtre **Contrôle Internet**, l'application vous propose de définir le mot de passe pour protéger les paramètres du Contrôle Internet. Sélectionnez une des options proposées :
   - Si vous voulez protéger l'accès aux paramètres du Contrôle Internet à l'aide du mot de passe, saisissez les champs **Mot de passe** et **Confirmation** et cliquez sur le bouton **Poursuivre**.
   - Si vous ne voulez pas protéger l'accès aux paramètres du Contrôle Internet à l'aide d'un mot de passe, à l'aide du lien **Ignorer**, passez à la configuration des paramètres du Contrôle Internet.

   La fenêtre **Contrôle Internet** s'ouvre.
4. Sélectionnez le compte utilisateur et à l'aide du lien **Configurer les restrictions**, passez à la fenêtre de configuration des paramètres du Contrôle Internet.

CONTROLE D'UTILISATION DE L'ORDINATEUR

Le Contrôle Internet permet de définir une limite d'utilisation de l'ordinateur. Vous pouvez indiquer une plage de temps pendant laquelle le Contrôle Internet doit bloquer l'accès à l'ordinateur (pendant la nuit par exemple) ou définir une durée d'utilisation maximum par journée. Ces restrictions peuvent varier pour les jours ouvrables et les jours de repos.

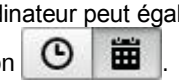
Pour configurer les durées d'utilisation autorisées de l'ordinateur, procédez comme suit :

1. Passez à la fenêtre de configuration des paramètres du Contrôle Internet (cf. section "Passage à la configuration des paramètres du Contrôle Internet" à la page 66).
2. Dans la fenêtre de configuration des paramètres du Contrôle Internet, sélectionnez la section **Ordinateur**.

3. Pour définir l'intervalle pendant lequel le Contrôle Internet va bloquer l'accès à l'ordinateur, cochez la case **Bloquer l'accès à partir de** dans les groupes **Jours ouvrables** et **Week-ends**.

4. Dans la liste déroulante, à côté de la case **Bloquer l'accès à partir de**, indiquez l'heure de début du blocage.

5. Dans la liste déroulante **jusqu'à**, indiquez l'heure de fin du blocage.

   La programmation de la durée d'utilisation de l'ordinateur peut également être effectuée à l'aide d'un tableau. Le tableau s'affiche lorsque vous cliquez sur le bouton  .

   Le Contrôle Internet empêchera l'utilisateur d'accéder à l'utilisateur pendant la période indiquée.

6. Pour limiter la durée globale d'utilisation de l'ordinateur, cochez la case **Autoriser l'accès pas plus de** dans les groupes **Jours ouvrables** et **Week-ends**, puis définissez l'intervalle à l'aide des listes déroulantes en regard des cases.

   Le Contrôle Internet empêchera l'utilisateur d'accéder à l'ordinateur une fois que la durée globale d'utilisation pour la journée dépassera l'intervalle défini.

7. Pour définir des pauses dans l'utilisation de l'ordinateur, cochez la case **Repos toutes les** dans le groupe **Repos**, puis définissez la fréquence (par exemple, toutes les heures) et la durée (par exemple, 10 minutes) des pauses à l'aide des listes déroulantes en regard de la case.

8. Dans la fenêtre **Contrôle Internet**, activez le commutateur **Contrôle Internet** situé en face du compte utilisateur.

Le Contrôle Internet empêchera l'utilisateur d'accéder à l'ordinateur conformément aux paramètres.

CONTROLE DE L'UTILISATION D'INTERNET

Le Contrôle Internet permet de limiter la durée d'utilisation d'Internet et de bloquer l'accès à des catégories de sites sélectionnées, voire à des sites en particulier. De plus, vous pouvez interdire le téléchargement de certains types de fichiers sur Internet (par exemple, des archives, des vidéos, etc.).

- *Pour configurer les durées d'utilisation autorisées d'Internet, procédez comme suit :*

  1. Passez à la fenêtre de configuration des paramètres du Contrôle Internet (cf. section "Passage à la configuration des paramètres du Contrôle Internet" à la page 66).

  2. Dans la fenêtre de configuration des paramètres du Contrôle Internet, sélectionnez la section **Internet**.

  3. Si vous souhaitez limiter la durée totale d'utilisation d'Internet pendant les jours ouvrables, cochez la case **Limiter l'accès les jours ouvrables jusqu'à <HH:MM> heures par jour** dans le groupe **Restriction d'accès sur Internet** et définissez la période à l'aide de la liste déroulante en regard de la case.

  4. Si vous souhaitez limiter la durée totale d'utilisation d'Internet les jours de repos, cochez la case **Limiter l'accès les week-ends jusqu'à <HH:MM> heures par jour** et définissez la période à l'aide de la liste déroulante en regard de la case.

  5. Dans la fenêtre **Contrôle Internet**, activez le commutateur **Contrôle Internet** situé en face du compte utilisateur.

  Le Contrôle Internet limitera la durée totale que l'utilisateur peut passer sur Internet conformément aux valeurs définies.

- *Pour limiter l'accès à certains sites Internet, procédez comme suit :*

  1. Passez à la fenêtre de configuration des paramètres du Contrôle Internet (cf. section "Passage à la configuration des paramètres du Contrôle Internet" à la page 66).

  2. Dans la fenêtre de configuration des paramètres du Contrôle Internet, sélectionnez la section **Internet**.

3. Pour que le contenu pour adulte n'apparaisse pas dans les résultats de la recherche, cochez la case **Activer la recherche sécurisée** dans le groupe **Consultation de sites**.

   Lors de la recherche d'informations sur les sites Internet, tels que Google™, YouTube™ (uniquement pour les utilisateurs qui ne sont pas connectés au site youtube.com sous ses comptes) Bing®, Yahoo!™, Mail.ru, VK.com, Yandex, le contenu "pour Adultes" ne sera pas présent parmi les résultats de recherche.

4. Pour interdire l'accès à certaines catégories de sites Internet, procédez comme suit :

   a. Dans le groupe **Consultation de sites**, cochez la case **Bloquer l'accès aux sites Internet suivants**.

   b. Sélectionnez l'option **Sites Internet pour adultes**, puis cliquez sur le lien **Sélectionner les catégories des sites Internet** pour ouvrir la fenêtre **Bloquer l'accès aux catégories des sites Internet**.

   c. Cochez les cases en regard des catégories de sites dont l'ouverture sera interdite.

      Le Contrôle Internet bloquera l'ouverture du site si son contenu appartient à une des catégories sélectionnées.

5. Pour bloquer l'accès à des sites Internet en particulier, procédez comme suit :

   a. Dans le groupe **Consultation de sites**, cochez la case **Bloquer l'accès aux sites Internet suivants**.

   b. Sélectionnez l'option **Tous les sites Internet sauf les sites autorisés dans la liste des exclusions**, puis cliquez sur le lien **Ajouter les exclusions** pour ouvrir la fenêtre **Exclusions**.

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

      La fenêtre **Ajouter un nouveau site Internet** s'ouvre.

   d. Saisissez l'adresse du site auquel vous souhaitez interdire l'accès dans le champ **Masque de l'adresse Internet**.

   e. Définissez la portée de l'interdiction dans le groupe **Zone d'application** : ensemble du site ou uniquement la page renseignée.

   f. Si vous souhaitez interdire l'accès au site indiqué, choisissez l'option **Interdire** dans le groupe **Action**.

   g. Cliquez sur le bouton **Ajouter**.

   Le site Internet renseigné apparaît dans la liste de la fenêtre **Exclusions**.

6. Dans la fenêtre **Contrôle Internet**, activez le commutateur **Contrôle Internet** situé en face du compte utilisateur.

Le Contrôle Internet va interdire l'accès aux sites repris dans la liste conformément aux paramètres définis.

Pour interdire le téléchargement de certains fichiers sur Internet, procédez comme suit :

1. Passez à la fenêtre de configuration des paramètres du Contrôle Internet (cf. section "Passage à la configuration des paramètres du Contrôle Internet" à la page 66).

2. Dans la fenêtre de configuration des paramètres du Contrôle Internet, sélectionnez la section **Internet**.

3. Dans le groupe **Interdiction de téléchargement des fichiers**, cochez les cases en regard des types de fichiers dont le téléchargement sera interdit.

4. Dans la fenêtre **Contrôle Internet**, activez le commutateur **Contrôle Internet** situé en face du compte utilisateur.

Le Contrôle Internet interdira le téléchargement du type de fichiers indiqué.

CONTROLE DU LANCEMENT DES APPLICATIONS

A l'aide du Contrôle Internet vous pouvez interdire l'exécution de certaines applications (par exemple, des jeux, des clients de messagerie instantanée) ou limiter la durée d'utilisation de celles-ci.

Pour restreindre le lancement d'une application précise, procédez comme suit :

1. Passez à la fenêtre de configuration des paramètres du Contrôle Internet (cf. section "Passage à la configuration des paramètres du Contrôle Internet" à la page 66).

2. Dans la fenêtre de configuration des paramètres du Contrôle Internet, sélectionnez la section **Applications**.

3. Dans la partie inférieure de la fenêtre, à l'aide du lien **Ajouter l'application dans la liste**, ouvrez la fenêtre **Ouvrir** et sélectionnez le fichier exécutable de l'application.

   L'application sélectionnée apparaît dans la liste dans le groupe **Bloquer les applications indiquées**. Kaspersky Small Office Security ajoute automatiquement ce programme à la catégorie définie, par exemple *Jeux*.

4. Si vous souhaitez interdire le lancement d'une application, cochez la case en regard de son nom dans la liste. Vous pouvez également interdire le lancement de toutes les applications d'une catégorie définie en cochant la case en regard du nom de la catégorie dans la liste (par exemple, vous pouvez appliquer l'interdiction aux applications de la catégorie *Jeux*).

5. Si vous voulez installer des restrictions durant l'utilisation de l'application, sélectionnez dans la liste une application ou une catégorie des applications et à l'aide du lien **Configurer les règles**, ouvrez la fenêtre **Restriction d'utilisation de l'application**.

6. Si vous souhaitez limiter la durée d'utilisation de l'application pendant les jours ouvrables et les jours de repos, dans les groupes **Jours ouvrables** et **Week-ends**, cochez les cases **Autoriser l'accès pas plus de** et dans la liste déroulante indiquez le nombre d'heures par jour durant lesquelles l'utilisateur a le droit d'utiliser l'application. Vous pouvez également définir les périodes exactes pendant lesquelles l'utilisateur peut ou ne peut pas utiliser l'application à l'aide du tableau. Le tableau s'affiche lorsque vous cliquez sur le bouton  .

7. Si vous souhaitez définir des interruptions dans l'utilisation d'une application, cochez la case **Repos toutes les** dans le groupe **Repos** et sélectionnez la fréquence et la longueur de la pause à l'aide de la liste déroulante.

8. Cliquez sur le bouton **Enregistrer**.

9. Dans la fenêtre **Contrôle Internet**, activez le commutateur **Contrôle Internet** situé en face du compte utilisateur.

Le Contrôle Internet appliquera les restrictions définies lorsque l'utilisateur utilisera l'application.

CONTROLE DES COMMUNICATIONS VIA LES RESEAUX SOCIAUX

Le Contrôle Internet permet de consulter les communications des utilisateurs des réseaux sociaux et de clients de messagerie instantanée et de bloquer les échanges avec certains contacts.

Pour configurer le contrôle des communications de l'utilisateur, procédez comme suit :

1. Passez à la fenêtre de configuration des paramètres du Contrôle Internet (cf. section "Passage à la configuration des paramètres du Contrôle Internet" à la page 66).

2. Dans la fenêtre de configuration des paramètres du Contrôle Internet, sélectionnez la section **Communication**.

3. Pour consulter les communications et, le cas échéant, bloquer certains contacts, procédez comme suit :

   a. Sélectionnez l'option **Interdire la correspondance avec tous les contacts sauf les contacts autorisés**.

   b. Le lien **Contacts connus** ouvre la fenêtre **Rapport sur la communication**.

   c. Consultez la liste des contacts avec lesquels l'utilisateur a communiqué. Vous pouvez afficher des contacts en particulier dans la fenêtre à l'aide d'une des méthodes suivantes :

      - Pour consulter les communications de l'utilisateur sur un réseau social ou un client de messagerie instantanée en particulier, sélectionnez l'élément requis dans la liste déroulante dans la partie gauche de la fenêtre.

      - Pour afficher les contacts avec lesquels l'utilisateur communique le plus, sélectionnez l'option **Par nombre de messages** dans la liste déroulante dans la partie droite de la fenêtre.

      - Pour afficher les contacts avec lesquels l'utilisateur communique un jour en particulier, sélectionnez l'option **Par date de correspondance** dans la liste déroulante dans la partie droite de la fenêtre.

   d. Pour consulter les communications de l'utilisateur avec un contact en particulier, cliquez sur le contact dans la liste.

      La fenêtre **Historique de la correspondance** s'ouvre.

   e. Si vous souhaitez interdire les communications de l'utilisateur avec le contact sélectionné, cliquez sur le bouton **Interdire la correspondance**.

4. Dans la fenêtre **Contrôle Internet**, activez le commutateur **Contrôle Internet** situé en face du compte utilisateur.

Le Contrôle Internet bloquera les communications entre l'utilisateur et le contact sélectionné.

CONTROLE DU CONTENU DE LA CORRESPONDANCE

Le Contrôle Internet permet de voir si l'utilisateur partage des données personnelles (nom de famille, numéro de téléphone, numéro de carte de crédit) ou utilise des expressions clés (par exemple, du langage vulgaire) dans sa correspondance et de bloquer ce type de messages.

Pour configurer le contrôle du transfert de données personnelles, procédez comme suit :

1. Passez à la fenêtre de configuration des paramètres du Contrôle Internet (cf. section "Passage à la configuration des paramètres du Contrôle Internet" à la page 66).

2. Dans la fenêtre de configuration des paramètres du Contrôle Internet, sélectionnez la section **Contrôle du contenu**.

3. Dans le groupe **Contrôle de transfert des données personnelles**, cochez la case **Interdire le transfert des données personnelles à des tiers**.

4. Le lien **Modifier la liste des données personnelles** ouvre la fenêtre **Liste des données personnelles**.

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

   La fenêtre d'ajout des données personnelles s'ouvre.

6. Sélectionnez le type de données personnelles (par exemple, "numéro de téléphone"), cliquez sur le lien ou saisissez la description dans le champ **Nom du champ**.

7. Indiquez les données personnelles (par exemple, un numéro de téléphone), dans le champ **Valeur**.

8. Cliquez sur le bouton **Ajouter**.

   Les données personnelles apparaissent dans la liste de la fenêtre **Liste des données personnelles**.

9. Dans la fenêtre **Contrôle Internet**, activez le commutateur **Contrôle Internet** situé en face du compte utilisateur.

Le Contrôle Internet surveillera la mention des données personnelles indiquées dans les messages instantanés ou sur des sites Internet et les bloquera.

Pour configurer le contrôle de l'utilisation d'expressions clés dans la correspondance, procédez comme suit :

1. Passez à la fenêtre de configuration des paramètres du Contrôle Internet (cf. section "Passage à la configuration des paramètres du Contrôle Internet" à la page 66).

2. Dans la fenêtre de configuration des paramètres du Contrôle Internet, sélectionnez la section **Contrôle du contenu**.

3. Dans le groupe **Contrôle de l'utilisation des mots clés**, cochez la case **Activer le contrôle de l'utilisation des mots clés**.

4. A l'aide du lien **Modifier la liste des mots clés**, ouvrez la fenêtre **Contrôle de l'utilisation des mots clés**.

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

   La fenêtre d'ajout du mot clé s'ouvre.

6. Saisissez l'expression clé dans le champ **Valeur**, puis cliquez sur le bouton **Ajouter**.

   L'expression clé indiquée apparaît dans la liste des mots clés de la fenêtre **Contrôle de l'utilisation des mots clés**.

7. Dans la fenêtre **Contrôle Internet**, activez le commutateur **Contrôle Internet** situé en face du compte utilisateur.

Le Contrôle Internet interdira la diffusion des messages contenant l'expression clé indiquée via Internet ou les clients de messagerie instantanée.

CONSULTATION DU RAPPORT SUR LES ACTIONS DE L'UTILISATEUR

Vous pouvez consulter les rapports sur les actions de chaque utilisateur pour lequel le Contrôle Internet 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. Passez à la fenêtre de configuration des paramètres du Contrôle Internet (cf. section "Passage à la configuration des paramètres du Contrôle Internet" à la page 66).

2. Sélectionnez le compte utilisateur et à l'aide du lien **Consulter le rapport**, accédez à la fenêtre des rapports.

3. Dans le groupe reprenant le type de restrictions souhaitées (par exemple, **Internet** ou **Communication**), ouvrez le rapport relatif aux actions contrôlées via le lien **Plus d'informations**.

Le rapport relatif aux actions contrôlées de l'utilisateur s'affiche dans la fenêtre.

ADMINISTRATION A DISTANCE DE LA PROTECTION DES ORDINATEURS

Cette section contient les informations sur l'administration à distance de la protection des ordinateurs de votre entreprise à l'aide du portail Centre d'administration de Kaspersky Small Office Security.

DANS CETTE SECTION

A PROPOS DE L'ADMINISTRATION A DISTANCE DE LA PROTECTION DES ORDINATEURS

Si l'application Kaspersky Small Office Security est installée sur les ordinateurs de votre entreprise, vous pouvez administrer à distance la protection de ces ordinateurs. L'administration à distance de la protection des ordinateurs est exécutée sur le portail Centre d'administration de Kaspersky Small Office Security.

La configuration de l'administration à distance est exécutée dans une séquence suivante :

1. L'enregistrement du compte administrateur sur le portail My Kaspersky (http://center.kaspersky.com).
2. L'enregistrement de la licence de Kaspersky Small Office Security sur le portail My Kaspersky (http://center.kaspersky.com).

   Suite à l'enregistrement de la licence, le portail Centre d'administration de Kaspersky Small Office Security devient accessible à l'utilisateur avec le compte administrateur.
3. La connexion des ordinateurs (cf. section "Connexion de l'ordinateur au portail Centre d'administration de Kaspersky Small Office Security" à la page 73), dont vous voulez administrer à distance, au portail Centre d'administration de Kaspersky Small Office Security sous le compte utilisateur.
4. L'entrée dans le portail Centre d'administration de Kaspersky Small Office Security sous le compte administrateur.

Le portail Centre d'administration de Kaspersky Small Office Security vous permet d'effectuer les tâches de protection suivantes des ordinateurs de votre entreprise :

- consulter la liste des problèmes de sécurité sur l'ordinateur et les résoudre à distance ;
- rechercher sur l'ordinateur les virus et autres programmes présentant une menace ;
- mettre à jour les bases et les modules d'application ;
- configurer les modules de l'application Kaspersky Small Office Security.

Si l'analyse de l'ordinateur est lancée depuis le portail Centre d'administration de Kaspersky Small Office Security, Kaspersky Small Office Security traite les objets détectés de manière automatique sans votre participation. En cas de détection d'un virus ou d'un autre programme présentant une menace, l'application Kaspersky Small Office Security tente d'effectuer une réparation sans redémarrer l'ordinateur. Si la réparation est impossible sans le redémarrage de l'ordinateur, le portail Centre d'administration de Kaspersky Small Office Security signale dans la liste des problèmes de protection de l'ordinateur que le redémarrage est requis pour réparer l'ordinateur.

CONNEXION DE L'ORDINATEUR AU PORTAIL CENTRE D'ADMINISTRATION DE KASPERSKY SMALL OFFICE SECURITY

Pour connecter l'ordinateur au portail Centre d'administration de Kaspersky Small Office Security, procédez comme suit :

1. Créez un compte administrateur sur le portail My Kaspersky (http://center.kaspersky.com).
2. Enregistrez la licence de Kaspersky Small Office Security sous le compte administrateur sur le portail My Kaspersky (http://center.kaspersky.com).

   Suite à l'enregistrement de la licence, le portail Centre d'administration de Kaspersky Small Office Security devient accessible à l'utilisateur avec le compte administrateur.
3. Installez Kaspersky Small Office Security sur l'ordinateur dont vous voulez administrer la protection.
4. Ouvrez la fenêtre principale de l'application.
5. Cliquez sur le bouton **Centre d'administration**.
6. Dans la fenêtre **Centre d'administration**, cliquez sur le bouton **Connecter l'ordinateur au portail**.
7. Dans la fenêtre **Protection par mot de passe**, saisissez le mot de passe de l'administrateur. Cette étape est présente si la protection d'accès à l'administration de l'application (cf. section "Protection de l'accès à l'administration de Kaspersky Small Office Security à l'aide du mot de passe" à la page 92) est établie..

   Le formulaire de connexion au portail Centre d'administration de Kaspersky Small Office Security sera téléchargé dans la fenêtre **Centre d'administration** si la connexion n'a pas été exécutée auparavant.
8. Remplissez les champs du formulaire de connexion et connectez-vous au portail Centre d'administration de Kaspersky Small Office Security.

La page du portail Centre d'administration de Kaspersky Small Office Security s'ouvrira par défaut à la section **Périphériques** dans la fenêtre du navigateur. Maintenant il est possible d'administrer à distance la protection sur le portail Centre d'administration de Kaspersky Small Office Security.

TRAITEMENT DES APPLICATIONS INCONNUES

Grâce à Kaspersky Small Office Security, vous pouvez réduire les risques liés à l'utilisation d'applications inconnues (par exemple, risques d'infection par des virus et autres programmes présentant une menace ou modification non désirée des paramètres du système d'exploitation).

Kaspersky Small Office Security inclut les modules et les outils qui permettent de vérifier la réputation d'une application et de contrôler l'activité de cette application sur votre ordinateur.

DANS CETTE SECTION

VERIFICATION DE LA REPUTATION DES APPLICATIONS

Kaspersky Small Office Security 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 d'une 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 dans Kaspersky Security Network ;
- pays dans lesquels l'application est la plus répandue.

La vérification de la réputation des applications est disponible uniquement si vous avez accepté de participer à 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).

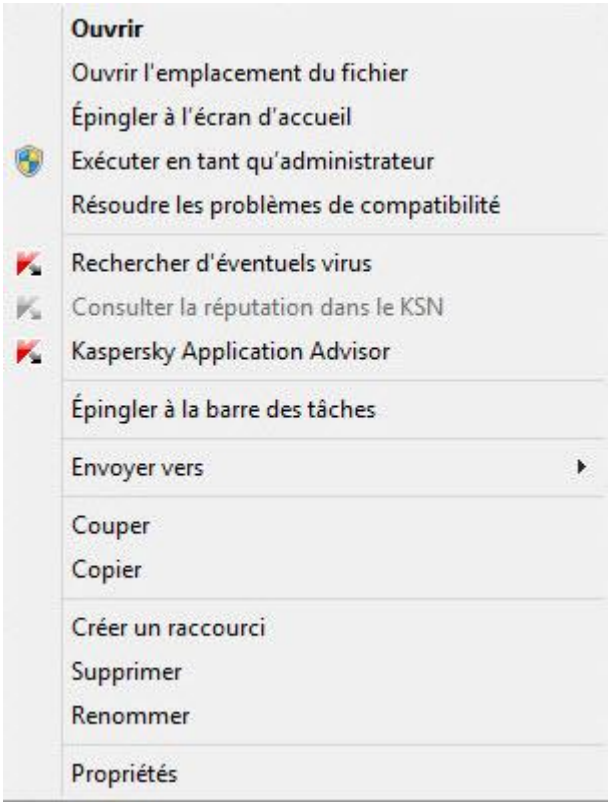


Illustration 7. Menu contextuel de l'objet

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

VOIR EGALEMENT

Participation à Kaspersky Security Network (KSN).....98

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

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

Le Contrôle des Applications surveille les actions en exécution dans le système d'exploitation par les applications installées sur les ordinateurs et les régit à partir des règles. Ces règles réglementent l'activité suspecte, y compris l'accès des applications aux ressources protégées (par exemple, aux fichiers, dossiers, clés du registre, adresses réseau, etc.).

En cas d'utilisation de systèmes d'exploitation 64 bits, les privilèges des applications pour l'exécution des actions suivantes ne peuvent être configurés :

- accès direct à la mémoire physique ;
- administration des pilotes de l'imprimante ;

- création du service ;
- ouverture du service pour la lecture ;
- ouverture du service pour la modification ;
- modification de la configuration du service ;
- administration du service ;
- lancement du service ;
- suppression du service ;
- accès aux données internes du navigateur ;
- accès aux objets critiques du système d'exploitation ;
- accès au stockage des mots de passe ;
- installation des privilèges du débogueur ;
- utilisation des interfaces logicielles du système d'exploitation ;
- utilisation des interfaces logicielles du système d'exploitation (DNS).

En cas d'utilisation de Microsoft Windows 8 64 bits, les privilèges des applications pour l'exécution des actions suivantes ne peuvent être configurés :

- envoi des messages de fenêtre aux autres processus ;
- opérations suspectes ;
- installation des intercepteurs ;
- interception des événements entrants du flux ;
- création d'impressions-écran.

Le module Pare-feu contrôle l'activité réseau des applications.

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

Kaspersky Small Office Security place les applications dans les groupes de confiance (De confiance, Douteuses, Restrictions élevées ou Restrictions faibles) uniquement si le module Contrôle des Applications ou Pare-feu est activé ou quand tous les deux sont activés. Si ces deux modules sont désactivés, la fonctionnalité de répartition des applications dans les groupes ne fonctionne pas.

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

CONFIGURATION DES PARAMETRES DU CONTROLE DES APPLICATIONS

Pour configurer les règles du Contrôle des Applications, procédez comme suit :

1. Ouvrez la fenêtre principale de Kaspersky Small Office Security.
2. Le lien **Afficher les outils complémentaires**, situé dans la partie inférieure de la fenêtre principale, permet d'ouvrir la fenêtre **Outils**.
3. Dans la fenêtre **Outils** à l'aide du lien **Contrôle des Applications**, ouvrez la fenêtre **Contrôle des Applications**.
4. Dans la fenêtre **Contrôle des Applications** dans le groupe **Applications** à l'aide du lien **Administration des applications**, ouvrez la fenêtre **Administration des applications**.
5. Sélectionnez l'application nécessaire dans la liste et ouvrez la fenêtre **Règles pour l'application** par un double clic.

   La fenêtre **Règles pour l'application** s'ouvre.
6. 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 registre**, sélectionnez la catégorie de ressources nécessaire.
     b. D'un clic droit de la souris dans la colonne indiquant l'action possible sur la ressource (**Lecture**, **Ecriture**, **Suppression** ou **Création**), ouvrez le menu contextuel et sélectionnez la valeur nécessaire (**Autoriser**, **Interdire**, **Action** ou **Hériter**).
   - Pour configurer les privilèges de l'application en vue de l'exécution de différentes actions dans le système d'exploitation, procédez comme suit :
     a. Sélectionnez la catégorie de privilèges nécessaire sous l'onglet **Privilèges**.
     b. D'un clic droit de la souris dans la colonne **Autorisation**, ouvrez le menu contextuel et sélectionnez la valeur nécessaire (**Autoriser**, **Interdire**, **Action** ou **Hériter**).
   - Pour configurer les privilèges de l'application en vue de 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 **Enregistrer**.
     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 exclure certaines actions de l'analyse par le Contrôle des Applications, cochez les cases pour les actions à ne pas contrôler sous l'onglet **Exclusions**.
7. Cliquez sur le bouton **Enregistrer**.

   Toutes les exclusions créées dans les règles de contrôle des applications sont accessibles dans la fenêtre de configuration de Kaspersky Small Office Security, dans la section **Menaces et exclusions**.

Le Contrôle des Applications va surveiller et limiter les actions conformément aux paramètres configurés.

A PROPOS DE L'ACCES DES APPLICATIONS A LA WEBCAM

Les individus malintentionnés peuvent tenter d'obtenir l'accès non autorisé à la webcam à l'aide de logiciels spéciaux. Kaspersky Small Office Security bloque l'accès non autorisé des applications à la webcam et affiche une notification sur le blocage de l'accès. Par défaut, Kaspersky Small Office Security interdit l'accès à la webcam aux applications qui font partie des groupes de confiance Restrictions élevées et Douteuses.

Vous pouvez autoriser l'accès à la webcam aux applications (cf. section "Autorisation d'accès de l'application à la webcam" à la page 79) qui font partie du groupe Restrictions élevées et Douteuses dans la fenêtre de configuration du Contrôle des Applications. Si une application qui fait partie du groupe de confiance Restrictions faibles tente de se connecter à la webcam, Kaspersky Small Office Security affiche une notification et vous propose de décider vous-même si vous souhaitez ou non autoriser à cette application l'accès à la webcam.

Si une application avec les droits d'accès par défaut tente de se connecter à la webcam, Kaspersky Small Office Security affiche une notification. La notification contient les informations sur le fait que l'application installée sur l'ordinateur (par exemple, Skype™) reçoit maintenant une image de la webcam. La liste déroulante de la notification permet d'interdire l'accès de l'application à la webcam ou d'accéder à la configuration des paramètres d'accès des applications à la webcam (cf. section "Configuration des paramètres d'accès des applications à la webcam" à la page 78). Cette notification ne s'affiche pas si votre ordinateur exécute déjà des applications en mode plein écran.

La liste déroulante de la notification sur la réception des données vidéo par l'application vous permet aussi de sélectionner l'option **Ne pas afficher cette notification** ou d'accéder à la configuration d'affichage des notifications (cf. section "Configuration des paramètres d'accès des applications à la webcam" à la page 78).

Kaspersky Small Office Security autorise par défaut l'accès à la webcam aux applications pour lesquelles votre autorisation est requise si l'interface graphique de l'application est en cours de chargement, de fermeture ou ne répond pas et que vous ne pouvez pas autoriser l'accès manuellement.

La fonctionnalité de protection de la webcam possède les particularités et les restrictions suivantes :

- L'application contrôle la vidéo et les images statiques obtenues suite au traitement des données de la webcam.
- L'application Kaspersky Small Office Security contrôle uniquement les webcams connectées via l'interface USB ou IEEE1394 et affichées dans le Gestionnaire de périphériques Windows en tant que Périphérique d'acquisition d'images (Imaging Device).

Vous pouvez prendre connaissance de la liste des webcams prises en charge à l'aide du lien http://support.kaspersky.com/fr/10978.

Pour que la protection contre l'accès non autorisé à la webcam fonctionne, le module Contrôle des Applications doit être activé.

Cette fonctionnalité est inaccessible si l'application Kaspersky Small Office Security est installée sur le serveur de fichier.

CONFIGURATION DES PARAMETRES D'ACCES DES APPLICATIONS A LA WEBCAM

Pour configurer les paramètres d'accès des applications à la webcam, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Cliquez sur le lien **Configuration** dans la partie inférieure de la fenêtre principale de l'application pour ouvrir la fenêtre **Configuration**.
3. Dans la section **Protection** dans la partie droite de la fenêtre, sélectionnez le module **Accès à la webcam**.

4. Configurez les paramètres d'accès à la webcam sur votre ordinateur :

   - Si vous voulez interdire l'accès de toutes les applications à la webcam, cochez la case **Interdire l'accès à la webcam à toutes les applications**.
   - Si vous voulez recevoir une notification quand la webcam est utilisée par une application autorisée, cochez la case **Afficher une notification quand la webcam est utilisée par une application autorisée**.
   - Si vous souhaitez autoriser l'accès à la webcam à toutes les applications, dans la fenêtre **Configuration** sous l'onglet **Protection**, désactivez **Accès à la webcam**.

AUTORISATION D'ACCES DE L'APPLICATION A LA WEBCAM

Pour autoriser l'accès de l'application à la webcam, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Le lien **Afficher les outils complémentaires**, situé dans la partie inférieure de la fenêtre principale, permet d'ouvrir la fenêtre **Outils**.
3. Dans la fenêtre **Outils** à l'aide du lien **Contrôle des Applications**, ouvrez la fenêtre **Contrôle des Applications**.
4. Dans la fenêtre **Contrôle des Applications** dans le groupe **Applications** à l'aide du lien **Administration des applications**, ouvrez la fenêtre **Administration des applications**.
5. Sélectionnez dans la liste l'application à laquelle vous voulez autoriser l'accès à la webcam et ouvrez la fenêtre **Règles pour l'application** à l'aide d'un double clic.
6. Dans la fenêtre **Règles pour l'application**, accédez à l'onglet **Privilèges**.
7. Dans la liste des catégories des privilèges, sélectionnez l'option **Modification du système → Modifications suspectes dans le système → Accès à la webcam**.
8. A l'aide du bouton droit de la souris dans la colonne **Autorisation**, ouvrez le menu contextuel et sélectionnez l'option **Autoriser**.
9. Cliquez sur le bouton **Enregistrer**.

L'accès de l'application à la webcam sera autorisé.

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 Small Office Security propose un module pour la suppression des données qui met en échec les outils de restauration logiciels traditionnels.

Kaspersky Small Office Security permet de supprimer de manière irréversible les données sur les types de support suivants :

- Disques réseau et locaux. La suppression est possible si vous possédez 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 cours d'exécution.

Pour supprimer définitivement les données, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Le lien **Afficher les outils complémentaires**, situé dans la partie inférieure de la fenêtre principale, permet d'ouvrir la fenêtre **Outils**.
3. Dans la fenêtre **Outils**, à l'aide du lien **Suppression définitive des données**, ouvrez la fenêtre **Suppression définitive des données** (cf. ill. ci-dessous).

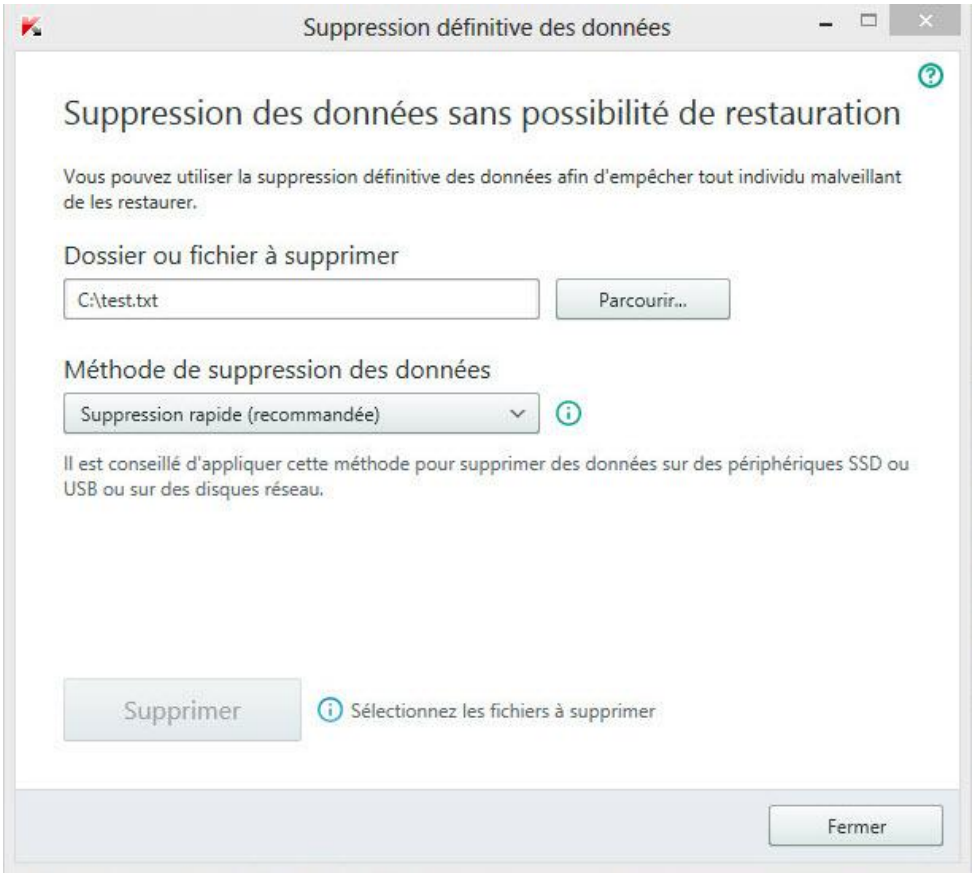


*Illustration 8. Fenêtre **Suppression définitive des données***

4. Cliquez sur le bouton **Parcourir** puis, dans la fenêtre **Sélection du dossier** qui s'ouvre, sélectionnez le dossier ou le fichier à supprimer définitivement.

   La suppression de fichiers système peut entraîner des échecs dans le système d'exploitation.

5. Sélectionnez la méthode de suppression des données souhaitée dans la liste déroulante **Méthode de suppression des données**.

   Pour supprimer les données d'un périphérique SSD, USB ou de disques réseau, il est conseillé d'utiliser la méthode **Suppression rapide** ou **GOST R 50739-95**. Les autres méthodes de suppression peuvent endommager votre périphérique SSD ou USB ou encore votre disque réseau.

6. Cliquez sur le bouton **Supprimer**.

7. Dans la fenêtre de confirmation de la suppression qui s'ouvre, cliquez sur le bouton **Oui**. 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 dossier à supprimer, cliquez sur le bouton **Terminer**.

SUPPRESSION DES DONNEES NON UTILISEES

Cette section contient les informations sur la suppression des fichiers temporaires et non utilisés.

DANS CETTE SECTION

A PROPOS DE LA 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, tout ces fichiers ne sont pas automatiquement supprimés. Kaspersky Small Office Security 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.

PROCEDURE DE SUPPRESSION DES DONNEES NON UTILISEES

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

1. Ouvrez la fenêtre principale de l'application.
2. Le lien **Afficher les outils complémentaires**, situé dans la partie inférieure de la fenêtre principale, permet d'ouvrir la fenêtre **Outils**.
3. Dans la fenêtre ouverte à l'aide du lien **Suppression des données non utilisées**, lancez l'Assistant de suppression des données non utilisées.

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. Guide de démarrage 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 de données non utilisées, la fenêtre avec la liste des actions s'ouvre.

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 décocher les cases sélectionnées par défaut. Cela pourrait créer des menaces pour 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 d'exploitation. Afin de pouvoir supprimer ces fichiers, l'Assistant propose de redémarrer le système d'exploitation.

Etape 5. Fin de l'Assistant

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

SAUVEGARDE DES DONNEES

Cette section contient les informations sur la sauvegarde des données.

DANS CETTE SECTION

A PROPOS DE LA SAUVEGARDE DES DONNEES

La sauvegarde des données est indispensable pour protéger vos données contre la perte suite à une panne ou un vol de matériel, contre la suppression accidentelle ou contre la perte suite aux actions d'individus malintentionnés.

Pour exécuter la sauvegarde des données, il faut créer (cf. section "Création d'une tâche de la sauvegarde" à la page 84) et lancer (cf. section "Lancement de la tâche de la sauvegarde" à la page 87) la tâche de la sauvegarde. La tâche peut être lancée automatiquement selon la planification ou manuellement. L'application permet de consulter les informations sur l'exécution de ces tâches.

Il est conseillé d'enregistrer les copies de sauvegarde des données sur les disques amovibles ou dans la Sauvegarde en ligne.

Pour créer des copies de sauvegarde, Kaspersky Small Office Security permet d'utiliser les types des stockages suivants :

- disque local ;
- disque amovible (par exemple, un disque dur externe) ;
- disque réseau ;
- serveur FTP ;
- Sauvegarde en ligne (cf. section "A propos de la Sauvegarde en ligne" à la page 88).

CREATION D'UNE TACHE DE SAUVEGARDE

Pour créer une tâche de sauvegarde, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Cliquez sur le bouton **Sauvegardes**.

3. Dans la fenêtre **Sauvegardes** qui s'ouvre, procédez comme suit :

   - cliquez sur le bouton **Sélectionner les fichiers pour la sauvegarde** si la tâche de sauvegarde n'a pas encore été créée ;

   - cliquez sur le bouton **Créer des copies de sauvegarde d'autres fichiers** si vous avez déjà une tâche de sauvegarde et que vous souhaitez en créer une nouvelle.

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

   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.

Sélection des fichiers

A cette étape de l'Assistant sélectionnez le type de fichiers et indiquez les dossiers pour lesquels vous voulez créer des copies de sauvegarde :

- Pour une configuration rapide, choisissez un des types de fichiers prédéfinis (fichiers des dossiers Mes documents et Bureau, photos et images, films et vidéos, fichiers musicaux). Lors de la confirmation de cette option, l'Assistant passe automatiquement à l'étape **Sélection du stockage des copies de sauvegarde**.

- Sélectionnez l'option **Créer des copies de sauvegarde des fichiers dans les dossiers indiqués** pour indiquer manuellement les dossiers pour lesquels vous voulez créer des copies de sauvegarde.

Choix des dossiers pour la sauvegarde

Si à l'étape précédente de l'Assistant vous avez sélectionné l'option **Créer des copies de sauvegarde des fichiers dans les dossiers indiqués**, cliquez sur le bouton **Ajouter un dossier** et sélectionnez le dossier dans la fenêtre **Sélection du dossier** qui s'ouvre ou faites glisser le dossier dans la fenêtre de l'application.

Cochez la case **Indiquer en supplément les types de fichiers** si vous voulez spécifier dans les dossiers indiqués les types de fichiers pour lesquels la création de copies de sauvegarde est requise.

Choix des types de fichiers pour la sauvegarde

Si à l'étape précédente de l'Assistant vous avez coché la case **Indiquer en supplément les types de fichiers**, dans la fenêtre suivante cochez les cases en regard des types des fichiers pour lesquels vous voulez créer des copies de sauvegarde.

Sélection du stockage des copies de sauvegarde

A cette étape, sélectionnez le stockage des copies de sauvegarde :

- **Sauvegarde en ligne**. Sélectionnez cette option si vous voulez conserver les copies de sauvegarde dans la Sauvegarde en ligne Dropbox. Avant l'utilisation, il faut activer la Sauvegarde en ligne (cf. section "Activation de la Sauvegarde en ligne" à la page 88). Lors de la création de copies de sauvegarde à l'aide du Stockage en ligne, Kaspersky Small Office Security ne crée pas de copies de sauvegarde des types de données soumis aux restrictions des règles d'utilisation de Dropbox.

- **Disque local**. Si vous voulez conserver les copies de sauvegarde sur un disque local, sélectionnez le disque local souhaité dans la liste.

- **Stockage réseau**. Si vous voulez conserver les copies de sauvegarde dans le stockage réseau, sélectionnez le stockage réseau souhaité dans la liste.

- **Disque amovible**. Si vous voulez conserver les copies de sauvegarde sur un disque amovible, sélectionnez le disque amovible souhaité dans la liste.

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.

Pour ajouter le stockage réseau, procédez comme suit :

1. En cliquant sur le lien **Ajouter le stockage réseau**, ouvrez la fenêtre **Ajout du stockage réseau** et sélectionnez le type de stockage réseau : disque réseau ou serveur FTP.
2. Indiquez les données nécessaires à la connexion au stockage réseau.
3. Cliquez sur le bouton **OK**.

Pour ajouter un disque amovible en tant que stockage de copies de sauvegarde, procédez comme suit :

1. Utilisez le lien **Connecter le stockage existant** pour ouvrir la fenêtre **Connexion au stockage**.
2. Sélectionnez la section **Disque amovible**.
3. Cliquez sur le bouton **Parcourir** puis dans la fenêtre qui s'ouvre, indiquez le disque amovible sur lequel vous souhaitez conserver les copies de sauvegarde des fichiers.

Cochez la case **Utiliser la configuration avancée du stockage** si vous voulez configurer les paramètres de conservation des fichiers, tels que le nombre de versions conservées des copies de sauvegarde et le temps de conservation des versions des copies de sauvegarde.

Programmation de la sauvegarde

A cette étape de l'Assistant exécutez l'une des actions suivantes :

- Etablissez la planification des lancements de la tâche de sauvegarde si vous souhaitez lancer la tâche automatiquement.
- Dans la liste déroulante **Lancer la sauvegarde**, sélectionnez l'option **à la requête** si vous souhaitez lancer la tâche vous-même.

Saisie du mot de passe pour protéger les copies de sauvegarde

Cochez la case **Activer la protection par mot de passe** et remplissez les champs **Mot de passe pour accéder aux copies de sauvegarde** et **Confirmation du mot de passe** si vous voulez protéger par un mot de passe l'accès aux copies de sauvegarde.

Paramètres de conservation des copies de sauvegarde des fichiers

Cette étape est accessible si vous avez coché la case **Utiliser la configuration élargie du stockage** à l'étape précédente.

Configurer les paramètres de sauvegarde des fichiers :

- Cochez la case **Limiter le nombre de versions des copies de sauvegarde** puis dans le champ **Nombre de versions conservées des copies de sauvegarde**, indiquez le nombre de versions des copies de sauvegarde d'un fichier qui doivent être conservées.
- Cochez la case **Limiter la durée de conservation des versions des copies de sauvegarde** puis dans le champ **Période de conservation de la version de la copie de sauvegarde**, indiquez le nombre de jours durant lesquels chaque version du fichier doit être conservée.

Saisie du nom de la tâche de sauvegarde

Cette étape requiert l'exécution des actions suivantes :

1. Saisissez le nom de la tâche de sauvegarde.
2. Cochez la case **Lancer la sauvegarde à la fin de l'Assistant** si vous souhaitez que la sauvegarde commence automatiquement au terme de l'exécution de l'Assistant.

Fin de l'Assistant

Cliquez sur le bouton **Terminer**.

La tâche de sauvegarde sera créée. La tâche créée est affichée dans la fenêtre **Sauvegardes**.

LANCEMENT D'UNE TACHE DE SAUVEGARDE

Pour lancer une tâche de sauvegarde, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Cliquez sur le bouton **Sauvegardes**.
3. Dans la liste déroulante **Sauvegardes**, sélectionnez une tâche de sauvegarde et cliquez sur le bouton **Lancer la copie**.

La tâche de sauvegarde sera lancée.

RESTAURATION DES DONNEES DEPUIS LA COPIE DE SAUVEGARDE

Pour restaurer des données depuis une copie de sauvegarde, procédez comme suit :

1. Ouvrez la fenêtre principale des applications.
2. Cliquez sur le bouton **Sauvegardes**.
3. Exécutez une des actions suivantes :
   - Cliquez sur le bouton **Restaurer les fichiers** à côté de la tâche de sauvegarde souhaitée.
   - A l'aide du lien **Administration des stockages** ouvrez la fenêtre et cliquez sur le bouton **Restaurer les fichiers** à côté du stockage de copies de sauvegarde souhaité.
4. Si le mot de passe a été spécifié lors de la création d'une copie de sauvegarde, indiquez ce mot de passe dans la fenêtre **Saisissez le mot de passe pour accéder au stockage**.
5. Dans la liste déroulante **Date/heure de la copie**, sélectionnez la date et l'heure de création de la copie de sauvegarde.
6. Cochez les cases en regard des dossiers que vous souhaitez restaurer.
7. Si vous souhaitez restaurer uniquement des types de fichiers spécifiques, sélectionnez ces types de fichiers dans la liste déroulante **Type de fichiers**.
8. Cliquez sur le bouton **Restaurer les fichiers sélectionnés**.

   La fenêtre **Restauration des fichiers depuis la copie de sauvegarde** s'ouvre.

9. Sélectionnez une de deux options proposées :

   - **Dans le dossier d'origine**. Si cette option est sélectionnée, l'application restaure les données dans le dossier d'origine.

   - **Dans le dossier indiqué**. Si cette option est sélectionnée, l'application restaure les données dans le dossier indiqué. Cliquez sur le bouton **Parcourir** pour sélectionner le dossier dans lequel restaurer les données.

10. Dans la liste déroulante **Lors de la correspondance des noms des fichiers**, sélectionnez l'action que l'application exécutera si le nom du fichier en cours de restauration coïncide avec le nom du fichier se trouvant dans le dossier indiqué pour la restauration.

11. Cliquez sur le bouton **Restaurer**.

    Les fichiers sélectionnés pour la restauration seront restaurés depuis la copie de sauvegarde et enregistrés dans le dossier indiqué.

A PROPOS DE LA SAUVEGARDE EN LIGNE

L'application Kaspersky Small Office Security permet d'enregistrer les copies de sauvegarde de vos données dans la Sauvegarde en ligne sur un serveur distant, en utilisant le service Web Dropbox.

Pour utiliser le Stockage en ligne, il est nécessaire de :

- S'assurer que l'ordinateur est connecté à Internet.

- Créer un compte sur le site Internet du prestataire de services d'enregistrement de données en ligne.

- Activer la Sauvegarde en ligne.

Vous pouvez utiliser le même compte utilisateur Dropbox pour conserver dans une seule Sauvegarde en ligne les données de divers périphériques dotés de l'application Kaspersky Small Office Security.

Le volume du Stockage en ligne est défini par le prestataire de services d'enregistrement de données en ligne, le service Web Dropbox. Vous trouverez de plus amples informations sur les conditions d'utilisation du service sur le site de Dropbox https://www.dropbox.com/.

ACTIVATION DU STOCKAGE EN LIGNE

Pour activer la Sauvegarde en ligne, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.

2. Cliquez sur le bouton **Sauvegardes**.

3. Dans la fenêtre **Sauvegardes** qui s'ouvre, procédez comme suit :

   - cliquez sur le bouton **Sélectionner les fichiers pour la sauvegarde** si la tâche de sauvegarde n'a pas encore été créée ;

   - cliquez sur le bouton **Créer des copies de sauvegarde d'autres fichiers** si vous disposez déjà d'une tâche de sauvegarde.

   L'Assistant de création d'une tâche de sauvegarde (cf. section "Création d'une tâche de la sauvegarde" à la page 84) sera lancé.

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

5. Dans la fenêtre de sélection du stockage, choisissez la Sauvegarde en ligne, puis cliquez sur **Activer**.

   Pour créer le Stockage en ligne, une connexion à Internet est requise.

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

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

   - Si vous ne possédez pas de compte sur le site Internet Dropbox, créez-en un maintenant.

   - Si vous avez un compte sur le site Internet Dropbox, saisissez vos données d'identification.

7. Pour terminer l'activation du Stockage en ligne, confirmez que Kaspersky Small Office Security peut utiliser votre compte Dropbox pour sauvegarder les données et pour restaurer les données depuis la copie de sauvegarde. Kaspersky Small Office Security va placer les copies de sauvegarde des données dans un dossier séparé créé dans le dossier d'enregistrement des applications de Dropbox.

   Une fois l'activation du Stockage 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 le Stockage en ligne activé.

ENREGISTREMENT DES DONNEES DANS LES COFFRES-FORTS

Cette section contient les informations sur la protection des données à l'aide des coffres-forts.

DANS CETTE SECTION

A PROPOS DU COFFRE-FORT

Les coffres-forts sont conçus pour protéger vos données confidentielles contre tout accès non autorisé. Le *coffre-fort* est un stockage de données sur votre ordinateur que vous pouvez ouvrir ou fermer à l'aide d'un mot de passe que vous seul connaissez. Pour modifier les fichiers enregistrés dans un coffre-fort fermé, il faut saisir le mot de passe.

Si vous perdez ou oubliez le mot de passe, il sera impossible de restaurer les données.

Pour créer des coffres-forts dans Kaspersky Small Office Security, les algorithmes de chiffrement de données suivants sont utilisées : AES XTS 256 avec une longueur efficace de la clé de 56 bits.

PLACEMENT DES FICHIERS DANS UN COFFRE-FORT

Pour placer des fichiers dans un coffre-fort, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Cliquez sur le bouton **Coffres-forts virtuels**.
3. Dans la fenêtre **Coffres-forts virtuels** qui s'ouvre, effectuez une des opérations suivantes :
   - Cliquez sur le bouton **Créer un nouveau coffre-fort** si vous n'en avez pas encore.
   - Cliquez sur le bouton **Créer un coffre-fort** si vous avez déjà créé des coffres-forts.
4. A l'aide du lien **Ajouter les fichiers et les dossiers dans le coffre-fort**, ouvrez l'Explorateur et indiquez les fichiers à placer dans le coffre-fort.

   Les fichiers sélectionnés s'affichent dans la fenêtre **Coffres-forts virtuels**.
5. Cliquez sur le bouton **Poursuivre**.
6. Saisissez le nom du coffre-fort et indiquez son emplacement ou utilisez les valeurs de ces paramètres par défaut.
7. Pour obtenir un accès rapide au coffre-fort, cochez la case **Créer un raccourci vers le coffre-fort sur le bureau**.

8. Cliquez sur le bouton **Poursuivre**.
9. Remplissez les champs **Mot de passe** et **Confirmation du mot de passe** et cliquez sur le bouton **Poursuivre**.
10. Sélectionnez l'action à effectuer sur les copies d'origine des fichiers en dehors du coffre-fort :
    - Pour supprimer les copies d'origine des fichiers en dehors du coffre-fort, cliquez sur le bouton **Supprimer**.
    - Pour conserver les copies d'origine des fichiers en dehors du coffre-fort, cliquez sur le bouton **Ignorer**.
11. Cliquez sur le bouton **Terminer**.

    Le coffre-fort que vous avez créé s'affiche dans la liste **Vos coffres-forts**.
12. Pour fermer le coffre-fort, cliquez sur le bouton **Fermer le coffre-fort**.

    Les données dans le coffre-fort fermé seront accessibles uniquement après la saisie du mot de passe.

OBTENTION D'ACCES AUX FICHIERS ENREGISTRES DANS UN COFFRE-FORT

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

1. Ouvrez la fenêtre principale de l'application.
2. Cliquez sur le bouton **Coffres-forts virtuels**.
3. Dans la fenêtre **Coffres-forts virtuels** qui s'ouvre, cliquez sur le bouton **Ouvrir le coffre-fort** à côté du coffre-fort souhaité.
4. Saisissez le mot de passe et cliquez sur le bouton **Ouvrir le coffre-fort dans l'Explorateur**.

Les fichiers enregistrés dans le coffre-fort s'afficheront dans la fenêtre de l'Explorateur. Vous pouvez apporter les modifications nécessaires aux fichiers et refermer le coffre-fort.

Pour ouvrir les coffres-forts créés dans la version précédente de l'application, vous devez exécuter une conversion de l'ancien format des coffres-forts vers le nouveau format. L'application vous proposera elle-même d'exécuter une conversion lors de la tentative d'ouverture d'un coffre-fort dans Kaspersky Small Office Security.

La conversion des coffres-forts vers un nouveau format dépend de la taille du coffre-fort et peut durer un certain temps.

PROTECTION DE L'ACCES A L'ADMINISTRATION DE KASPERSKY SMALL OFFICE SECURITY A L'AIDE DU MOT DE PASSE

Il peut arriver que plusieurs personnes aux connaissances informatiques différentes utilisent le même ordinateur. L'accès sans restriction de différents utilisateurs à l'administration de Kaspersky Small Office Security et à ses paramètres peut entraîner 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 qui ne pourront être exécutées qu'après la saisie de ce mot de passe :

- configuration des paramètres de l'application ;
- arrêt de l'application ;
- suppression de l'application.

Pour protéger l'accès à Kaspersky Small Office Security 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 la partie inférieure de la fenêtre principale de l'application pour accéder à la section **Configuration**.
3. Dans la partie gauche de la fenêtre, sélectionnez la section **Général**, puis cliquez sur le lien **Activer la protection par mot de passe** afin d'ouvrir la fenêtre **Protection par mot de passe**.
4. Dans la fenêtre qui s'ouvre, remplissez les champs **Nouveau mot de passe** et **Confirmation du mot de passe**.
5. Indiquez dans le groupe de paramètres **Zone d'action du mot de passe** les actions qui ne pourront être exécutée qu'après la saisie du mot de passe.

Il est impossible de récupérer un mot de passe oublié. Si vous oubliez un mot de passe, il faudra contacter le Support Technique pour pouvoir accéder aux paramètres de Kaspersky Small Office Security.

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.

Pendant la suspension de la protection ou pendant la désactivation de Kaspersky Small Office Security, la fonction de contrôle de l'activité des applications en cours sur votre ordinateur est activée. Les informations sur les résultats de contrôle de l'activité des applications sont enregistrées dans le système d'exploitation. Au lancement suivant ou lors de la reprise de la protection, Kaspersky Small Office Security utilise ces informations pour protéger votre ordinateur contre les actions malveillantes ayant pu être exécutées lors de la suspension de la protection ou lors de la désactivation de Kaspersky Small Office Security. L'enregistrement des informations sur les résultats de contrôle d'activité des applications n'est pas limité selon le temps. Ces informations sont supprimées en cas de suppression de Kaspersky Small Office Security de votre ordinateur.

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 9. 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 pour 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 rétablir la protection de l'ordinateur,

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

RESTAURATION DES PARAMETRES STANDARDS DE FONCTIONNEMENT DE L'APPLICATION

Vous pouvez à tout moment restaurer les paramètres de fonctionnement de Kaspersky Small Office Security 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 la protection. Lors de la restauration du niveau de protection recommandé, vous pouvez choisir d'enregistrer les valeurs des paramètres configurés auparavant pour les modules de l'application.

Pour lancer l'Assistant de configuration de l'application, procédez comme suit :

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

   La section **Configuration** apparaît dans la fenêtre.
3. Sélectionnez la section **Général**.

   La fenêtre affiche les paramètres de configuration de Kaspersky Small Office Security.
4. Dans la partie inférieure de la fenêtre, dans la liste déroulante **Gestion des paramètres**, sélectionnez l'élément **Restaurer les paramètres**.

Examinons en détails les étapes de l'Assistant.

Etape 1. Guide de démarrage 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 Small Office Security dont les paramètres ont été modifiés par l'utilisateur ou assimilés par Kaspersky Small Office Security durant l'apprentissage 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).

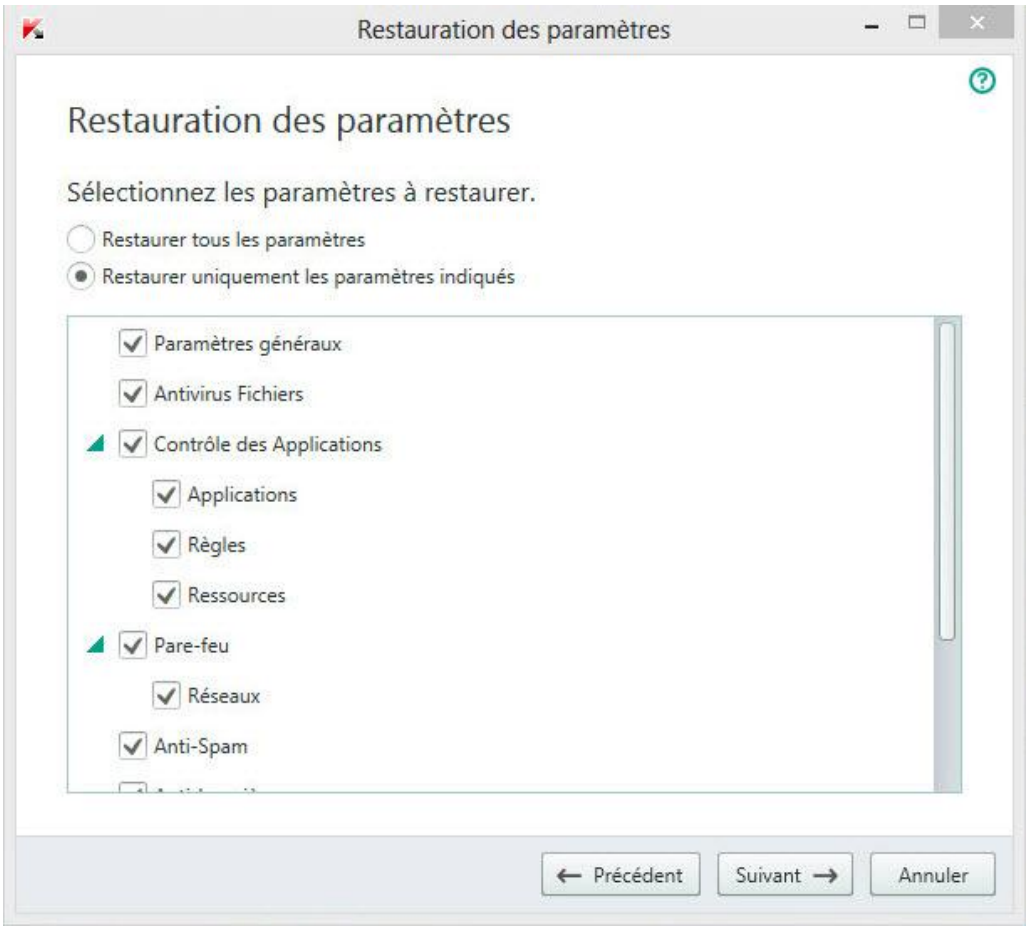


Illustration 10. Fenêtre Restauration des paramètres

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 composés pendant l'utilisation de Kaspersky Small Office Security 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 d'exploitation

Cette étape exécute la recherche 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 d'exploitation.

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**.

CONSULTATION DU RAPPORT SUR L'UTILISATION DE L'APPLICATION

Kaspersky Small Office Security génère des rapports sur le fonctionnement de chaque module de protection. Ce rapport donne des données statistiques sur le fonctionnement de l'application (par exemple, nombre d'objets malveillants détectés et neutralisés pendant la période indiquée, nombre de fois que l'application a été mise à jour, nombre de messages non sollicités détectés, etc.). Les rapports sont réalisés en utilisant le chiffrement.

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

1. Ouvrez la fenêtre principale de l'application.
2. Le lien **Afficher les outils complémentaires**, situé dans la partie inférieure de la fenêtre principale, permet d'ouvrir la fenêtre **Outils**.
3. Dans la fenêtre **Outils** à l'aide du lien **Rapport**, ouvrez la fenêtre **Rapports**.

   La fenêtre **Rapports** reprend les rapports sur le fonctionnement de l'application pour la journée en cours (partie gauche de la fenêtre) et pour la période définie (partie droite de la fenêtre).
4. Si vous souhaitez consulter un rapport détaillé sur le fonctionnement de l'application, ouvrez la fenêtre **Rapports détaillés** via le lien **Rapports détaillés** situé dans la partie supérieure de la fenêtre **Rapports**.

La fenêtre **Rapports détaillés** présente les données sous forme d'un tableau. Pour faciliter la lecture du tableau, vous pouvez regrouper les entrées du tableau selon différents critères.

APPLICATION DES PARAMETRES DE L'APPLICATION SUR UN AUTRE ORDINATEUR

En configurant l'application, vous pouvez appliquer les paramètres de son fonctionnement à une application Kaspersky Small Office Security installée sur un autre ordinateur. Ainsi, l'application sera configurée de la même manière sur les deux ordinateurs.

Les paramètres de fonctionnement de l'application sont enregistrés dans le fichier de configuration que vous pouvez transmettre d'un ordinateur vers un autre.

Le transfert des paramètres de Kaspersky Small Office Security d'un ordinateur à un autre s'effectue en trois étapes :

1. Enregistrement des paramètres de l'application dans le fichier de configuration.
2. Le transfert du fichier de configuration vers un autre ordinateur (par exemple, par courrier électronique ou à l'aide d'un support amovible).
3. L'importation des paramètres depuis le fichier de configuration vers l'application installée sur un autre ordinateur.

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

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre à l'aide du lien **Configuration**, ouvrez la fenêtre **Configuration**.
3. Dans la fenêtre **Configuration**, sélectionnez la section **Général**.
4. Dans la liste déroulante **Gestion des paramètres**, sélectionnez l'option **Exporter les paramètres**.

   La fenêtre **Enregistrer sous** s'ouvre.
5. Définissez le nom du fichier de configuration et cliquez sur le bouton **Enregistrer**.

Les paramètres de l'application seront enregistrés dans le fichier de configuration.

Vous pouvez aussi exporter les paramètres de fonctionnement de l'application à l'aide d'une ligne de commande, en utilisant la commande : `avp.com EXPORT <nom_du_fichier>`.

Pour importer les paramètres dans l'application installée sur un autre ordinateur, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application Kaspersky Small Office Security installée sur un autre ordinateur.
2. Dans la partie inférieure de la fenêtre à l'aide du lien **Configuration**, ouvrez la fenêtre **Configuration**.
3. Dans la fenêtre **Configuration**, sélectionnez la section **Général**.
4. Dans la liste déroulante **Gestion des paramètres**, sélectionnez l'élément **Importer les paramètres**.

   La fenêtre **Ouvrir** s'ouvre.
5. Indiquez le fichier de configuration et cliquez sur le bouton **Ouvrir**.

Les paramètres seront importés dans l'application installée sur un autre ordinateur.

PARTICIPATION A KASPERSKY SECURITY NETWORK (KSN)

Afin d'améliorer l'efficacité de la protection de votre ordinateur, Kaspersky Small Office Security utilise la protection cloud. La protection cloud est réalisée à l'aide de l'infrastructure Kaspersky Security Network qui utilise des données obtenues auprès d'utilisateurs dans le monde entier.

Kaspersky Security Network (KSN) est un ensemble de services en ligne qui permet d'accéder à la Base des connaissances de Kaspersky Lab sur la réputation des fichiers, des sites et des applications. Grâce aux données du Kaspersky Security Network, Kaspersky Small Office Security peut réagir plus rapidement aux menaces inconnues, améliorer l'efficacité de certains modules et réduire la probabilité de faux positifs.

La participation des utilisateurs à Kaspersky Security Network permet à Kaspersky Lab de recueillir efficacement des informations sur les nouvelles menaces et leurs sources, de développer des moyens de neutralisation et de réduire le nombre de faux positifs. La participation à Kaspersky Security Network vous donne accès aux données sur la réputation des applications et des sites Internet.

Si vous participez à Kaspersky Security Network, vous envoyez à Kaspersky Lab en mode automatique des informations sur la configuration de votre système d'exploitation et sur l'heure de début et de fin des processus de Kaspersky Small Office Security (cf. section "A propos des données" à la page 34).

DANS CETTE SECTION

ACTIVATION ET DESACTIVATION DE LA PARTICIPATION A KASPERSKY SECURITY NETWORK

La participation à Kaspersky Security Network est volontaire. Vous pouvez activer ou désactiver l'utilisation de Kaspersky Security Network pendant l'installation de Kaspersky Small Office Security et/ou à tout moment après l'installation de l'application.

Pour activer ou désactiver la participation à Kaspersky Security Network, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Cliquez sur le lien **Configuration** dans la partie inférieure de la fenêtre principale de l'application pour ouvrir la fenêtre **Configuration**.
3. Dans la section **Avancé**, sélectionnez le groupe **Kaspersky Security Network**.

   Cette fenêtre affiche les informations relatives à Kaspersky Security Network (KSN) ainsi que les paramètres de participation à KSN.
4. Les boutons **Activer**/**Désactiver** permettent d'activer ou de désactiver la participation à Kaspersky Security Network :

   - si vous voulez participer à Kaspersky Security Network, cliquez sur **Activer** ;
   - si vous ne voulez pas participer à Kaspersky Security Network, cliquez sur **Désactiver**.

VERIFICATION DE LA CONNEXION A KASPERSKY SECURITY NETWORK

La connexion à Kaspersky Security Network peut être absente pour une des raisons suivantes :

- Vous ne participez pas à Kaspersky Security Network.
- Votre ordinateur n'est pas connecté à Internet.
- L'état actuel de la clé ne permet pas d'effectuer la connexion à Kaspersky Security Network.

L'état actuel de la clé s'affiche dans la fenêtre **Licence**.

Pour vérifier la connexion à Kaspersky Security Network, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Cliquez sur le lien **Configuration** dans la partie inférieure de la fenêtre principale de l'application pour ouvrir la fenêtre **Configuration**.
3. Dans la section **Avancé**, choisissez la sous-section **Kaspersky Security Network**.

La fenêtre indique l'état de la participation à Kaspersky Security Network.

UTILISATION DE L'APPLICATION DEPUIS LA LIGNE DE COMMANDE

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

Syntaxe de la ligne de commande :

```
avp.com <commande> [paramètres]
```

Pour consulter l'aide sur la syntaxe de la commande, la commande suivante est prévue :

```
avp.com [ /? | HELP ]
```

Cette commande permet d'obtenir la liste complète des commandes accessibles pour travailler avec Kaspersky Small Office Security via la ligne de commande.

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

```
avp.com <commande> /?
avp.com HELP <commande>
```

Il faut faire appel à l'application via la ligne de commande depuis le dossier d'installation de l'application ou en indiquant le chemin complet à avp.com.

CONTACTER LE SUPPORT TECHNIQUE

Cette section reprend les informations sur les différentes méthodes d'obtention de l'assistance 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 12), 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/support/rules).

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

- Par téléphone. Vous pouvez contacter les experts du Support Technique en France.
- Envoyer une demande depuis le portail Centre d'administration de Kaspersky Small Office Security. Cette méthode permet de contacter les experts du Support Technique via un formulaire.

L'assistance technique est uniquement accessible aux utilisateurs qui ont acheté une licence d'utilisation de l'application. Les utilisateurs des versions d'évaluation n'ont pas droit à l'assistance technique.

ASSISTANCE TECHNIQUE PAR TELEPHONE

Si vous êtes confronté à un problème que vous ne parvenez pas à résoudre, vous pouvez contacter les experts du Support Technique francophones (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/fr/support/rules). Ceci permettra à nos experts de vous venir en aide le plus vite possible.

OBTENTION D'ASSISTANCE TECHNIQUE DANS INTERNET

Pour obtenir l'assistance technique dans Internet, il faut s'inscrire sur la page d'enregistrement (https://my.kaspersky.com/fr/). Pour ce faire, il faut indiquer l'adresse du courrier électronique et le mot de passe.

Sur le site Internet du Support Technique, vous pouvez exécuter les actions 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 à votre question sur le site Internet ou par 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 au Laboratoire d'étude des virus des demandes de recherche sur des fichiers suspects ou des ressources Internet. Vous pouvez aussi le contacter pour les cas de faux positifs de Kaspersky Small Office Security sur les fichiers ou ressources Internet que vous ne considérez pas comme dangereux.

COLLECTE D'INFORMATIONS POUR LE SUPPORT TECHNIQUE

Après avoir signalé un problème aux experts du Support Technique, ceux-ci 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 Support Technique peuvent également vous demander de créer un fichier de trace. Le fichier de trace 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 à la recherche d'un code malveillant, de rechercher la présence 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.

Pour une assistance plus efficace dans le cas d'apparition des questions concernant l'utilisation de l'application, les experts du Support Technique peuvent vous demander de modifier les paramètres de l'application dans les buts de mise au point lors des travaux de diagnostic. Pour ce faire, l'exécution des actions suivantes peut être requise :

- Activer la fonction de collecte des informations diagnostiques élargies.
- Exécuter une configuration plus fine (inaccessible via les moyens standards de l'interface utilisateur) d'utilisation des modules spécifiques de l'application.

- Modifier les paramètres de conservation et d'envoi des informations diagnostiques récoltées.
- Configurer l'interception et l'enregistrement du trafic réseau dans un fichier.

Toutes les informations nécessaires à l'exécution des actions citées (la description de la suite des étapes, les paramètres modifiables, les fichiers de configuration, les scripts, les possibilités complémentaires de la ligne de commande, les modules de mise au point, les utilitaires spécialisés, etc.), ainsi que la composition des données, récoltées dans les buts de mise au point, seront vous communiquées par les experts du Support Technique. Les informations diagnostiques élargies récoltées sont enregistrées sur l'ordinateur de l'utilisateur. L'envoi automatique des données récoltées à Kaspersky Lab n'est pas exécuté.

Les actions citées ci-dessus doivent être exécutées uniquement sous l'administration des experts du Support Technique à l'aide de leurs instructions. La modification indépendante des paramètres d'utilisation de l'application à l'aide des moyens non décrits dans le Manuel de l'administrateur ou dans les recommandations des experts du Support Technique peut amener au ralentissement et aux échecs du système d'exploitation, à la baisse du niveau de protection de l'ordinateur, ainsi qu'à la perturbation de l'accessibilité et de l'intégrité des informations traitées.

DANS CETTE SECTION

CREATION D'UN RAPPORT D'ETAT DU SYSTEME D'EXPLOITATION

Pour créer un rapport d'état du système d'exploitation, 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 lien **Outils de support**.

   La fenêtre **Outils de support** s'ouvre.
4. Dans la fenêtre qui s'ouvre, cliquez sur le lien **Créer un rapport sur le système d'exploitation**.

Le rapport d'état du système d'exploitation est généré au format HTML et XML et il est enregistré dans l'archive sysinfo.zip. Une fois la collecte d'informations sur le système d'exploitation 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 afin d'ouvrir la fenêtre **Support Technique**.
3. Dans la fenêtre qui s'ouvre, cliquez sur le lien **Outils de support**.

   La fenêtre **Outils de support** s'ouvre.
4. Dans la fenêtre qui s'ouvre, cliquez sur le lien **Consulter le rapport**.

   La fenêtre du Navigateur Microsoft Windows s'ouvre.
5. Dans la fenêtre qui s'ouvre, ouvrez l'archive sysinfo.zip qui contient les fichiers du rapport.

ENVOI DES FICHIERS DE DONNEES

Une fois que les fichiers de traçage et le rapport d'état du système d'exploitation ont été créés, il faut les envoyer aux experts du Support Technique de Kaspersky Lab.

Pour charger les fichiers sur le serveur du Support Technique, il faut obtenir un numéro de requête. Ce numéro est accessible sur le portail Centre d'administration de Kaspersky Small Office Security en cas de présence d'une demande active.

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 lien **Outils de support**.

   La fenêtre **Outils de support** s'ouvre.
4. Dans la fenêtre qui s'ouvre, cliquez sur le lien **Envoyer le rapport 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.
6. Cliquez sur le bouton **Envoyer le rapport**.

Les fichiers de données sélectionnés seront compressés 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 le portail Centre d'administration de Kaspersky Small Office Security.

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 lien **Outils de support**.
4. La fenêtre **Outils de support** s'ouvre.
5. Dans la fenêtre qui s'ouvre, cliquez sur le lien **Envoyer le rapport au Support Technique**.

   La fenêtre **Envoi du rapport** s'ouvre.
6. Sélectionnez les types de données à envoyer :

   - **Informations relatives au système d'exploitation**. Cochez cette case si vous voulez envoyer au Support Technique des informations sur le système d'exploitation de votre ordinateur.
   - **Données collectées pour analyse**. Cochez cette case si vous voulez envoyer au Support Technique des fichiers de traçage de l'application. Le lien **<nombre de> fichiers>, <volume de données>** ouvre la fenêtre **Données collectées pour analyse**. Cochez les cases en regard des fichiers de traçage à envoyer.
7. Cliquez sur le lien **Enregistrer le rapport**.

   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 le portail Centre d'administration de Kaspersky Small Office Security.

A PROPOS DE LA COMPOSITION ET DE LA CONSERVATION DES FICHIERS DE TRACE

Les fichiers de trace sont conservés sur votre ordinateur sous forme protégée pendant toute la période d'utilisation de l'application et sont définitivement supprimés lors de la suppression de l'application.

Les fichiers de trace sont conservés dans le dossier ProgramData\Kaspersky Lab.

Les fichiers de trace ont les noms suivants : `KAV<numéro de version_dateXX.XX_timeXX.XX_pidXXX.><type de fichier de trace>.log.enc1`.

Tous les fichiers de trace contiennent les données générales suivantes :

- Heure de l'événement.
- Numéro de flux d'exécution.
- Module de l'application à l'origine de l'événement.
- Degré d'importance de l'événement (information, avertissement, critique, erreur).
- Description de l'événement d'exécution de la commande du module de l'application et du résultat de l'exécution de cette commande.

Composition des fichiers de trace SRV.log, GUI.log et ALL.log

Les informations suivantes peuvent être enregistrées dans les fichiers de trace SRV.log et GUI.log :

- Les données personnelles, y compris le nom, le prénom et le patronyme, si ces données font partie du chemin d'accès aux fichiers sur l'ordinateur local.
- Le nom d'utilisateur et le mot de passe s'ils sont transmis sous forme non protégée. Ces données peuvent être enregistrées dans les fichiers de trace lors de l'analyse du trafic Internet. Le trafic est enregistré dans les fichiers de trace uniquement depuis trafmon2.ppl.
- Le nom d'utilisateur et le mot passe, les fichiers cookies, s'ils apparaissent dans les en-têtes du protocole HTTP.
- Le nom du compte pour entrer dans Microsoft Windows s'il fait partie du nom du fichier.
- Votre adresse de courrier électronique ou l'adresse Internet avec le nom du compte et le mot de passe, s'ils apparaissent dans le nom de l'objet détecté.
- Les sites Internet que vous visitez, ainsi que les liens depuis ces sites Internet. Ces données sont enregistrées dans les fichiers de trace quand l'application analyse les sites Internet.
- Le numéro du serveur proxy, le nom de l'ordinateur, le port, l'adresse IP et le nom d'utilisateur saisi lors de l'autorisation sur le serveur proxy. Ces données sont enregistrées dans les fichiers de trace quand l'application utilise un serveur proxy.
- Les adresses IP externes avec lesquelles la connexion depuis votre ordinateur a été établie.
- L'objet du message, l'identificateur, le nom de l'expéditeur et l'adresse de la page Internet de l'expéditeur du message sur le réseau social. Ces données sont enregistrées dans les fichiers de trace si le module Contrôle Internet est activé.
- Les informations sur l'activation de l'application qui peuvent inclure les codes d'activation actuel et précédent, la localisation de l'application, les identificateurs de l'application, du produit, de la personnalisation, la version de l'application, l'identificateur unique généré pour chaque installation unique du système d'exploitation, l'identificateur de l'ordinateur de l'utilisateur, la date et l'heure sur l'ordinateur de l'utilisateur au moment d'activation dans TUC.

Contient les fichiers de trace HST.log, BL.log et Dumpwriter.log

Le fichier de trace HST contient les informations sur la mise à jour des bases et des modules d'application.

Le fichier de trace BL contient les informations sur les événements apparus pendant le fonctionnement de l'application, ainsi que les données nécessaires pour éliminer les incidents au cours du fonctionnement de l'application. Ce fichier est créé si l'application est lancée avec le paramètre avp.exe –bl. Le fichier BL peut aussi comprendre les informations sur l'activation de l'application qui peuvent inclure les codes d'activation actuel et précédent, la localisation de l'application, les identificateurs de l'application, du produit, de la personnalisation, la version de l'application, l'identificateur unique généré pour chaque installation unique du système d'exploitation, l'identificateur de l'ordinateur de l'utilisateur, la date et l'heure sur l'ordinateur de l'utilisateur au moment d'activation dans TUC.

Le fichier de trace dumpwriter.log contient les informations de service nécessaires pour éliminer les incidents apparus lors de l'enregistrement du vidage de la mémoire de l'application.

Le fichier de trace dumpwriter.log contient les informations de service nécessaires pour éliminer les incidents apparus lors de l'enregistrement du vidage de la mémoire de l'application.

Composition des fichiers de trace des plug-ins de l'application

Les fichiers de trace des plug-ins de l'application contiennent les informations suivantes :

- VirtualKeyboard (VKB.log) contient les informations de service sur le fonctionnement du plug-in et les données nécessaires à l'élimination des incidents dans le fonctionnement du plug-in (ce fichier est absent si Kaspersky Small Office Security est installé sur le serveur).

- Online Banking (OB.log) contient les informations de service sur le fonctionnement du plug-in, y compris les informations sur les événements de l'analyse des sites Internet et sur les résultats de cette analyse, sur la connexion avec les adresse IP distantes et sur les paramètres du serveur proxy, ainsi que les fichiers cookie. Le fichier contient aussi les données nécessaires à l'élimination des incidents dans le fonctionnement du plug-in (ce fichier est absent si Kaspersky Small Office Security est installé sur le serveur).

- ContentBlocker (CB.log) contient les informations de service sur le fonctionnement du plug-in, y compris les informations sur les événements de l'analyse des adresses Internet, sur les résultats de l'analyse, sur la connexion avec les adresses IP distantes et sur les paramètres du serveur proxy. Le fichier contient aussi les données nécessaires à l'élimination des incidents dans le fonctionnement du plug-in (ce fichier est absent si Kaspersky Small Office Security est installé sur le serveur).

- Office Anti-Virus (OA.log) contient les informations sur l'analyse des documents Microsoft Office. Ce fichier peut aussi contenir des informations sur le chemin d'accès complet au document ou à l'adresse du site Internet depuis lequel ce document a été téléchargé (ce fichier est absent si Kaspersky Small Office Security est installé sur le serveur).

- Le fichier de trace du plug-in de lancement de la tâche d'analyse depuis le menu contextuel (shellex.dll.log). Contient des informations sur l'exécution de la tâche d'analyse et les données nécessaires pour éliminer les incidents au cours du fonctionnement du plug-in.

- Les fichiers de traçage du plug-in pour Microsoft Outlook® :

  - mcouas.OUTLOOK.EXE. Le plug-in de l'Anti-Spam (ce fichier est absent si l'application Kaspersky Small Office Security est installée sur le serveur de fichier) ;

  - mcou.OUTLOOK.EXE. Le plug-in de l'Antivirus Courrier (ce fichier est absent si l'application Kaspersky Small Office Security est installée sur le serveur de fichier).

  Les fichiers peuvent contenir des parties de messages, y compris des adresses.

- Le fichier de trace du plug-in pour enregistrer les extensions Google Chrome (NativeMessagingHost.log) contient les informations de service sur le fonctionnement du plug-in (ce fichier est absent si l'application Kaspersky Small Office Security est installée sur le serveur de fichier).

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.

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 lien **Outils de support**.

   La fenêtre **Outils de support** s'ouvre.
4. Dans la fenêtre qui s'ouvre, cliquez sur le lien **Exécuter le script**.

   La fenêtre **Exécution du script** 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 **Exécuter**.

L'exécution du script sera lancée.

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

RESTRICTIONS ET AVERTISSEMENTS

Kaspersky Small Office Security présente une série de restrictions n'affectant pas de manière critique l'utilisation de l'application.

Restrictions lors de la mise à jour de la version précédente de l'application

- Lors de la mise à jour de la version précédente de Kaspersky Small Office Security, les paramètres de l'application suivants sont remplacés par les paramètres par défaut : sources des mises à jour, liste des adresses Internet de confiance, paramètres de l'URL Advisor.

- Lors de l'installation de la nouvelle version de Kaspersky Small Office Security par-dessus Kaspersky Small Office Security 1, les objets se trouvant en quarantaine seront perdus, parce que leur format n'est pas pris en charge et ne peut pas être transformé dans un nouveau format. Lors de la mise à jour de l'application depuis la version Kaspersky Small Office Security 2 et Kaspersky Small Office Security 3, il est possible d'exécuter la transformation des objets se trouvant en quarantaine dans un nouveau format.

Restrictions d'utilisation de certains modules et du traitement automatique des fichiers

Le traitement des fichiers infectés est exécuté de manière automatique selon les règles composées par les experts de Kaspersky Lab. Vous pouvez modifier manuellement ces règles. Les règles peuvent être actualisées suite à une mise à jour des bases et des modules d'application. Les règles du Pare-feu, du Contrôle des Applications et du mode Applications de confiance sont aussi mises à jour de manière automatique.

Restrictions de l'analyse des fichiers et des certificats des sites Internet

Lors de l'analyse du fichier ou du certificat du site Internet, l'application peut s'adresser à Kaspersky Security Network pour obtenir des informations. S'il est impossible d'obtenir les données depuis Kaspersky Security Network, l'application prend une décision quant à la sûreté du fichier ou à la validité du certificat en s'appuyant sur les bases antivirus locales.

Restrictions de la fonctionnalité Surveillance du système

La fonctionnalité de réaction aux crypteurs (chiffrement des fichiers de l'utilisateur par un programme malveillant) a des restrictions suivantes :

- Le dossier système Temp est utilisé pour assurer la fonctionnalité. Si le disque système avec le dossier Temp n'a pas assez d'espace pour créer des fichiers temporaires, la protection contre les crypteurs n'est pas accordée. Avec cela, une notification sur la non exécution de la copie (non octroi de la protection) ne s'affiche pas.

- Les fichiers temporaires sont supprimés automatiquement à l'arrêt de Kaspersky Small Office Security ou lors de la désactivation du module Surveillance du système.

- En cas d'arrêt anormal de Kaspersky Small Office Security, les fichiers temporaires ne sont pas supprimés automatiquement. Pour supprimer les fichiers temporaires, il faut purger manuellement le dossier Temp. Pour ce faire, ouvrez la fenêtre **Exécuter** (**Lancement de l'application** dans Windows XP) et dans le champ **Ouvrir** saisissez `%TEMP%`. Cliquez sur le bouton **OK**.

Avertissement sur la collecte d'informations diagnostiques

Les informations diagnostiques sur l'utilisation de l'application que vous récoltez pour le Support Technique sont chiffrées durant la collecte. En cas de nécessité, le chiffrement peut être désactivé.

Restrictions de la fonctionnalité Connexions sécurisées

En raison des restrictions techniques au niveau de la réalisation des algorithmes d'analyse, l'analyse des connexions sécurisées ne prend pas en charge certaines extensions du protocole TLS 1.0 et suivant (notamment, NPN et ALPN). La connexion via ces protocoles peut être limitée. Les navigateurs Internet prenant en charge le protocole SPDY utilisent le protocole HTTP par-dessus TLS à la place de SPDY, même si le serveur avec lequel s'effectue la connexion prend en charge SPDY. Ainsi, le niveau de protection de la connexion ne diminue pas.

Avertissement sur l'utilisation du module Anti-Spam

La fonctionnalité du module de protection Anti-Spam peut être modifiée suite à la modification du fichier de configuration du module Anti-Spam.

Restrictions de la Sauvegarde

La Sauvegarde est soumise aux restrictions suivantes :

- La Sauvegarde en ligne des copies de sauvegarde devient inaccessible en cas de changement du disque dur ou d'ordinateur. Les informations sur le rétablissement de la connexion au Stockage en ligne en cas de changement de matériel sont présentées sur le site Internet du Support Technique de Kaspersky Lab.

- La modification des fichiers de service du stockage des copies de sauvegarde peut entraîner la perte de l'accès au stockage des copies de sauvegarde et l'impossibilité de restaurer vos données.

Restriction de la fonctionnalité Coffres-forts virtuels

Lors de la création d'un coffre-fort dans le système de fichiers FAT32, la taille du fichier du coffre-fort sur le disque ne doit pas dépasser 4 Go.

Particularités de la recherche de rootkits éventuels dans la mémoire du noyau pendant une session de Navigation sécurisée

En cas de détection d'un module suspect pendant une session de Navigation sécurisée, un nouvel onglet contenant une notification sur la détection d'un programme malveillant s'ouvre dans le navigateur. Dans ce cas, il est conseillé de fermer le navigateur et d'exécuter une analyse complète de l'ordinateur.

Particularités de la protection des données du presse-papiers

Kaspersky Small Office Security autorise l'application à communiquer avec le presse-papiers dans les cas suivants :

- Une application avec une fenêtre active tente de placer des données dans le presse-papiers. La fenêtre dans laquelle vous travaillez actuellement est considérée comme active.

- Un processus protégé de l'application tente de placer des données dans le presse-papiers.

- Un processus protégé de l'application ou un processus avec une fenêtre active tente de recevoir des données depuis le presse-papiers.

- Le processus de l'application qui avait précédemment placé ces données dans le presse-papiers tente de les récupérer depuis le presse-papiers.

Avertissement sur la compatibilité avec les applications de Kaspersky Lab

L'application Kaspersky Small Office Security est incompatible avec les applications de Kaspersky Lab suivantes :

- Kaspersky Internet Security (2011, 2012, 2013, 2014, 2015).

- Kaspersky CRYSTAL (2, 3).

- Kaspersky Total Security.
- Kaspersky Small Office Security 1.
- Kaspersky Anti-Virus for Windows Workstation 6.
- Kaspersky Anti-Virus for Windows Server 6.
- Kaspersky Endpoint Protection 8 et 10.

L'application Kaspersky Small Office Security est compatible avec les applications de Kaspersky Lab suivantes :

- Kaspersky Fraud Prevention 2.0 et 2.5
- Kaspersky Password Manager 2.0, 5.0, 7.0.

Particularités de traitement des objets malveillants par des modules de l'application

L'application peut supprimer par défaut les fichiers si leur réparation est impossible. La suppression par défaut peut être exécutée lors du traitement des fichiers par des modules, tels que le Contrôle des Applications, l'Antivirus Courrier, l'Antivirus Fichiers, lors de l'exécution des tâches d'analyse, ainsi que lors de la détection d'une activité dangereuse des applications par le module Surveillance du système.

Particularité de connexion au portail Centre d'administration de Kaspersky Small Office Security

Pour assurer une possibilité de connexion au portail Centre d'administration de Kaspersky Small Office Security, lors de l'installation sur le serveur de fichier, Kaspersky Small Office Security ajoute kaspersky.com à la liste des sites Internet de confiance dans les paramètres du navigateur Internet Explorer.

Restrictions de fonctionnement de certains modules lors de l'installation collective de l'application avec Kaspersky Fraud Prevention for Endpoint

Le fonctionnement des modules suivants de Kaspersky Small Office Security est limité dans la Navigation sécurisée si l'application est installée ensemble avec Kaspersky Fraud Prevention for Endpoint :

- Antivirus Internet, sauf Anti-Phishing ;
- Contrôle Internet ;
- URL Advisor ;
- Anti-bannière.

GLOSSAIRE

A

Activation de l'application

Toutes les fonctions de l'application sont disponibles. 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 transmis via 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 d'exploitation peut présenter une menace pour la sécurité. Les objets identifiés à l'aide de l'analyseur heuristique sont considérés comme potentiellement infectés. Par exemple, un objet contenant une succession d'instructions propres aux objets malveillants (ouverture d'un fichier, écriture dans le fichier) peut être considéré comme potentiellement infecté.

Application incompatible

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

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 adresses de 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 antivirus

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

Blocage d'un objet

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

C

Code d'activation

Code que vous obtenez après avoir acheté une licence d'utilisation de Kaspersky Small Office Security. Ce code est indispensable pour activer l'application.

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

COFFRE-FORT VIRTUEL

Stockage spécial des données dans lequel les fichiers sont conservés sous forme chiffrée. Pour obtenir l'accès à ces fichiers, un mot de passe doit être saisi. Les coffres-forts virtuels servent à empêcher l'accès non autorisé aux données des utilisateurs.

COURRIER INDESIRABLE

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

COURRIER INDESIRABLE POTENTIEL

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 DE MENACE

Indice de probabilité selon lequel le programme d'ordinateur peut présenter 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 en environnement virtuel (l'analyse des fonctions de système appelées par l'application).

Le degré de menace permet d'identifier le comportement type des 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

ENREGISTREUR DE FRAPPES

Application conçue pour enregistrer de façon masquée les touches sur lesquelles l'utilisateur appuie pendant l'utilisation de l'ordinateur. Les enregistreurs de frappe sont aussi appelés keyloggers.

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 COMPRESSE

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

G

GROUPE DE CONFIANCE

Groupe dans lequel Kaspersky Small Office Security place une application ou un processus en fonction de l'existence d'une signature numérique pour l'application, de la réputation de l'application dans Kaspersky Security Network, de la fiabilité de la source de l'application et du danger potentiel des actions exécutées par l'application ou le processus. Sur la base de l'appartenance de l'application au groupe de confiance, Kaspersky Small Office Security peut imposer des restrictions dans le système d'exploitation sur les actions de l'application en question.

Kaspersky Small Office Security prévoit les groupes de confiance suivants : De confiance, Restrictions faibles, Restrictions élevées et Douteuses.

H

HYPERVISEUR

L'application qui assure l'utilisation parallèle de plusieurs systèmes d'exploitation sur un ordinateur.

K

KASPERSKY SECURITY NETWORK (KSN)

Infrastructure des services en ligne et des services offrant l'accès à la base opérationnelle de connaissances de Kaspersky Lab sur la réputation des fichiers, des ressources Internet et du logiciel. L'utilisation des données de Kaspersky Security Network permet aux applications de Kaspersky Lab de réagir plus rapidement 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 deux caractères principaux utilisés dans les masques de fichiers sont * et ? (où * représente n'importe quel nombre de n'importe quel caractère et ? représente un seul caractère).

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.

MODULES DE L'APPLICATION

Fichiers qui font partie du paquet d'installation d'une application de Kaspersky Lab et qui sont chargés d'effectuer les tâches principales. A chaque type de tâches réalisées par l'application (protection, analyse, mise à jour des bases et des modules d'application) correspond son propre module d'application.

MODULES DE LA PROTECTION

Parties de Kaspersky Small Office Security conçues pour protéger l'ordinateur contre les différents types de menaces (par exemple, Anti-Spam, Anti-Phishing). Chaque module de la protection est relativement indépendant des autres modules et peut être désactivé ou configuré séparément.

N

NAVIGATION SECURISEE

Mode spécial du navigateur Internet standard conçu pour les opérations financières et les achats sur Internet. L'utilisation de la Navigation sécurisée protège les données que vous saisissez sur les sites Internet des banques et des systèmes de paiement (par exemple, numéro de carte bancaire, mots de passe pour accéder aux services de la banque en ligne), et empêche le vol des moyens de paiement lors de la réalisation de transactions en ligne. Dans ce cas, un message de lancement de la Navigation sécurisée protégé s'affiche dans le navigateur normal utilisé pour la connexion au site Internet.

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 une partie du code correspond parfaitement à une partie du code d'un programme connu présentant une menace. Les experts de Kaspersky Lab déconseillent de manipuler ce type d'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 ce type de 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 d'un individu malintentionné ou d'un programme malveillant dans le système d'exploitation.

Dans les systèmes d'exploitation Windows, tout programme qui s'infiltre dans le système d'exploitation et intercepte les fonctions système (Windows API) est considéré comme un rootkit (outil de dissimulation d'activité). L'interception et la modification des fonctions API de bas niveau permet avant tout à ce genre de programme de bien masquer sa présence dans le système d'exploitation. De plus, en général, un rootkit masque la présence dans le système d'exploitation 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 d'exploitation (ils sont aussi invisibles).

P

PAQUET DE MISE A JOUR

Paquets des fichiers pour la mise à jour des bases et 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 LA TACHE

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

PHISHING

Type d'escroquerie sur Internet dans le but d'obtenir un accès illégal aux données confidentielles des utilisateurs.

PROCESSUS DE CONFIANCE

Processus d'une application dont les opérations sur les fichiers ne sont pas contrôlées par l'application de Kaspersky Lab dans le cadre de la protection en temps réel. En cas de détection d'une activité suspecte du processus de confiance, Kaspersky Small Office Security exclut ce processus de la liste des processus de confiance et bloque ses actions.

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.

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 présentent aucun danger pour l'ordinateur.

S

SAUVEGARDE DES DONNEES

Création de copies de sauvegarde des données enregistrées sur l'ordinateur. Les copies de sauvegarde sont créées pour prévenir toute perte de données due à un vol, à une panne du matériel ou aux actions d'individus malintentionnés.

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.

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 d'application.

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.

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 pour autant 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 pour l'analyse à la demande.

Supposons que vous ayez une archive qui a été analysée par une application de Kaspersky Lab et à laquelle on a attribué 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 à nouveau.

Restrictions de la technologie iChecker :

- cette 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.

TRAÇAGES

Exécution et débogage de l'application qui s'arrêtent après l'exécution de chaque étape afin d'en afficher les résultats.

TACHE

Fonctions, exécutées par l'application de Kaspersky Lab, sont réalisées sous forme des tâches, par exemple : la tâche d'analyse complète, la tâche de mise à jour.

V

VIRUS

Programme qui infecte d'autres programmes : y ajoute son propre code pour obtenir l'administration lors du lancement des fichiers infectés. Cette définition simple permet de révéler l'action principale exécutée par un virus : l'infection.

VIRUS INCONNU

Nouveau virus pour lequel 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.

VULNERABILITE

Défaut dans le système d'exploitation ou dans le programme qui peut être utilisé par les éditeurs d'un logiciel malveillant pour pénétrer dans le système d'exploitation ou dans le programme et pour nuire à son intégrité. Un grand nombre de vulnérabilités dans un système d'exploitation en fragilise le fonctionnement car les virus installés dans le système d'exploitation peuvent entraîner des erreurs de fonctionnement du système d'exploitation et des programmes installés.

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 tablettes, des smartphones et d'autres appareils nomades.

La société offre également des services pour la protection des postes de travail, des serveurs de fichiers, des serveurs 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 mises à jour toutes les heures*, tandis que *les bases antispam* sont *mises à jour 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), Openwave Messaging (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.

REALISATIONS. 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.viruslist.com/fr
Laboratoire de virus :	newvirus@kaspersky.com (uniquement pour l'envoi d'objets suspects sous forme d'archive)
Forum de Kaspersky Lab :	http://forum.kaspersky.com/index.php?showforum=105

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 marques déposées et les marques de services appartiennent à leurs propriétaires respectifs.

Android, Google, Google Chrome, YouTube sont des marques de commerce de Google, Inc.

Dropbox est une marque déposée de Dropbox, Inc.

Intel, Celeron, Atom sont des marques déposées de Intel Corporation aux États-Unis et dans d'autres pays.

Mac est une marque déposée de Apple Inc.

Mail.ru est une marque déposée de OOO "Mail.Ru".

Microsoft, Windows, Windows Vista, Winwos Server, DirectX, Bing, Outlook, 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.

OpenGL est une marque déposée de SGI.

Skype est une marque de commerce de la société Skype.

VMware est une marque de commerce de VMware, Inc. enregistrée aux Etats-Unis ou dans d'autres juridictions VMware, Inc.

INDEX